PEMBUATAN BANK SOAL DAN ANALISIS BUTIR SOAL MATA KULIAH KRIPTOGRAFI UNTUK MAHASISWA PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER UNIVERSITAS NEGERI JAKARTA

NELA MAHLIANA LATUCONSINA
5235117124

Skripsi Ini Ditulis Sebagai Persyaratan dalam Memperoleh Gelar Sarjana Pendidikan

PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS NEGERI JAKARTA
2015

HALAMAN PENGESAHAN

NAMA DOSEN	TANDA TANGAN	TANGGAL
Prasetyo Wibowo Yunanto, ST, M.Eng (Dosen Pembimbing I)		29/7/2015
Drs. Bachren Zaini, M.Pd (Dosen Pembimbing II)		29/7/2015

PENGESAHAN PANITIA UJIAN SKRIPSI

NAMA DOSEN	TANDA TANGAN	TANGGAL
Drs. Wisnu Djatmiko, MT (Ketua Sidang)		29/7/2015
Dr. Yuliatri Sastrawijaya, M.Pd (Dosen Penguji)		29/7 2015
Bambang Prasetya Adhi, M.Kom (Dosen Ahli)		29/7/2015

Tanggal Lulus:

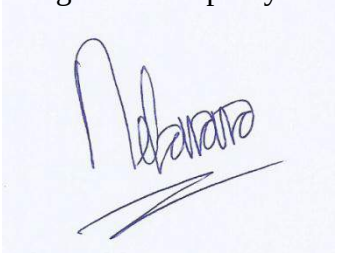
HALAMAN PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Karya tulis skripsi saya ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik sarjana, baik di Universitas Negeri Jakarta maupun di perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendiri dengan arahan dosen pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Penyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma yang berlaku di Universitas Negeri Jakarta.

Jakarta, 21 Juni 2015

Yang membuat pernyataan



Nela Mahliana Latuconsina

5235117124

PEMBUATAN BANK SOAL DAN ANALISIS BUTIR SOAL MATA KULIAH KRIPTOGRAFI UNTUK MAHASISWA PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER UNIVERSITAS NEGERI JAKARTA

NELA MAHLIANA LATUCONSINA

ABSTRAK

Latar belakang dari penelitian ini adalah tingkat kecurangan mahasiswa yang tinggi pada saat ujian mata kuliah kriptografi. Hal ini dapat di atasi dengan penggunaan tes esai. Akan tetapi, tes esai memiliki banyak kelemahan dalam hal pengkoreksian. Oleh karena itu, solusi yang tepat untuk mengatasi masalah di atas adalah pemberian paket soal yang berbeda-beda kepada mahasiswa. Butir soal dikumpulkan dan dijadikan sebuah bank soal mata kuliah kriptografi.

Penelitian ini bertujuan untuk membuat bank soal mata kuliah kriptografi untuk mahasiswa program studi Pendidikan Teknik Informatika dan Komputer Universitas Negeri Jakarta. Penelitian ini berfungsi sebagai bahan ujian mata kuliah kriptografi di Pendidikan Teknik Informatika dan Komputer Universitas Negeri Jakarta. Selain itu, bank soal dapat digunakan sebagai bank soal ujian online. Penelitian dilakukan dengan menggunakan sampel yaitu mahasiswa PTIK UNJ yang sedang mengambil mata kuliah kriptografi. Metode yang digunakan pada penelitian ini adalah metode kuantitatif berupa analisis data dengan menggunakan perhitungan statistika. Metode kuantitatif yang digunakan pada penelitian ini adalah metode korelasi.

Tahap awal yang dilakukan pada penelitian ini adalah membuat indikator mata kuliah kriptografi. Hal ini dibuat berdasarkan rencana program kegiatan pembelajaran semester mata kuliah kriptografi yang dibuat oleh dosen pengampu mata kuliah kriptografi.

Berdasarkan indikator yang telah dibuat, penyusunan soal mata kuliah kriptografi dilakukan. Selanjutnya dilakukan uji taraf kesukaran, daya beda, efektivitas pengecoh, dan validitas butir soal. Kesimpulan dari penelitian ini adalah bank soal mata kuliah kriptografi yang dibuat telah dilakukan analisis butir soal berupa taraf kesukaran, daya beda, efektivitas pengecoh, dan validitas butir soal.

Kata kunci: bank soal, kriptografi, analisis butir soal.

BUILD A QUESTION BANK AND ITEM ANALYSIS OF CRYPTOGRAPHY SUBJECT FOR STUDY PROGRAM STUDENTS OF EDUCATIONAL INFORMATICS AND COMPUTER ENGINEERING JAKARTA STATE UNIVERSITY

NELA MAHLIANA LATUCONSINA

ABSTRACT

The background of this research is a high level of cheating students when the test in cryptography subject. This can be overcome with the use of an essay test. However, an essay test correction have many weaknesses in it. Because of that, a solution to overcome the problem is the difference package test for students. The question will be collected and used as a question bank of cryptography subject.

This research is aimed to make questions bank of cryptography subject for study program students of Educational Informatics and Computer Engineering Jakarta State University. This study serves as an examination of cryptography subject at Educational Informatics and Computer Engineering Jakarta State university. Besides, the questions bank can be used as a test of online. This research used students of PTIK UNJ who taking the cryptography subject as a sample. The method used in this research is a quantitative method as a data analysis by using calculation of statistics. A quantitative method used in this research is the correlation method.

An early stage conducted in this research are to make indicators of cryptography subject. These are made based on the program plan learning semester activities of cryptography subject that made by lecturer teaching of cryptography subject.

Based on the indicators that have been made, do the preparation of question about cryptography. Futhermore, do the test of the difficulty level, diference of resources, the effectiveness of distractor, and item validity. The conclusion of this research is the questions bank of cryptography subject that made by the researcher has been done about item analysis form the difficulty level, diference of resources, the effectiveness of distractor, and item validity.

Keywords: questions bank, cryptography, item analysis

KATA PENGANTAR

Ucapan syukur kepada Tuhan Yang Maha Esa sehingga skripsi dengan judul "Pembuatan Bank Soal dan Analisis Butir Soal Mata Kuliah Kriptografi untuk Mahasiswa Program Studi Pendidikan Teknik Informatika dan Komputer Universitas Negeri Jakarta" dapat diselesaikan. Skripsi disusun untuk memenuhi persyaratan mendapatkan gelar sarjana pendidikan.

Selama penyusunan skripsi, banyak bantuan yang saya terima dari berbagai pihak. Oleh karena itu, dalam kesempatan ini saya mengucapkan terima kasih kepada:

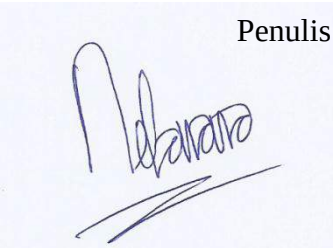
1. Bapak Wisnu Djatmiko, M.T., selaku Ketua Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Jakarta.
2. Bapak Prasetyo Wibowo Yunanto, S.T., M.Eng., selaku Ketua Program Studi Pendidikan Teknik Informatika dan Komputer, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Jakarta serta selaku dosen pembimbing pertama dalam penyusunan skripsi.
3. Bapak Drs. Bachren Zaini, M.Pd., selaku dosen pembimbing kedua dalam penyusunan skripsi.
4. Alm. Hamid Latuconsina dan Sumiati Latulanit, selaku kedua orang tua saya tercinta yang selama ini dengan sabar telah mendidik dan membimbing saya.
5. Riel Thamrin Latuconsina dan Deni Sidik Latuconsina, selaku paman saya yang selama ini dengan sabar telah membimbing saya.
6. Annisa Anggraini, Anissa Dhea Priscilia, Arum Rusintya, Angelina Margareth, Dini Puspitasari, Fariqa Afiani, Nur Meilinda, Septriana Putri, Windya Putri Yuliani, dan Yohana Eltidya yang telah mendukung, membantu, memberi masukan, dan bertukar pikiran kepada saya selama ini.
7. Abdul Aziz Fitriono dan Rima Irmayani Rahmat yang banyak membantu dan memberikan informasi yang berguna selama penyusunan skripsi.

Saya juga mengucapkan terima kasih kepada kakak dan adik saya tercinta, teman-teman saya, keluarga besar mahasiswa PTIK 2011, dan pihak-pihak yang mendukung kelancaran pengerjaan skripsi ini.

Akhir kata saya meminta maaf atas segala kesalahan dalam skripsi ini dan berharap skripsi ini bermanfaat bagi semua pihak serta dapat dikembangkan menjadi lebih baik lagi.

Jakarta, 01 Juli 2015

Penulis



Nela Mahliana Latuconsina

DAFTAR ISI

Halaman

HALAMAN PENGESAHAN i

HALAMAN PERNYATAAN ii

ABSTRAK iii

ABSTRACT iv

KATA PENGANTAR v

DAFTAR ISI vii

DAFTAR TABEL ix

DAFTAR GAMBAR x

DAFTAR LAMPIRAN xi

BAB I PENDAHULUAN 1

1.1 Latar Belakang Masalah 1

1.2 Identifikasi Masalah 4

1.3 Pembatasan Masalah 4

1.4 Perumusan Masalah 5

1.5 Tujuan Penelitian 5

1.6 Manfaat Penelitian 5

BAB II LANDASAN TEORI 6

2.1 Kerangka Teori 6

2.1.1 Analisis 6

2.1.2 Butir Soal 7

2.1.3 Kriptografi 9

2.1.4 Bank Soal 12

2.1.5 Ujian 13

2.1.6 Analisis Butir Soal 14

2.1.7 Analisis Butir Soal Mata Kuliah Kriptografi 17

2.1.8 Analisis Butir Soal Mata Kuliah Kriptografi sebagai Bank Soal 17

2.1.9 Analisis Butir Soal Mata Kuliah Kriptografi sebagai Bank Soal Ujian 17
2.2 Kerangka Berpikir 18
BAB III METODE PENELITIAN 20
3.1 Tempat dan Waktu Pelaksanaan 20
3.2 Metode Penelitian 20
3.3 Sampel 20
3.4 Peranan Penelitian dalam Analisis Butir Soal 21
3.5 Rancangan Penelitian 21
3.5.1 Strategi Penelitian 21
3.5.2 Implementasi Penelitian 25
3.5.3 Uji Coba dan Evaluasi pada Butir Soal 25
3.6 Instrumen Penelitian 25
3.7 Teknik Analisis Data 26
3.7.1 Pengujian Taraf Kesukaran Butir Soal 26
3.7.2 Pengujian Daya Beda Butir Soal 26
3.7.3 Pengujian Efektivitas Pengecoh Butir Soal 27
3.7.4 Pengujian Validitas Butir Soal 27
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 28
4.1 Hasil Penelitian 28
4.1.1 Standar Kompetensi, Kompetensi Dasar, dan Indikator Mata Kuliah Kriptografi 28
4.1.2 Hasil Analisis Butir Soal Mata Kuliah Kriptografi Tahap I 33
4.1.3 Hasil Analisis Butir Soal Mata Kuliah Kriptografi Tahap II 41
4.1.2 Hasil Analisis Butir Soal Mata Kuliah Kriptografi Tahap III 52
4.1.5 Hasil Analisis Butir Soal untuk Bank Soal Mata Kuliah Kriptografi..63
4.2 Pembahasan 77
BAB V KESIMPULAN DAN SARAN 79
5.1 Kesimpulan 79
5.2 Saran 80
DAFTAR PUSTAKA 81

LAMPIRAN 82

DAFTAR TABEL

Halaman

Tabel 4.1 SK, KD, dan Indikator Mata Kuliah Kriptografi 29
Tabel 4.2 Hasil Analisis Butir Soal untuk Paket A 34
Tabel 4.3 Hasil Analisis Butir Soal untuk Paket B 36
Tabel 4.4 Hasil Analisis Butir Soal untuk Paket C 38
Tabel 4.5 Hasil Analisis Butir Soal untuk Paket D 40
Tabel 4.6 Hasil Analisis Butir Soal untuk Paket E 42
Tabel 4.7 Hasil Analisis Butir Soal untuk Paket F 45
Tabel 4.8 Hasil Analisis Butir Soal untuk Paket G 47
Tabel 4.9 Hasil Analisis Butir Soal untuk Paket H 50
Tabel 4.10 Hasil Analisis Butir Soal untuk Paket 1 53
Tabel 4.11 Hasil Analisis Butir Soal untuk Paket 2 56
Tabel 4.12 Hasil Analisis Butir Soal untuk Paket 3 58
Tabel 4.13 Hasil Analisis Butir Soal untuk Paket 4 60
Tabel 4.14 Hasil Analisis Butir Soal untuk Bank Soal Mata Kuliah Kriptografi 64

DAFTAR GAMBAR

Halaman

Gambar 1.1 Pembagian Soal I 2
Gambar 1.2 Pembagian Soal II 2

DAFTAR LAMPIRAN

Halaman

Lampiran 1: Kisi-kisi Instrumen Pengujian Tahap I 82
Lampiran 2: Validitas Butir Paket Soal A 85
Lampiran 3: Paket Soal A 90
Lampiran 4: Perhitungan Analisis Butir Soal untuk Paket A 94
Lampiran 5: Validitas Butir Paket Soal B 96
Lampiran 6: Paket Soal B 101
Lampiran 7: Perhitungan Analisis Butir Soal untuk Paket B 105
Lampiran 8: Validitas Butir Paket Soal C 107
Lampiran 9: Paket Soal C 112
Lampiran 10: Perhitungan Analisis Butir Soal untuk Paket C 116
Lampiran 11: Validitas Butir Paket Soal D 118
Lampiran 12: Paket Soal D 123
Lampiran 13: Perhitungan Analisis Butir Soal untuk Paket D 127
Lampiran 14: Kisi-kisi Instrumen Pengujian Tahap II 129
Lampiran 15: Validitas Butir Paket Soal E 133
Lampiran 16: Paket Soal E 140
Lampiran 17: Perhitungan Analisis Butir Soal untuk Paket E 146
Lampiran 18: Validitas Butir Paket Soal F 149
Lampiran 19: Paket Soal F 156
Lampiran 20: Perhitungan Analisis Butir Soal untuk Paket F 163
Lampiran 21: Validitas Butir Paket Soal G 166
Lampiran 22: Paket Soal G 173
Lampiran 23: Perhitungan Analisis Butir Soal untuk Paket G 179
Lampiran 24: Validitas Butir Paket Soal H 182
Lampiran 25: Paket Soal H 189
Lampiran 26: Perhitungan Analisis Butir Soal untuk Paket H 195
Lampiran 27: Kisi-kisi Instrumen Pengujian Tahap III 198

Lampiran 28: Validitas Butir Paket Soal 1 200
Lampiran 29: Paket Soal 1 209
Lampiran 30: Perhitungan Analisis Butir Soal untuk Paket1 216
Lampiran 31: Validitas Butir Paket Soal 2 218
Lampiran 32: Paket Soal 2 227
Lampiran 33: Perhitungan Analisis Butir Soal untuk Paket 2 234
Lampiran 34: Validitas Butir Paket Soal 3 236
Lampiran 35: Paket Soal 3 245
Lampiran 36: Perhitungan Analisis Butir Soal untuk Paket 3 252
Lampiran 37: Validitas Butir Paket Soal 4 254
Lampiran 38: Paket Soal 4 262
Lampiran 39: Perhitungan Analisis Butir Soal untuk Paket 4 269
Lampiran 40: Kisi-kisi Instrumen Bank Soal Mata Kuliah Kriptografi 271
Lampiran 41: Bank Soal Mata Kuliah Kriptografi..... 274

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Universitas Negeri Jakarta (UNJ) merupakan salah satu universitas negeri di Indonesia yang bergerak dalam bidang pendidikan. Salah satu program studi yang banyak diminati oleh calon mahasiswa baru adalah Pendidikan Teknik Informatika dan Komputer (PTIK). Program studi PTIK merupakan satu-satunya program studi pendidikan yang bergerak dalam bidang komputer.

Mahasiswa program studi PTIK wajib mengambil 131 sks mata kuliah wajib dan minimal 13 sks untuk mata kuliah pilihan. Mata kuliah pilihan yang dibuka pada semester 102 adalah pengolahan citra, kriptografi, *e-commerce*, perancangan strategis sistem informasi, dan data mining. Salah satu mata kuliah pilihan yang cukup diminati adalah kriptografi. Pada semester 102, mahasiswa yang mengambil mata kuliah kriptografi sebanyak 93 orang. Karena banyaknya mahasiswa yang mengambil mata kuliah kriptografi, kelas harus dibagi menjadi tiga dengan jumlah maksimal mahasiswa per kelas yaitu 40 orang.

Dengan padatnya mahasiswa dalam kelas, hal yang perlu dihindari adalah perbuatan curang mahasiswa pada saat ujian berlangsung. Pada saat ujian berlangsung, kelas harus dibagi menjadi dua kembali dengan jumlah maksmimal mahasiswa per kelas yaitu 20 orang. Apabila hal tersebut dilakukan, kelas menjadi tidak padat dan mengurangi resiko perbuatan curang mahasiswa. Namun dengan

membagi kelas menjadi dua saja tidak cukup. Soal ujian yang sama antar mahasiswa dalam kelas juga dapat meningkatkan resiko perbuatan curang mahasiswa. Soal ujian harus dikelompokkan menjadi beberapa paket soal. Dua paket soal saja belum bisa mengurangi resiko perbuatan curang mahasiswa. Sebagai contoh lihat Gambar 1.1 dan Gambar 1.2 di bawah ini.

A	B	A	B
B	A	B	A
A	B	A	B
B	A	B	A

Gambar 1.1 Pembagian Soal I

A	B	A	B
A	B	A	B
A	B	A	B
A	B	A	B

Gambar 1.2 Pembagian Soal II

Apabila soal hanya terbagi menjadi dua paket seperti Gambar 1.1, mahasiswa yang mendapatkan paket soal yang sama yaitu berada di serong depan dan belakangnya. Hal tersebut membuat mahasiswa masih dapat menanyakan jawaban soal ujian. Selain itu, pembagian soal dengan dua paket yang berselingan seperti Gambar 1.1 tidak efisien waktu karena waktu yang diperlukan untuk mebagikan soal kepada peserta ujian sangat lama. Sedangkan apabila soal terbagi menjadi dua paket seperti Gambar 1.2, mahasiswa yang berada di baris yang sama akan mendapatkan paket soal yang sama. Hal ini tentu memudahkan mahasiswa untuk menanyakan jawaban soal ujian.

Salah satu solusi untuk menurunkan tingkat kecurangan mahasiswa pada saat ujian adalah penggunaan tes dalam bentuk esai. Akan tetapi, tes esai memiliki

banyak kelemahan dalam hal pengkoreksian jawaban. Diantaranya adalah cara memeriksanya banyak dipengaruhi oleh unsur-unsur subjektif, waktu untuk koreksinya lama, serta membutuhkan pertimbangan individual lebih banyak dari penilai.

Oleh karena itu, solusi yang tepat untuk mengurangi resiko perbuatan curang mahasiswa pada saat ujian berlangsung adalah dengan membuat bank soal yang terdiri dari minimal lima model soal setiap indikator pada mata kuliah kriptografi. Model soal yang dibuat tentunya harus tervalidasi dan memiliki tingat kesulitan yang sama.

Dalam proses validasi, soal yang telah dibuat sesuai dengan indikator pada mata kuliah kriptografi akan divalidasi terlebih dahulu oleh ahli materi. Ahli materi akan melihat apakah setiap soal yang telah dibuat sesuai dengan indikator pada mata kuliah kriptografi. Setelah ahli materi menyatakan bahwa soal telah valid, soal akan diujikan sebagai sampel kepada mahasiswa program studi PTIK. Setelah soal diujikan, penulis akan melakukan perhitungan statistika pada setiap butir soal dengan menggunakan skor peserta ujian. Setelah itu, setiap butir soal dapat diketahui tingkat kevaliditasannya.

Berdasarkan hal tersebut, penulis membuat karya tulis yang berjudul “Pembuatan Bank Soal dan Analisis Butir Soal Mata Kuliah Kriptografi untuk Mahasiswa Program Studi Pendidikan Teknik Informatika dan Komputer Universitas Negeri Jakarta”.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, penulis mengidentifikasi masalah sebagai berikut:

a. Tingkat kecurungan mahasiswa meningkat pada saat ujian berlangsung.
b. Dua paket soal tidak dapat dijadikan solusi untuk menurunkan tingkat kecurangan mahasiswa pada saat ujian berlangsung.
c. Penggunaan tes esai tidak dapat digunakan karena memiliki banyak kelemahan pada teknik pengkoreksian jawaban.

1.3 Pembatasan Masalah

Penulis membuat pembatasan masalah dengan tujuan agar pembahasannya dapat terarah pada sasarannya. Adapun masalah yang dibahas penulis di dalam penulisan ilmiah yaitu:

a. Bank soal ini merupakan soal yang dibuat untuk ujian tertulis maupun ujian online.
b. Bank soal ini terdiri atas minimal lima model soal setiap indikator pada mata kuliah kriptografi yang sudah melewati proses validasi.
c. Setiap model soal untuk setiap indikator yang terdapat pada bank soal ini memiliki tingkat kesulitan yang sama.
d. Setiap butir soal dibuat untuk menilai ranah kognitif mahasiswa program studi PTIK UNJ.

1.4 Perumusan Masalah

Permasalahan yang akan dibahas dalam penelitian ini adalah:

- Bagaimana membuat bank soal mata kuliah kriptografi untuk mahasiswa program studi PTIK UNJ yang terdiri atas minimal lima model soal setiap indikator dan setiap butir soal pada setiap indikator telah tervalidasi dan memiliki tingkat kesulitan yang sama.

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk membuat bank soal mata kuliah kriptografi untuk mahasiswa program studi PTIK UNJ yang terdiri atas minimal lima model soal setiap indikator dan setiap butir soal pada setiap indikator telah tervalidasi dan memiliki tingkat kesulitan yang sama.

1.6 Manfaat Penelitian

Hasil dari pembuatan tugas akhir ini diharapkan dapat bermanfaat untuk mahasiswa dan dosen, diantaranya yaitu:

a. Dapat mengukur hasil belajar mahasiswa dengan resiko perbuatan curang mahasiswa yang kecil.
b. Dapat menjadi bank soal ujian mata kuliah kriptografi.
c. Dapat menjadi bank soal ujian online.

BAB II

LANDASAN TEORI

2.1 Kerangka Teori

2.1.1 Analisis

Secara etimologis, kata ‘analisis’ yang dalam Bahasa Inggris ‘*analysis*’ berasal dari leksem bahasa Yunani *analyein* (gabungan morfem *ana-* dan *lyein*) berarti ‘melonggarkan’ atau ‘memisahkan’ (memisahkan keseluruhan menjadi bagian-bagian).

Menurut Kamus Besar Bahasa Indonesia analisis /ana·li·sis/ berarti (1) Penyelidikan terhadap suatu peristiwa (karangan, perbuatan, dsb) untuk mengetahui keadaan yang sebenarnya (sebab-musabab, duduk perkaranya, dsb); (2) Penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri serta hubungan antarbagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan; (3) Penyelidikan kimia dengan menguraikan sesuatu untuk mengetahui zat bagiannya dsb; (4) Penjabaran sesudah dikaji sebaik-baiknya; (5) Pemecahan persoalan yang dimulai dengan dugaan akan kebenarannya.

Menurut Dwi Prastowo Darminto dan Rifka Julianty (2005;52), analisis adalah penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan. Berdasarkan pengertian di atas, penulis menyimpulkan bahwa analisis adalah suatu kegiatan memperhatikan, mengamati,

dan memecahkan suatu masalah (mencari jalan keluar) yang dilakukan oleh seseorang.

2.1.2 Butir Soal

Menurut Purwanto (2009;74), soal merupakan pertanyaan atau pernyataan yang menimbulkan situasi masalah yang harus dipecahkan oleh siswa. Penugasan siswa diketahui dari kemampuannya membuat pemecahan masalah. Satuan untuk soal adalah butir sehingga tiap item pertanyaan atau pernyataan dikenal sebagai butir soal.

Berdasarkan pengertian di atas, penulis menyimpulkan bahwa butir soal adalah tiap-tiap item pertanyaan atau pernyataan yang berisikan suatu masalah yang harus dipecahkan oleh siswa guna mengukur tingkat hasil belajar mahasiswa.

Setiap butir soal yang dibuat dapat mengukur kemampuan siswa ataupun mahasiswa. Kemampuan mahasiswa yang diukur dalam analisis pada skripsi ini adalah ranah kognitif dengan menggunakan taksonomi *Bloom*. Benjamin S. Bloom membagi dan menyusun tingkat hasil belajar kognitif mulai dari yang paling rendah dan sederhana yaitu hafalan sampai yang paling tinggi dan kompleks yaitu evaluasi (Arikunto, 2002:117-120; Purwanto, 2009:50-51). Terdapat enam tingkatan pada taksonomi Bloom untuk mengukur ranah kognitif, yaitu:

1. Hafalan (C1)

Kemampuan menghafal (*knowledge*) merupakan kemampuan kognitif yang paling rendah. Kemampuan ini merupakan kemampuan memanggil kembali fakta

yang disimpan dalam otak yang digunakan untuk merespon suatu masalah. Dalam kemampuan tingkat ini fakta dipangggil kembali persis seperti ketika disimpan. Mengenal dan mengungkap kembali, pada umumnya dikategorikan menjadi satu jenis yaitu ingatan. Contoh: Tanggal proklamasi kemerdekaan Republik Indonesia adalah 17 Agustus 1945.

2. Pemahaman (C2)

Kemampuan pemahaman (*comprehension*) merupakan kemampuan kognitif untuk melihat hubungan fakta dengan fakta. Menghafal fakta tidak lagi cukup karena pemahaman menuntut pengetahuan akan fakta dan hubungannya. Contoh: Memahami proses terjadinya hujan.

3. Penerapan (C3)

Kemampuan penerapan (*application*) merupakan kemampuan kognitif untuk memahami aturan, hukum, rumus, dan sebagainya yang digunakan untuk memecahkan masalah. Contoh: Berapakah volume air yan dapat ditampung pada sebuah tabung dengan tinggi 500 cm dengan alas berdiameter 460 cm?

4. Analisis (C4)

Kemampuan analisis (*analysis*) merupakan kemampuan kognitif untuk menganalisis suatu hubungan atau situasi yang kompleks atas konsep-konsep dasar. Contoh: Mengapa pada saat mendung dan angin kencang tidak segera turun hujan?

5. Sintesis (C5)

Kemampuan sintesis (*synthesis*) merupakan kemampuan kognitif untuk menggabungkan atau menyusun kembali hal-hal yang spesifik agar dapat

mengembangkan suatu struktur baru. Secara singkat dapat dikatakan bahwa dengan soal sintesis ini, kemampuan yang diukur adalah kemampuan untuk melakukan generalisasi. Contoh: Dengan mengetahui situasi daerah dan milik dalam hal kekayaan bahan mentah serta semangat penduduk di suatu daerah yang kini dapat berkembang pesat menjadi kota pelabuhan yang besar maka kota-kota kecil di tepi mana yang mempunyai potensi untuk menjadi sebuah kota pelabuhan yang besar?

6. Evaluasi (C6)

Kemampuan evaluasi (*evaluation*) merupakan kemampuan kognitif untuk menerapkan pengetahuan dan kemampuan yang telah dimiliki untuk menilai suatu kasus yang diajukan oleh penyusun soal. Contoh: Bagaimanakah kondisi morfologi lembah anai? Jelaskan tingkat potensi longsor di daerah tersebut?

2.1.3 Kriptografi

Mata kuliah kriptografi pada Prodi PTIK UNJ memiliki bobot senilai 2 sks. Mata kuliah kriptografi menjelaskan tentang pengenalan kriptografi, protokol kriptografi, algoritma kriptografi klasik, cipher blok dan cipher aliran, algoritma kriptografi simetris, algoritma kriptografi asimetris, manajemen kunci, algoritma *hash*, konsep tanda tangan digital, serta penggunaan kriptografi dalam kehidupan sehari-hari.

Setelah mengikuti mata kuliah kriptografi, mahasiswa diharapkan dapat mampu mengembangkan pemahaman dan apresiasi untuk keamanan komputer, khususnya keamanan jaringan. Selain itu, mahasiswa diharapkan mampu

mengembangkan infrastruktur teknologi informasi dengan pengamanan data dan informasi yang baik.

Tingkat kesulitan menurut taksonomi Bloom yang dimiliki oleh indikator pada mata kuliah kriptografi berada pada rentang C1 (hafalan) sampai dengan C4 (analisis). Materi perkembangan kriptografi, jenis-jenis serangan terhadap kriptografi, algoritma kriptografi DES, AES, RC4, A5, RSA, Rabin, cipher blok, serangan terhadap cipher aliran, fungsi *hash*, dan konsep tanda tangan digital memiliki tingkat taksonomi Bloom yaitu C1. Pemilihan tingkat C1 pada materi perkembangan kriptografi dan jenis-jenis serangan terhadap kriptografi karena materi ini dianggap materi yang relatif mudah. Materi ini mejelaskan tentang konsep dasar kriptografi. Pemilihan tingkat C1 pada materi algoritma kriptografi DES, AES, RC4, A5, RSA, Rabin, cipher blok, serangan terhadap cipher aliran, fungsi *hash*, dan konsep tanda tangan digital karena materi ini dianggap materi yang relatif sulit sehingga dikhawatirkan mahasiswa tidak dapat menjawab butir soal yang memiliki tingkat kesulitan yang tinggi.

Materi keamanan algoritma kriptografi, cipher aliran, kriptografi kunci publik, algoritma ElGamal, pembangkit bilangan prima dan acak semu memiliki tingkat taksonomi Bloom yaitu C2. Pemilihan tingkat C2 pada materi tersebut karena mahasiswa diharapkan dapat menjawab soal pada materi tersebut dengan tingkat kesulitan C2 (pemahaman).

Materi landasan matematika pada kriptografi, algoritma kriptografi klasik, operasi rangkaian bit, serta pembangkitan kunci memiliki tingkat taksonomi Bloom yaitu C3 (penerapan). Pemilihan tingkat C3 pada materi tersebut karena

materi tersebut dianggap sangat penting dalam penggunaan kriptografi dalam kehidupan sehari-hari. Mahasiswa diharapkan dapat menerapkan materi tersebut dengan baik. Materi penggunaan kriptografi dalam kehidupan sehari-hari memiliki tingkat taksonomi Bloom yaitu C4 (analisis). Pemilihan tingkat C4 pada materi tersebut karena mahasiswa diharapkan dapat melakukan analisis dari manfaat dan penggunaan kriptografi dalam kehidupan sehari-hari.

Jumlah tatap muka pada perkuliahan ini adalah 16 pertemuan di mana setiap pertemuan memiliki alokasi waktu sebanyak 100 menit. Alokasi waktu untuk UTS dan UAS adalah 200 menit di mana masing-masingnya memiliki alokasi waktu sebanyak 100 menit. Tugas terstruktur diberikan di luar waktu tatap muka. Mahasiswa dianjurkan untuk belajar mandiri minimal 25 kali dengan alokasi waktu masing-masingnya sebanyak 50 menit. Mahasiswa dianjurkan untuk belajar mandiri agar dapat mempersiapkan diri sebelum mendapatkan materi perkuliahan pada saat tatap muka.

Metode pembelajaran yang digunakan pada perkuliahan ini berupa ceramah, diskusi, penggunaan *viewer*, laptop, OHP, dan papan tulis atau *white board*. Penilaian yang dinilai dalam perkuliahan ini adalah kehadiran, UTS, UAS, dan tugas. Mahasiswa harus memiliki kehadiran minimal 80% untuk dapat mengikuti UAS. Bobot penilaian pada UTS sebanyak 30 %, sedangkan untuk UAS sebanyak 40%. Mahasiswa harus memahami minimal 80% dari materi yang diberikan. Bobot penilaian pada tugas sebanyak 30% dengan kriteria penilaiannya adalah menyelesaikan 100% tugas terstruktur.

Buku yang digunakan sebagai bahan referensi pada mata kuliah ini adalah "*Handbook of Applied Cryptography*" oleh Alfred Menezes, Paul Oorschot, dan Scott Vanstone. Selain itu, buku lainnya yang digunakan sebagai referensi pada mata kuliah ini adalah "*Cryptography and Network Security*" oleh William Stalling dan "*Aplied Cryptography*" oleh Bruce Schneier.

2.1.4 Bank Soal

Secara singkat, bank soal yang biasa dikenal pendidik didefinisikan sebagai kumpulan dari butir-butir soal. Bank soal tidak hanya mengacu pada sekumpulan soal-soal saja. Bank soal mengacu pada proses pengumpulan soal-soal, pemantauan dan penyimpanannya dengan informasi yang terkait sehingga mempermudah pengambilannya untuk merakit soal-soal (Thorndike, 1982).

Millman (dalam J. Umar, 1999) mendefinisikan bank soal sebagai kumpulan yang relatif besar, yang mempermudah dalam memperoleh pertanyaan-pertanyaan penyusun tes. "Mudah" mememiliki pengertian bahwa soal-soal tersebut diberi indeks, terstruktur, dan diberi keterangan sehingga mudah dalam pemilihannya untuk disusun sebagai perangkat tes pada suatu ujian.

Menurut Choppin (dalam J. Umar,1999) memberikan definisi bahwa bank soal merupakan sekumpulan dari butir-butir tes yang diorganisasikan dan dikatalogan untuk mencapai jumlah tertentu berdasarkan isi dan juga karakteristik butir. Karakteristik butir ini meliputi tingkat kesulitan, reliabilitas, validitas dan lain-lain.

Berdasarkan pengertian di atas, penulis menyimpulkan bahwa bank soal adalah kumpulan dari butir-butir soal yang terorganisir mulai dari penyusunan dan

penyimpanannya dengan menggunakan suatu informasi seperti nomor soal, indikator, maupun indeks soal yang dapat memudahkan penyusun soal untuk menyusun sebuah perangkat tes pada suatu ujian.

Berdasarkan pengertian di atas, dapat disimpulkan bahwa penyimpanan bank soal harus dilakukan di dalam komputer. Dalam pengembangan bank soal berskala kecil, kemungkinan besar dapat dilakukan tanpa bantuan komputer. Akan tetapi dalam pengembangan bank soal yang berskala besar, kemungkinannya kecil apabila pengembangan bank soal dilakukan tanpa bantuan komputer. Hal ini disebabkan karena dalam pengembangan bank soal yang besar, ada beberapa tahapan yang tidak mungkin dilakukan tanpa bantuan komputer.

2.1.5 Ujian

Ujian berasal dari kata uji. Menurut Kamus Besar Bahasa Indonesia uji berarti percobaan untuk mengetahui mutu sesuatu (ketulenan, kecakapan ketahanan, dsb). Ujian /uji·an/ berarti (1) Hasil menguji; hasil memeriksa; (2) Sesuatu yg dipakai untuk menguji mutu sesuatu (kepandaian, kemampuan, hasil belajar, dsb). Contoh: ujian kenaikan kelas diselenggarakan di sekolah masing-masing*;* (3) Cobaan. Contoh: musibah ini adalah ujian dari Tuhan.

Menurut Bernadette Tynan (2004;29-31) Ujian merupakan cara terbatas untuk mengukur kemampuan seseorang. Pelaksanaan ujian dimaksudkan untuk mengukur pengetahuan seseorang atau peserta didik. Menurut Tim Redaksi Kanisius (2010;63) ujian dapat dijadikan alat evaluasi untuk menilai berapa jauh pengetahuan yang telah dikuasai dan keteramplian yang telah diperoleh. Ujian dapat mendorong seseorang dalam kegiatan pembelajaran baik itu secara wawasan

ataupun pengetahuan lainnya. Ujian dapat diberikan secara kertas ataupun komputer.

Berdasarkan pengertian di atas, penulis menyimpulkan bahwa ujian merupakan salah satu alat evaluasi untuk mengukur kemampuan, pengetahuan, serta keterampilan yang telah diperoleh seseorang atau peserta didik.

2.1.6 Analisis Butir Soal

Menurut Nana Sudjana (1990;135), analisis butir soal atau analisis item adalah pengkajian pertanyaan-pertanyaan tes agar diperoleh perangkat pertanyaan yang memiliki kualitas yang memadai. Menurut Suharsimi Arikuno (1999;205), analisis soal adalah suatu prosedur yang sistematis, yang akan memberikan informasi-informasi yang sangat khusus terhadap butir tes yang kita susun. Butir dalam kata analisis menunjukkan bahwa tiap-tiap instrumen soal akan dianalisis.

Berdasarkan pengertian di atas, penulis menyimpulkan bahwa analisis butir soal adalah suatu kegiatan memperhatikan, mengamati, dan memecahkan masalah yaitu bagaimana membuat sebuah instumen soal yang dapat dikategorikan sebagai instrumen soal yang baik guna mengukur tingkat hasil belajar mahasiswa.

Menurut Suharsimi Arikuno (1999;207-221) dan Purwanto (2009;99-108), karateristik yang dapat dinilai dalam analisis butir soal terbagi menjadi tiga bagian, yaitu:

1. Taraf Kesukaran

Taraf kesukaran dapat didefinisikan sebagai proporsi siswa peserta tes yang menjawab benar (Crocker dan Algina dalam Purwanto, 2009;100). Definisi

tersebut dapat dinyatakan dengan sebuah rumus di mana taraf kesukaran adalah jumlah peserta yang menjawab benar dibagi dengan jumlah peserta.

$$P = \frac{B}{JS}$$

Keterangan:

P = Indeks kesukaran
B = Banyaknya siswa yang menjawab soal itu dengan benar
JS = Jumlah seluruh siswa peserta tes

Menurut ketentuan yang sering diikuti, indeks kesukaran sering diklasifikasikan sebagai berikut:

- Soal dengan P 1,00 sampai 0,30 adalah soal sukar
- Soal dengan P 0,30 sampai 0,70 adalah soal sedang
- Soal dengan P 0,70 sampai 1,00 adalah soal mudah

2. Daya Beda

Daya beda adalah kemampuan butir soal membedakan siswa yang mempunyai kemampuan tinggi dan rendah. Daya beda berhubungan dengan derajad kemampuan butir membedakan dengan baik perilaku pengambil tes dalam tes yang dikembangkan (Anastasi dan Urbina dalam Purwanto, 2009;101). Daya beda harus diusahakan positif dan setinggi mungkin. Nilai daya beda akan merentang antara – 1,00 hingga + 1,00. Daya beda positif dan tinggi berarti butir tersebut dapat membedakan dengan baik siswa kelompok atas dan bawah. Siswa kelompok atas adalah kelompok siswa yang memperoleh skor total yang tinggi sedangkan siswa kelompok bawah adalah kelompok siswa yang memperoleh skor total yang rendah. Rumus untuk menentukan daya beda adalah:

$$D = \frac{B_A}{J_A} - \frac{B_B}{J_B}$$

Keterangan:

D = Daya beda
B_A = Banyaknya peserta kelompok atas yang menjawab soal itu dengan benar
B_B = Banyaknya peserta kelompok bawah yang menjawab soal itu dengan benar
J_A = Banyaknya peserta kelompok atas
J_B = Banyaknya peserta kelompok bawah

Dalam menghitung daya beda terdapat beberapa kejadian khusus yang harus diperhatikan:

a. Apabila data di tengah sama, data yang sama dikeluarkan dari analisis.
b. Apabila jumlah siswa yang diuji coba lebih dari 100 orang, penentuan kelompok atas dan kelompok bawah dengan mengambil 27% siswa yang memperoleh skor tertinggi sebagai kelompok atas dan 27% siswa yang memperoleh siswa terendah sebagai kelompok bawah.

3. Efektivitas Pengecoh

Pengecoh (*distractor*) yang juga dikenal dengan istilah penyesat adalah pilihan jawaban yang bukan merupakan kunci jawaban. Pengecoh bukan sekedar pelengkap jawaban. Pengecoh diadakan untuk menyesatkan siswa agar tidak memilih kunci jawaban. Pengecoh menjadikan siswa yang kurang begitu memahami materi pelajaran untuk memilihnya. Agar dapat melakukan fungsinya untuk pengecoh, pengecoh harus dibuat semirip mungkin dengan kunci jawaban. Pengecoh dikatakan berfungsi efektif apabila paling tidak terdapat siswa yang terkecoh memilih.

2.1.7 Analisis Butir Soal Mata Kuliah Kriptografi

Analisis butir soal mata kuliah kriptografi berarti suatu kegiatan memperhatikan, mengamati, dan memecahkan masalah yaitu bagaimana membuat sebuah instumen soal yang dapat dikategorikan sebagai instrumen soal yang baik guna mengukur tingkat hasil belajar siswa pada sebuah bidang ilmu yang berhubungan tentang sebuah informasi/pesan yang disandikan dengan berbagai macam skema dan dapat terjamin aspek keamanan informasinya.

2.1.8 Analisis Butir Soal Mata Kuliah Kriptografi Sebagai Bank Soal

Analisis butir soal mata kuliah kriptografi sebagai bank soal berarti suatu kegiatan memperhatikan, mengamati, dan memecahkan masalah yaitu bagaimana membuat sebuah instumen soal yang dapat dikategorikan sebagai instrumen soal yang baik guna mengukur tingkat hasil belajar siswa pada sebuah bidang ilmu yang berhubungan tentang sebuah informasi/pesan yang disandikan dengan berbagai macam skema dan dapat terjamin aspek keamanan informasinya sebagai kumpulan dari butir-butir soal yang terorganisir mulai dari penyusunan dan penyimpanannya dengan menggunakan suatu informasi seperti nomor soal, indikator, maupun indeks soal.

2.1.9 Analisis Butir Soal Mata Kuliah Kriptografi Sebagai Bank Soal Ujian

Analisis butir soal mata kuliah kriptografi sebagai bank soal berarti suatu kegiatan memperhatikan, mengamati, dan memecahkan masalah yaitu bagaimana membuat sebuah instumen soal yang dapat dikategorikan sebagai instrumen soal yang baik guna mengukur tingkat hasil belajar siswa pada sebuah bidang ilmu yang berhubungan tentang sebuah informasi/pesan yang disandikan dengan

berbagai macam skema dan dapat terjamin aspek keamanan informasinya sebagai kumpulan dari butir-butir soal yang terorganisir mulai dari penyusunan dan penyimpanannya dengan menggunakan suatu informasi seperti nomor soal, indikator, maupun indeks soal yang dapat memudahkan penyusun soal untuk menyusun sebuah perangkat tes pada suatu ujian.

2.2 Kerangka Berpikir

Analisis butir soal dilakukan untuk mengadakan identifikasi soal-soal yang baik, kurang baik, dan buruk. Soal yang baik adalah soal yang valid dan memenuhi karateristik taraf kesukaran, daya beda, dan efektivitas pengecoh. Butir soal dibuat untuk mengukur tingkat pemahaman, pengetahuan, serta keterampilan yang telah diperoleh siswa. Pendidik dapat mengukur tingkat pemahaman, pengetahuan, serta keterampilan yang telah diperoleh siswa pada ranah kognitif, afektif, dan psikomotorik. Menurut taksonomi Bloom, ranah kognitif yang dapat diukur pada siswa memiliki enam tingkatan (C1 – C6). C1 memiliki tingkatan yang paling rendah sedangkan C6 memiliki tingkatan paling tinggi. Urutan pada tingkatan tersebut yaitu hafalan (C1), pemahaman (C2), penerapan (C3), analisis (C4), sintesis (C5), dan evaluasi (C5).

Penggunaan bank soal berfungsi untuk melakukan penyusunan serta penyimpanan kumpulan soal-soal yang diberi suatu informasi seperti nomor atau indeks yang digunakan untuk memudahkan penyusun soal melakukan pemaketan tes soal ujian. Penggunaan soal yang berbeda-beda atau paket soal berfungsi untuk menurunkan prosentase tingkat kecurangan siswa. Penggunaan dua paket soal belum optimal dalam menurunkan tingkat kecurangan siswa. Oleh karena itu, soal

dalam setiap indikator perlu diperbanyak. Setiap butir soal yang telah disusun pada setiap indikator harus diadakan uji validitas, taraf kesukaran, daya beda, dan efektivitas pengecoh. Pada akhirnya, penyusun soal dapat memilih soal yang berbeda dalam bank soal pada setiap indikator untuk membuat paket-paket soal. Dengan dilakukannya cara tersebut, pengambilan secara acak soal pada setiap indikator yang diujikan membuat kemungkinan paket soal yang banyak sehingga diharapkan dapat menurunkan tingkat kecurangan siswa.

BAB III

METODE PENELITIAN

3.1 Tempat dan Waktu Pelaksanaan

Penelitian akan dilaksanakan di Prodi Pendidikan Teknik Informatika dan Komputer Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Jakarta pada bulan Maret 2015 sampai bulan Juni 2015.

3.2 Metode Penelitian

Penelitian akan dilakukan dengan metode kuantitatif. Hasil dari penelitian menggunakan metode kuantitatif berupa analisis data dengan menggunakan perhitungan statistika. Metode kuantitatif yang digunakan pada penelitian ini adalah metode korelasi. Metode korelasi yang digunakan bertujuan untuk mengetahui sifat-sifat dari butir soal. Sifat atau kategori butir soal yang diteliti adalah taraf kesukaran, daya beda, efektivitas pengecoh dan validitas butir soal.

3.3 Sampel

Teknik pengambilan sampel yang digunakan peneliti adalah *random sampling* dengan metode *stratified random sampling* atau pengambilan acak berdasarkan lapisan. Instrumen diujikan kepada mahasiswa Prodi PTIK UNJ yang sedang mengambil mata kuliah kriptografi. Setiap instrumen yang diujikan dibagi ke dalam beberapa paket soal. Setiap paket soal yang diujikan memiliki jumlah sampel yang sama.

3.4 Peranan Penelitian dalam Analisis Butir Soal

Penelitian dilakukan untuk membuat bank soal mata kuliah kriptografi. Bank soal tersebut berisikan minimal lima butir soal setiap indikatornya. Penelitian berupa analisis butir soal yang meliputi taraf kesukaran pada butir soal, daya beda, efetivitas pengecoh atau distraktor, dan validitas butir soal. Hasil penelitian berupa bank soal mata kuliah kriptografi yang berisikan minimal lima butir soal setiap indikatornya. Butir soal pada bank soal mata kuliah kriptografi telah melewati uji taraf kesukaran butir soal, daya beda, efektivitas pengecoh atau distraktor, dan validitas butir soal.

3.5 Rancangan Penelitian

3.5.1 Strategi Penelitian

Strategi yang digunakan pada penelitian iniadalah:

1. Mencari studi pustaka yang relevan

   Studi pustaka yang digunakan berupa buku, buku elektronik, skripsi, jurnal ilmiah, dan situs yang berisi informasi penunjang yang berkaitan dengan penelitian yang dilakukan.

2. Penentuan metode penelitian

   Peneliti telah menentukan metode yang digunakan untuk penelitian yaitu metode kuantitatif. Pemilih memilih metode kuantitatif karena metode ini sesuai dengan masalah yang diteliti.

3. Penentuan responden

Responden yang digunakan pada penelitian ini adalah mahasiswa Prodi PTIK UNJ. Jumlah mahasiswa yang digunakan sebagai responden adalah 20 orang pada setiap butir soal yang diujian. Karateristik responden yang digunakan pada penelitian ini adalah responden harus mendapatkan materi tes yang diujicobakan serta kelompok responden harus memiliki tingkat pengetahuan mata kuliah kriptografi yang bervariasi.

4. Penyusunan indikator mata kuliah kriptografi

Pada tahap ini, penyusunan indikator mata kuliah kriptografi dilakukan berdasarkan Rencana Program Kegiatan Pembelajaran Semester (RPKPS) mata kuliah kriptografi yang dibuat oleh dosen pengampu mata kuliah kriptografi yaitu Bapak Prasetyo Wibowo Yunanto, M.Eng.

5. Penyusunan butir soal

Pada tahap ini, penyusunan butir soal mata kuliah kriptografi dilakukan berdasarkan indikator yang telah dibuat. Butir soal yang dibuat terdiri dari minimal 5 butir soal setiap indikatornya. Butir soal yang diujikan pada mahasiswa prodi PTIK UNJ yang sedng mengambil mata kuliah kriptografi dibentuk ke dalam beberapa paket soal. Butir soal yang telah dibuat telah dilakukan validasi oleh dosen pengampu mata kuliah kriptografi yaitu Bapak Prasetyo Wibowo Yunanto, M. Eng.

6. Uji taraf kesukaran

Uji taraf kesukaran dilakukan untuk mengetahui seberapa besar proporsi mahasiswa peserta tes menjawab soal dengan benar. Taraf kesukaran dapat

dinyatakan dengan sebuah rumus di mana taraf kesukaran adalah jumlah peserta yang menjawab benar dibagi dengan jumlah peserta. Nilai taraf kesukaran memiliki rentang antara 0,0 sampai dengan 1,0.

7. Uji daya beda

Uji daya beda dilakukan untuk mengetahui kemampuan butir soal membedakan siswa yang mempunyai kemampuan tinggi dan rendah. Daya beda harus diusahakan positif dan setinggi mungkin. Nilai daya beda akan merentang antara – 1,00 sampai dengan + 1,00. Daya beda positif dan tinggi berarti butir tersebut dapat membedakan dengan baik siswa kelompok atas dan bawah. Siswa kelompok atas adalah kelompok siswa yang memperoleh skor total yang tinggi sedangkan siswa kelompok bawah adalah kelompok siswa yang memperoleh skor total yang rendah.

8. Uji efektivitas pengecoh

Uji efektivitas pengecoh dilakukan pada setiap butir soal dengan cara melihat ada atau tidaknya mahasiswa yang terkecoh memilih jawaban yang salah. Pengecoh dikatakan berfungsi efektif apabila paling tidak terdapat mahasiswa yang terkecoh memilih.

9. Analisis hasil uji taraf kesukaran

Hasil dari uji taraf kesukaran dapat dikategorikan sebagai berikut:

- Soal dengan P 1,00 sampai 0,30 adalah soal sukar
- Soal dengan P 0,30 sampai 0,70 adalah soal sedang
- Soal dengan P 0,70 sampai 1,00 adalah soal mudah

P merupakan hasil dari uji taraf kesukaran.

10. Analisis hasil uji daya beda

Hasil dari uji daya beda harus diusahakan positif dan setinggi mungkin. Nilai daya beda akan merentang antara – 1,00 hingga + 1,00. Daya beda positif dan tinggi berarti butir tersebut dapat membedakan dengan baik siswa kelompok atas dan bawah. Siswa kelompok atas adalah kelompok siswa yang memperoleh skor total yang tinggi sedangkan siswa kelompok bawah adalah kelompok siswa yang memperoleh skor total yang rendah.

11. Analisis hasil uji efektivitas pengecoh

Hasil uji dari efektivitas pengecoh terbagi menjadi dua kategori yaitu efektif dan tidak efektif. Butir soal dikatakan efektif apabila paling tidak terdapat mahasiswa yang memilih jawaban pengecoh. Butir soal dikatakan tidak efektif apabila tidak terdapat mahasiswa yang memilih jawaban pengecoh.

12. Uji validitas

Uji validitas dilakukan untuk mengetahui apakah butir soal sesuai dengan kriterium. Sebuah tes dikatakan memiliki validitas jika hasilnya sesuai dengan kriterium, dalam arti memiliki kesejajaran antara hasil tes tersebut dengan kriterium. Pada penelitian ini, teknik yang digunakan untuk mengetahui kesejajaran adalah teknik korelasi *product moment* yang dikemukakan oleh Pearson.

13. Analisis hasil uji validitas

Hasil uji validitas terbagi menjadi dua kategori yaitu valid dan tidak valid. Sebuah soal dikatakan valid apabila nilai r hitung > r tabel. Nilai r tabel dalam penelitian ini adalah 0,444. Nilai ini didapat dari r tabel dengan taraf signifikan

5% dan derajat kebebasannya 18. Niai 18 didapat dari jumlah sampel dikurang 2 yaitu 20 dikurang 2. Sebuah soal dikatakan tidak valid apabila nilai r hitung < r tabel.

3.5.2 Implementasi Penelitian

Pada tahap ini, setiap butir soal yang telah melewati uji taraf kesukaran, daya beda, efektivitas pengecoh atau distraktor, serta validitas butir soal akan disimpan dan disusun menjadi sebuah bank soal mata kuliah kriptografi yang dapat digunakan sebagai bahan penyusun soal ujian pada Prodi PTIK UNJ.

3.5.3 Uji Coba dan Evaluasi pada Butir Soal

Tahap uji coba butir soal dilakukan dengan uji taraf kesukaran, uji daya beda, uji efektivas pengecoh, dan validitas dengan menggunakan sampel mahasiswa Prodi PTIK UNJ yang sedang mengambil mata kuliah kriptografi. Evaluasi butir soal dilakukan dengan cara melihat apakah hasil uji taraf kesukaran, daya beda, efektivitas pengecoh, dan validitas termasuk ke dalam butir soal yang baik.

3.6 Instrumen Penelitian

Instrumen penelitian yang digunakan dalam penelitian ini adalah tes. Tes diberikan kepada mahasiswa PTIK UNJ. Tes yang diberikan berupa tes objektif, yaitu tes pilihan ganda (*multiple choice test*). Sebelum butir soal diujikan kepada mahasiswa PTIK UNJ, butir soal telah divalidasi oleh dosen pengampu mata kuliah kriptografi.

3.7 Teknik Analisis Data

3.7.1 Pengujian Taraf Kesukaran Butir Soal

Pengujian taraf kesukaran dilakukan pada setiap butir soal dengan rumus:

$$P = \frac{B}{JS}$$

Keterangan:

P = Indeks kesukaran
B = Banyaknya siswa yang menjawab soal itu dengan benar
JS = Jumlah seluruh siswa peserta tes

Hasil dari uji taraf kesukaran dapat dikategorikan sebagai berikut:

- Soal dengan P 1,00 sampai 0,30 adalah soal sukar
- Soal dengan P 0,30 sampai 0,70 adalah soal sedang
- Soal dengan P 0,70 sampai 1,00 adalah soal mudah

P merupakan hasil dari uji taraf kesukaran.

3.7.2 Pengujian Daya Beda Butir Soal

Pengujian daya beda dilakukan pada setiap butir soal dengan rumus:

$$D = \frac{B_A}{J_A} - \frac{B_B}{J_B}$$

Keterangan:

D = Daya beda
B_A = Banyaknya peserta kelompok atas yang menjawab soal itu dengan benar
B_B = Banyaknya peserta kelompok bawah yang menjawab soal itu dengan benar
J_A = Banyaknya peserta kelompok atas
J_B = Banyaknya peserta kelompok bawah

3.7.3 Pengujian Efektivitas Pengecoh Butir Soal

Pengujian efektivitas pengecoh dilakukan pada setiap butir soal dengan cara melihat ada atau tidaknya mahasiswa yang terkecoh memilih jawaban yang salah. Pengecoh dikatakan berfungsi efektif apabila paling tidak terdapat mahasiswa yang terkecoh memilih.

3.7.4 Pengujian Validitas Butir Soal

Pengujian validitas dilakukan pada setiap butir soal dengan rumus korelasi *product moment* dengan angka kasar, yaitu:

$$r_{xy} = \frac{N\Sigma XY - (\Sigma X)(\Sigma Y)}{\sqrt{\{N\Sigma X^2 - (\Sigma X)^2\}\{N\Sigma Y^2 - (\Sigma Y)^2\}}}$$

Keterangan:

N = Jumlah sampel mahasiswa yang diuji
X = Skor item soal yang duji
Y = Skor total
ΣX = Jumlah mahasiswa yang menjawab item soal yang diuji dengan benar
ΣY = Jumlah skor total
ΣXY = Jumlah skor item soal yang diuji dikalikan dengan skor total
ΣX^2 = Jumlah skor item soal yang diuji dikuadratkan
ΣY^2 = Jumlah skor total dikuadratkan

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

Hasil penelitian adalah bank soal mata kuliah kriptografi yang telah dilakukan analisis butir soal meliputi uji taraf kesukaran, daya beda, efektivitas pengecoh, dan validitas butir soal. Berikut merupakan standar kompetensi, kompetensi dasar, dan indikator mata kuliah kriptografi, hasil analisis butir soal mata kuliah tahap I, hasil analisis butir soal mata kuliah kriptografi tahap II, hasil analisis butir soal mata kuliah kriptografi tahap III, serta hasil analisis butir soal untuk bank soal mata kuliah kriptografi.

4.1.1 Standar Kompetensi, Kompetensi Dasar, dan Indikator Mata Kuliah Kriptografi

Standar kompetensi, kompetensi dasar, dan indikator mata kuliah kriptografi di bawah ini dibuat oleh peneliti berdasarkan Rencana Program Pembelajaran Semester (RPKPS) yang dibuat oleh dosen pengampu mata kuliah kriptografi yaitu Bapak Prasetyo Wibowo Yunanto, M.Eng. Standar kompetensi dibuat berdasarkan topik yang terdapat pada RPKSP, sedangkan kompetensi dasar dibuat berdasarkan substansi yang terdapat pada RPKPS. Standar kompetensi, kompetensi dasar, dan indikator mata kuliah kriptografi yang dibuat oleh peneliti ditunjukkan pada tabel 4.1 di bawah ini.

Tabel 4.1 SK, KD, dan Indikator Mata Kuliah Kriptografi

Nomor	Topik / Standar Kompetensi	Substansi / Kompetensi Dasar	Indikator	Taksonomi Bloom
1.	Pengantar kriptografi	1. Pengertian dan terminologi 2. Tujuan kriptografi 3. Sejarah Kriptografi 4. Kriptanalisis 5. Kriptografi kunci simetris 6. Kriptografi kunci asimetris	Mahasiswa dapat mendeskripsikan terminologi kriptografi	C1
			Mahasiswa dapat mengidentifikasikan tujuan kriptografi	C1
			Mahasiswa dapat menyebutkan sejarah kriptografi	C1
			Mahasiswa dapat mendefinisikan pengertian dari kriptanalisis	C1
			Mahasiswa dapat mengidentifikasikan perbedaan antara kriptografi kunci simetris dengan kriptografi kunci asimetris	C1
2.	Serangan terhadap kriptografi	1. Keamanan algoritma kriptografi 2. Jenis-jenis serangan 3. Kompleksitas serangan	Mahasiswa dapat menjelaskan fungsi keamanan algoritma kriptografi	C2
			Mahasiswa dapat menyebutkan jenis-jenis serangan terhadap kriptografi	C1
			Mahasiswa dapat mengidentifikasikan kompleksitas serangan terhadap kriptografi	C1

Nomor	Topik / Standar Kompetensi	Substansi / Kompetensi Dasar	Indikator	Taksonomi Bloom
3.	Landasan matematika pada kriptografi	1. Fungsi 2. Permutasi dan kombinasi 3. Teori peluang 4. Teori bilangan	Mahasiswa dapat menerapkan penggunaan fungsi matematika pada kriptografi	C3
			Mahasiswa dapat menghitung fungsi permutasi	C3
			Mahasiswa dapat meneghitung fungsi kombinasi	C3
			Mahasiswa dapat menerapkan teori peluang	C3
			Mahasiswa dapat menerapkan teori bilangan	C3
4.	Algoritma kriptografi klasik	1. Algoritma *cipher* substitusi 2. Algoritma *cipher* transposisi 3. Algoritma *affine cipher* 4. Algoritma *vigenere* 5. Algoritma *playfair* 6. Algoritma *one-time pad*	Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi	C3
			Mahasiswa dapat mengaplikasikan algoritma *cipher* transposisi	C3
			Mahasiswa dapat mengaplikasikan algoritma *affine cipher*	C3
			Mahasiswa dapat mengaplikasikan algoritma *vigenere*	C3
			Mahasiswa dapat mengaplikasikan algoritma *playfair*	C3
			Mahasiswa dapat mengaplikasikan algoritma *one-time pad*	C3

Nomor	Topik / Standar Kompetensi	Substansi / Kompetensi Dasar	Indikator	Taksonomi Bloom
5.	Algoritma kriptografi modern	1. Rangkaian bit dan operasinya 2. Algoritma enkripsi dengan XOR sederhana 3. Pembangkitan kunci 4. DES dan AES 5. RC4 dan A5 6. *Cipher* aliran dan serangan terhadap *cipher* aliran 7. *Ciphe*r blok 8. Prinsip perancangan *cipher* blok	Mahasiswa dapat menerapkan rangkaian bit dan operasinya	C3
			Mahasiswa dapat menerapkan algoritma enkripsi dengan XOR sederhana	C3
			Mahasiswa dapat mengoperasikan pembangkitan kunci	C3
			Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	C1
			Mahasiswa dapat mengidentifikasikan perbedaan antara RC4 dengan A5	C1
			Mahasiswa dapat menjelaskan *cipher* aliran	C2
			Mahasiswa dapat mengidentifikasikan serangan terhadap *cipher* aliran	C1
			Mahasiswa dapat mengidentifikasikan *cipher* blok	C1
			Mahasiswa dapat mendeskripsikan prinsip perancangan *cipher* blok	C1
6.	Kriptografi kunci publik		Mahasiswa dapat menjelaskan konsep kriptografi kunci publik	C2
			Mahasiswa dapat mengidentifikasikan algoritma RSA	C1

Nomor	Topik / Standar Kompetensi	Substansi / Kompetensi Dasar	Indikator	Taksonomi Bloom
		1. Konsep kriptografi kunci publik 2. Konsep kriptografi kunci publik 3. Algoritma RSA 4. Algoritma *ElGamal* 5. Algoritma *rabin* 6. Pembangkit bilangan prima 7. Pembangkit bilangan acak semu	Mahasiswa dapat menjelaskan algoritma *ElGamal*	C2
			Mahasiswa dapat mengidentifikasikan algoritma *rabin*	C1
			Mahasiswa dapat menjelaskan pembangkit bilangan prima	C2
			Mahasiswa dapat menjelaskan pembangkit bilangan acak semu	C2
7.	Fungsi *hash* dan tanda tangan digital	1. Fungsi *hash* satu arah 2. Algoritma MD5 3. Algoritma MAC 4. Konsep tanda tangan digital 5. Protokol kriptografi	Mahasiswa dapat mengidentifikasikan fungsi *hash* satu arah	C1
			Mahasiswa dapat menyebutkan algoritma MD5	C1
			Mahasiswa dapat mengidentifikasikan algoritma MAC	C1
			Mahasiswa dapat mengidentifikasikan konsep tanda tangan digital	C1
			Mahasiswa dapat mengidentifikasikan protokol kriptografi	C1
8.	Kriptografi dalam kehidupan sehari-hari	1. Pemanfaatan kriptografi dalam kehidupan sehari-hari seperti kartu cerdas, ATM, *e-commerce*, dll	Mahasiswa dapat menganalisis penggunaan kriptografi dalam kehidupan sehari-hari	C4

4.1.2 Hasil Analisis Butir Soal Mata Kuliah Kriptografi Tahap I

Analisis butir soal mata kuliah kriptografi tahap I dilakukan pada tanggal 22 April 2015. Butir soal yang dibuat dibagi menjadi 4 paket soal yaitu paket soal A, paket soal B, paket soal C, dan paket soal D. Setiap paket soal yang diujikan berisi 30 soal pilihan ganda. Setiap paket soal diujikan kepada 20 mahasiswa Prodi PTIK UNJ yang sedang mengambil mata kuliah kriptografi. Materi yang diujikan mulai dari terminologi kriptografi sampai dengan perbedaan DES dan AES. Berikut ini merupakan hasil analisis butir soal mata kuliah kriptografi untuk paket soal A, paket soal B, paket soal C, dan paket soal D. Kisi-kisi instrumen untuk pengujian tahap I akan dilampirkan pada Lampiran 1.

1. Paket Soal A

Validitas butir paket soal A oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 2. Butir soal pada paket soal A akan dilampirkan pada Lampiran 3. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 4. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal A akan ditunjukkan oleh Tabel 4.2 di bawah ini. Kata TE pada hasil analisis efektivitas pengecoh berarti Tidak Efektif (TE). Huruf E pada hasil analisis efektivitas pengecoh berarti Efektif (E). Kata KJ pada hasil analisis efektivitas pengecoh berarti Kunci Jawaban (KJ) dari nomor soal tersebut.

Tabel 4.2 Hasil Analisis Butir Soal untuk Paket Soal A

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Mudah	0,4	E	KJ	TE	E	TE	0,590	Valid
2	Mudah	0,1	E	KJ	E	TE	TE	0,171	Tidak Valid
3	Sedang	0,1	E	KJ	E	E	TE	0,089	Tidak Valid
4	Sedang	0,4	E	E	KJ	E	TE	0,622	Valid
5	Sedang	0,4	E	TE	KJ	E	E	0,530	Valid
6	Mudah	0,4	TE	E	TE	KJ	E	0,574	Valid
7	Sedang	0	E	E	TE	E	KJ	0,245	Tidak Valid
8	Sukar	-0,1	KJ	E	E	E	E	0,174	Tidak Valid
9	Sedang	0,4	E	E	KJ	E	E	0,487	Valid
10	Sedang	0,5	TE	E	TE	KJ	E	0,517	Valid
11	Sedang	0,5	KJ	E	E	TE	TE	0,517	Valid
12	Sedang	0	E	KJ	E	E	TE	0,045	Tidak Valid
13	Mudah	0,6	KJ	E	E	E	E	0,536	Valid
14	Sedang	0,3	E	E	E	E	KJ	0,221	Tidak Valid
15	Mudah	0,6	TE	E	KJ	E	E	0,455	Valid
16	Sukar	0,3	E	E	E	KJ	E	0,520	Valid
17	Sedang	0	TE	KJ	E	E	E	-0,111	Tidak Valid
18	Mudah	0	KJ	TE	TE	TE	TE	∞	Tidak Valid
19	Mudah	0	TE	TE	TE	TE	KJ	∞	Tidak Valid
20	Mudah	0	TE	TE	KJ	TE	TE	∞	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
21	Sedang	0	E	E	E	KJ	E	0,081	Tidak Valid
22	Sedang	0,1	KJ	E	E	E	TE	0,145	Tidak Valid
23	Sedang	0,2	E	KJ	E	E	E	0,030	Tidak Valid
24	Sedang	0,7	E	E	KJ	E	E	0,624	Valid
25	Sedang	0,2	E	TE	E	E	KJ	0,599	Valid
26	Sedang	0,3	E	E	TE	KJ	E	0,549	Valid
27	Mudah	0,1	E	E	KJ	TE	E	-0,071	Tidak Valid
28	Mudah	0	E	TE	E	KJ	E	-0,003	Tidak Valid
29	Sedang	-0,1	KJ	E	E	E	E	0,089	Tidak Valid
30	Sedang	0,3	TE	E	KJ	TE	E	0,517	Valid

2. Paket Soal B

Validitas butir paket soal B oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 5. Butir soal pada paket soal B akan dilampirkan pada Lampiran 6. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 7. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal B akan ditunjukkan oleh Tabel 4.3 di bawah ini.

Tabel 4.3 Hasil Analisis Butir Soal untuk Paket Soal B

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Mudah	0,1	TE	TE	KJ	E	TE	0,216	Tidak Valid
2	Mudah	0,3	E	TE	TE	E	KJ	0,487	Valid
3	Mudah	0,4	E	KJ	E	E	E	0,499	Valid
4	Sedang	0,7	KJ	E	TE	TE	E	0,661	Valid
5	Mudah	0,1	TE	E	TE	KJ	TE	0,096	Tidak Valid
6	Sukar	0,4	E	E	KJ	TE	E	0,601	Valid
7	Sukar	0,2	E	E	E	KJ	E	0,149	Tidak Valid
8	Sukar	0,4	E	E	KJ	E	E	0,627	Valid
9	Sukar	0,3	E	E	E	E	KJ	0,495	Valid
10	Sedang	0,4	KJ	E	E	E	E	0,521	Valid
11	Sedang	-0,1	TE	KJ	E	E	TE	-0,018	Tidak Valid
12	Sukar	0,2	TE	TE	E	KJ	E	0,279	Tidak Valid
13	Mudah	0,4	E	E	KJ	E	E	0,579	Valid
14	Sedang	0,6	E	KJ	E	TE	E	0,595	Valid
15	Sedang	0,4	KJ	E	E	E	E	0,505	Valid
16	Sedang	-0,1	E	E	E	TE	KJ	-0,063	Tidak Valid
17	Sedang	0,1	E	E	E	KJ	E	0,229	Tidak Valid
18	Mudah	-0,1	TE	TE	KJ	TE	E	-0,276	Tidak Valid
19	Mudah	0	KJ	E	TE	TE	TE	0,029	Tidak Valid
20	Mudah	0	TE	KJ	TE	TE	TE	∞	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
21	Mudah	0,6	KJ	E	E	E	E	0,501	Valid
22	Sedang	0,6	E	E	KJ	E	E	0,468	Valid
23	Sedang	0,4	E	E	E	E	KJ	0,521	Valid
24	Sedang	0,7	TE	E	E	KJ	E	0,630	Valid
25	Sedang	0,4	TE	KJ	E	E	E	0,482	Valid
26	Sedang	0,6	KJ	E	E	E	E	0,483	Valid
27	Sedang	0,1	KJ	E	TE	E	TE	0,108	Tidak Valid
28	Mudah	0,3	KJ	TE	E	TE	E	0,517	Valid
29	Sukar	0,3	E	KJ	E	E	E	0,475	Valid
30	Mudah	0,1	E	E	TE	KJ	E	0,198	Tidak Valid

3. Paket Soal C

Validitas butir paket soal C oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 8. Butir soal pada paket soal C akan dilampirkan pada Lampiran 9. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 10. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal C akan ditunjukkan oleh Tabel 4.4 di bawah ini.

Tabel 4.4 Hasil Analisis Butir Soal untuk Paket Soal C

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Mudah	0,3	TE	TE	E	KJ	TE	0,225	Tidak Valid
2	Mudah	-0,1	KJ	E	E	TE	TE	0,259	Tidak Valid
3	Sedang	-0,2	E	E	KJ	E	TE	-0,183	Tidak Valid
4	Sedang	0,5	E	E	E	E	KJ	0,497	Valid
5	Sedang	-0,1	E	E	E	KJ	E	-0,075	Tidak Valid
6	Sukar	0,3	E	TE	KJ	E	TE	0,524	Valid
7	Sedang	0	KJ	E	E	E	E	-0,033	Tidak Valid
8	Sedang	0,3	E	KJ	E	E	E	0,527	Valid
9	Sedang	0,6	TE	KJ	E	E	TE	0,550	Valid
10	Sedang	0,7	E	E	E	KJ	E	0,738	Valid
11	Sedang	0,1	E	E	KJ	E	E	0,173	Tidak Valid
12	Mudah	0,3	KJ	E	E	E	TE	0,467	Valid
13	Mudah	0,1	TE	E	E	E	KJ	0,190	Tidak Valid
14	Mudah	0	E	E	E	KJ	TE	0,196	Tidak Valid
15	Sedang	0,1	E	KJ	E	TE	E	0,196	Tidak Valid
16	Sedang	0,2	E	E	KJ	E	E	0,306	Tidak Valid
17	Sedang	0,2	KJ	E	TE	E	TE	0,122	Tidak Valid
18	Mudah	-0,1	TE	E	TE	KJ	E	-0,378	Tidak Valid
19	Mudah	-0,1	E	TE	E	E	KJ	-0,147	Tidak Valid
20	Mudah	0	TE	TE	KJ	TE	TE	∞	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
21	Sukar	0,2	E	KJ	E	E	E	0,524	Valid
22	Sedang	0,3	KJ	E	E	E	TE	0,487	Valid
23	Sedang	0,6	E	TE	E	KJ	E	0,642	Valid
24	Sukar	0	E	E	E	E	KJ	0,150	Tidak Valid
25	Sedang	0	E	E	KJ	TE	E	-0,060	Tidak Valid
26	Sedang	0,4	E	KJ	E	E	TE	0,210	Tidak Valid
27	Mudah	0,4	KJ	E	E	E	TE	0,487	Valid
28	Mudah	0,4	E	E	KJ	E	E	0,214	Tidak Valid
29	Sukar	0,2	E	E	E	KJ	E	0,499	Valid
30	Sedang	0	E	E	E	E	KJ	0,000	Tidak Valid

4. Paket Soal D

Validitas butir paket soal D oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 11. Butir soal pada paket soal D akan dilampirkan pada Lampiran 12. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 13. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal D akan ditunjukkan oleh Tabel 4.5 di bawah ini.

Tabel 4.5 Hasil Analisis Butir Soal untuk Paket Soal D

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Mudah	0,2	KJ	E	TE	TE	E	0,464	Valid
2	Mudah	0,2	TE	TE	E	E	KJ	0,464	Valid
3	Sedang	0,6	E	E	E	KJ	E	0,683	Valid
4	Sedang	0,5	KJ	TE	TE	E	E	0,556	Valid
5	Sukar	0,1	E	TE	KJ	E	E	0,115	Tidak Valid
6	Sedang	0,5	E	KJ	E	E	E	0,481	Valid
7	Sedang	0,3	E	E	KJ	E	E	0,237	Tidak Valid
8	Sedang	0	E	E	TE	KJ	E	0,084	Tidak Valid
9	Sedang	-0,3	KJ	E	E	E	E	-0,269	Tidak Valid
10	Sedang	0,4	E	E	E	E	KJ	0,229	Tidak Valid
11	Sedang	0,3	E	TE	KJ	E	E	0,481	Valid
12	Sedang	-0,1	E	E	KJ	E	E	-0,163	Tidak Valid
13	Sedang	0,6	E	KJ	E	E	E	0,655	Valid
14	Sedang	0,5	E	E	TE	KJ	E	0,507	Valid
15	Mudah	0,2	KJ	E	TE	E	E	0,095	Tidak Valid
16	Sedang	0,6	E	E	E	E	KJ	0,516	Valid
17	Sedang	0,4	E	E	KJ	E	TE	0,535	Valid
18	Mudah	-0,2	TE	KJ	TE	TE	E	-0,355	Tidak Valid
19	Mudah	-0,1	E	TE	E	KJ	TE	-0,136	Tidak Valid
20	Mudah	0	KJ	TE	TE	TE	TE	∞	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
21	Mudah	0,4	E	E	KJ	TE	E	0,503	Valid
22	Sedang	0,4	E	E	TE	E	KJ	0,516	Valid
23	Sedang	0,4	E	KJ	E	E	E	0,468	Valid
24	Sedang	0,2	KJ	E	E	TE	TE	0,176	Tidak Valid
25	Sedang	0,6	E	E	E	KJ	E	0,655	Valid
26	Sedang	0,4	TE	E	KJ	E	E	0,503	Valid
27	Sedang	0,2	E	E	E	E	KJ	0,277	Tidak Valid
28	Mudah	0,3	E	KJ	TE	E	E	0,454	Valid
29	Sedang	-0,1	E	E	KJ	E	E	0,225	Tidak Valid
30	Sedang	0	E	E	E	KJ	TE	0,129	Tidak Valid

4.1.3 Hasil Analisis Butir Soal Mata Kuliah Kriptografi Tahap II

Analisis butir soal mata kuliah kriptografi tahap II dilakukan pada tanggal 20 Mei 2015. Butir soal yang dibuat dibagi menjadi 4 paket soal yaitu paket soal E, paket soal F, paket soal G, dan paket soal H. Setiap paket soal yang diujikan berisi 45 soal pilihan ganda. Setiap paket soal diujikan kepada 20 mahasiswa Prodi PTIK UNJ yang sedang mengambil mata kuliah kriptografi. Materi yang diujikan mulai dari terminologi kriptografi sampai dengan algoritma *Rabin*. Berikut ini merupakan hasil analisis butir soal mata kuliah kriptografi untuk paket soal E, paket soal F, paket soal G, dan paket soal H. Kisi-kisi instrumen untuk pengujian tahap II akan dilampirkan pada Lampiran 14.

1. Paket Soal E

Validitas butir paket soal E oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 15. Butir soal pada paket soal E akan dilampirkan pada Lampiran 16. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 17. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal E akan ditunjukkan oleh Tabel 4.6 di bawah ini.

Tabel 4.6 Hasil Analisis Butir Soal untuk Paket Soal E

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Sedang	0,4	E	E	KJ	E	E	0,563	Valid
2	Mudah	0,4	E	TE	E	TE	KJ	0,482	Valid
3	Sedang	0,5	E	KJ	E	E	TE	0,233	Tidak Valid
4	Sedang	0,4	E	E	KJ	E	E	0,244	Tidak Valid
5	Sukar	0,4	KJ	E	E	E	TE	0,447	Valid
6	Mudah	0,3	TE	E	TE	KJ	TE	0,498	Valid
7	Mudah	-0,1	E	KJ	TE	TE	E	-0,258	Tidak Valid
8	Sedang	0,5	E	E	E	E	KJ	0,549	Valid
9	Sedang	-0,1	E	E	KJ	E	E	-0,144	Tidak Valid
10	Sedang	0,1	E	E	E	KJ	E	0,209	Tidak Valid
11	Sedang	0,5	KJ	E	TE	E	E	0,491	Valid
12	Sedang	0,4	E	TE	KJ	E	TE	0,517	Valid
13	Sedang	0,7	E	KJ	E	E	TE	0,689	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
14	Mudah	0,4	TE	TE	E	E	KJ	0,540	Valid
15	Sedang	0,6	TE	E	KJ	E	E	0,598	Valid
16	Sedang	0,5	TE	E	E	KJ	E	0,514	Valid
17	Sukar	0,3	KJ	E	TE	E	E	0,500	Valid
18	Sukar	0,5	E	E	KJ	E	E	0,620	Valid
19	Mudah	0,1	TE	KJ	E	E	TE	0,466	Valid
20	Mudah	0	TE	TE	E	E	KJ	0,473	Valid
21	Mudah	0,2	TE	E	E	KJ	TE	0,447	Valid
22	Mudah	0	KJ	TE	TE	E	E	-0,075	Tidak Valid
23	Sedang	0,4	E	TE	KJ	TE	TE	0,517	Valid
24	Sedang	-0,3	E	E	E	E	KJ	-0,205	Tidak Valid
25	Sukar	0	E	KJ	E	E	E	0,084	Tidak Valid
26	Sukar	0,3	KJ	E	E	E	E	0,526	Valid
27	Sukar	0,4	KJ	E	E	E	E	0,462	Valid
28	Sedang	0,2	E	E	E	KJ	TE	0,296	Tidak Valid
29	Mudah	0,3	E	KJ	E	TE	E	0,546	Valid
30	Mudah	0,2	E	E	KJ	TE	E	0,587	Valid
31	Mudah	0,3	KJ	E	TE	TE	TE	0,498	Valid
32	Mudah	0,4	TE	E	E	TE	KJ	0,523	Valid
33	Sedang	0,3	TE	E	TE	KJ	E	0,502	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
34	Sukar	0,4	KJ	E	E	E	E	0,491	Valid
35	Sedang	0,5	E	E	E	E	KJ	0,514	Valid
36	Sedang	0,6	E	E	KJ	TE	TE	0,576	Valid
37	Mudah	0,3	E	KJ	E	E	TE	0,531	Valid
38	Sedang	0,5	KJ	E	E	E	E	0,525	Valid
39	Sedang	0,3	E	E	E	KJ	E	0,449	Valid
40	Sedang	0,3	TE	E	E	E	KJ	0,464	Valid
41	Sedang	0,3	E	E	KJ	E	E	0,595	Valid
42	Sedang	0,6	TE	KJ	TE	TE	E	0,491	Valid
43	Sukar	0,3	KJ	E	E	E	E	0,526	Valid
44	Sedang	0,4	TE	E	E	KJ	E	0,517	Valid
45	Mudah	0,5	E	KJ	E	E	E	0,493	Valid

2. Paket Soal F

Validitas butir paket soal F oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 18. Butir soal pada paket soal F akan dilampirkan pada Lampiran 19. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 20. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal G akan ditunjukkan oleh Tabel 4.7 di bawah ini.

Tabel 4.7 Hasil Analisis Butir Soal untuk Paket Soal F

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Sedang	0,4	KJ	TE	TE	E	E	0,531	Valid
2	Sedang	0,4	E	E	E	KJ	E	0,491	Valid
3	Sedang	0,4	E	E	KJ	TE	E	0,483	Valid
4	Sedang	0,5	TE	KJ	E	E	E	0,540	Valid
5	Sukar	0,3	KJ	E	TE	E	E	0,456	Valid
6	Sedang	0,5	E	E	KJ	TE	E	0,513	Valid
7	Sukar	0,3	E	E	E	E	KJ	0,566	Valid
8	Sukar	0	E	E	E	E	KJ	-0,124	Tidak Valid
9	Sedang	0,2	E	E	E	KJ	E	0,098	Tidak Valid
10	Sedang	0,2	E	KJ	E	E	E	0,469	Valid
11	Sedang	0,2	KJ	E	E	TE	E	0,202	Tidak Valid
12	Sedang	0,5	E	E	E	KJ	TE	0,523	Valid
13	Mudah	-0,1	TE	TE	KJ	E	TE	0,070	Tidak Valid
14	Mudah	0,3	E	E	E	KJ	E	0,479	Valid
15	Mudah	0,2	KJ	E	E	E	TE	0,500	Valid
16	Mudah	0	TE	KJ	E	E	TE	0,276	Tidak Valid
17	Sedang	0,3	E	E	KJ	E	E	0,528	Valid
18	Sukar	0,1	E	E	E	E	KJ	0,109	Tidak Valid
19	Mudah	0,5	E	E	E	KJ	TE	0,479	Valid
20	Sedang	0,4	KJ	E	E	E	TE	0,464	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
21	Mudah	-0,1	E	TE	KJ	E	E	-0,182	Tidak Valid
22	Mudah	0,2	TE	KJ	E	E	E	0,202	Tidak Valid
23	Mudah	0,2	E	TE	TE	E	KJ	0,385	Tidak Valid
24	Mudah	0	KJ	E	TE	E	E	-0,124	Tidak Valid
25	Sedang	0,3	TE	E	E	KJ	E	0,526	Valid
26	Sedang	0,5	E	KJ	E	TE	E	0,513	Valid
27	Sedang	0,4	E	E	KJ	E	E	0,483	Valid
28	Sukar	0,5	KJ	E	E	E	TE	0,532	Valid
29	Mudah	-0,1	TE	TE	TE	E	KJ	-0,036	Tidak Valid
30	Mudah	0	TE	E	E	KJ	E	0,137	Tidak Valid
31	Mudah	0,1	TE	KJ	E	E	E	0,147	Tidak Valid
32	Mudah	-0,1	KJ	E	E	E	TE	0,001	Tidak Valid
33	Sedang	0,4	E	E	TE	E	KJ	0,469	Valid
34	Sedang	0,2	E	E	KJ	E	E	0,497	Valid
35	Sedang	0,4	KJ	E	TE	TE	E	0,529	Valid
36	Sedang	0,3	E	E	E	KJ	E	0,446	Valid
37	Sukar	0,4	E	E	TE	E	KJ	0,451	Valid
38	Sukar	0,5	E	E	KJ	TE	E	0,486	Valid
39	Sedang	0,3	E	KJ	E	E	E	0,475	Valid
40	Sedang	0,4	TE	E	KJ	E	E	0,540	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
41	Sedang	0,6	KJ	E	E	E	E	0,569	Valid
42	Sukar	0,3	TE	E	E	KJ	TE	0,501	Valid
43	Sedang	0,5	E	E	E	E	KJ	0,567	Valid
44	Sedang	0,3	E	KJ	E	E	E	0,527	Valid
45	Sukar	0,2	E	E	KJ	E	E	0,500	Valid

3. Paket Soal G

Validitas butir paket soal G oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 21. Butir soal pada paket soal G akan dilampirkan pada Lampiran 22. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 23. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal G akan ditunjukkan oleh Tabel 4.8 di bawah ini.

Tabel 4.8 Hasil Analisis Butir Soal untuk Paket Soal G

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Mudah	0	E	E	TE	KJ	TE	-0,160	Tidak Valid
2	Mudah	0,2	KJ	E	TE	TE	E	0,447	Valid
3	Sedang	-0,1	E	E	E	TE	KJ	0,085	Tidak Valid
4	Sukar	0,3	E	TE	KJ	E	E	0,545	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
5	Mudah	0,1	TE	KJ	TE	TE	E	0,169	Tidak Valid
6	Sedang	0,5	TE	TE	E	KJ	E	0,567	Valid
7	Sukar	0,1	KJ	E	E	E	E	0,048	Tidak Valid
8	Sedang	0,3	E	E	KJ	E	E	0,477	Valid
9	Sedang	0	TE	E	TE	TE	KJ	-0,040	Tidak Valid
10	Sedang	0,5	E	E	E	KJ	E	0,543	Valid
11	Sedang	0	E	E	E	E	KJ	-0,071	Tidak Valid
12	Sedang	0,1	E	KJ	TE	E	TE	0,251	Tidak Valid
13	Sedang	0,6	E	E	E	KJ	E	0,563	Valid
14	Sedang	0,5	KJ	TE	E	E	TE	0,602	Valid
15	Mudah	0,3	TE	E	KJ	E	E	0,494	Valid
16	Mudah	0,4	TE	E	E	E	KJ	0,517	Valid
17	Sedang	0,3	E	E	E	E	KJ	0,498	Valid
18	Sedang	0,7	E	KJ	E	E	E	0,567	Valid
19	Sedang	0	E	E	E	KJ	E	-0,122	Tidak Valid
20	Mudah	0,4	KJ	E	E	TE	E	0,298	Tidak Valid
21	Mudah	0	TE	TE	KJ	E	TE	∞	Tidak Valid
22	Mudah	0,2	E	TE	E	TE	KJ	0,132	Tidak Valid
23	Mudah	0,1	TE	KJ	TE	E	TE	0,346	Tidak Valid
24	Mudah	0,3	KJ	TE	E	E	TE	0,471	Valid
25	Sedang	0,1	E	E	TE	KJ	E	0,012	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
26	Sedang	0,2	E	E	E	E	KJ	0,260	Tidak Valid
27	Sedang	-0,3	E	KJ	E	E	E	-0,203	Tidak Valid
28	Sedang	0,4	KJ	E	E	E	E	0,595	Valid
29	Sedang	0	E	E	E	E	KJ	-0,047	Tidak Valid
30	Mudah	0,4	E	TE	E	KJ	TE	0,505	Valid
31	Mudah	0,2	TE	E	KJ	E	TE	0,236	Tidak Valid
32	Mudah	0	KJ	E	TE	TE	TE	-0,022	Tidak Valid
33	Mudah	0	KJ	E	TE	TE	E	-0,022	Tidak Valid
34	Sedang	0,5	E	KJ	E	TE	E	0,543	Valid
35	Mudah	0,3	E	E	E	TE	KJ	0,487	Valid
36	Sedang	0,5	TE	TE	E	KJ	E	0,531	Valid
37	Sedang	0,3	KJ	E	E	E	E	0,526	Valid
38	Sedang	0	E	E	KJ	TE	E	-0,115	Tidak Valid
39	Sedang	0,4	E	E	E	E	KJ	0,503	Valid
40	Sedang	0,5	TE	KJ	E	E	E	0,448	Valid
41	Mudah	0,3	KJ	E	E	E	E	0,468	Valid
42	Sedang	0,3	E	E	TE	KJ	TE	0,448	Valid
43	Sedang	-0,1	E	E	KJ	E	E	-0,047	Tidak Valid
44	Sedang	0,4	E	E	E	E	KJ	0,546	Valid
45	Sedang	0,6	E	E	E	TE	KJ	0,561	Valid

4. Paket Soal H

Validitas butir paket soal H oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 24. Butir soal pada paket soal H akan dilampirkan pada Lampiran 25. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 26. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal H akan ditunjukkan oleh Tabel 4.9 di bawah ini.

Tabel 4.9 Hasil Analisis Butir Soal untuk Paket Soal H

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Sedang	-0,1	E	KJ	E	E	TE	0,038	Tidak Valid
2	Mudah	0	KJ	TE	TE	TE	TE	∞	Tidak Valid
3	Sedang	0,5	E	KJ	E	E	E	0,565	Valid
4	Sedang	0,4	E	E	TE	E	KJ	0,565	Valid
5	Sedang	0,5	E	TE	KJ	TE	E	0,632	Valid
6	Sedang	0,4	KJ	E	E	TE	E	0,581	Valid
7	Sedang	0,3	E	KJ	TE	E	E	0,462	Valid
8	Sukar	0	E	TE	E	E	KJ	-0,093	Tidak Valid
9	Sedang	-0,1	E	E	E	KJ	TE	0,040	Tidak Valid
10	Sedang	0	E	E	TE	E	KJ	0,090	Tidak Valid
11	Sedang	0,3	TE	E	E	KJ	TE	0,493	Valid
12	Sedang	0,2	E	TE	KJ	E	TE	0,292	Tidak Valid
13	Mudah	0	KJ	E	TE	TE	TE	-0,022	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
14	Mudah	0,4	E	KJ	E	E	TE	0,404	Tidak Valid
15	Sedang	0,1	E	E	KJ	TE	E	0,076	Tidak Valid
16	Mudah	0,2	TE	E	E	KJ	E	0,080	Tidak Valid
17	Sedang	0	E	E	KJ	E	E	-0,025	Tidak Valid
18	Sedang	0,3	E	E	E	KJ	E	0,163	Tidak Valid
19	Sedang	0,3	E	KJ	E	E	TE	0,076	Tidak Valid
20	Sedang	0,5	E	E	KJ	E	E	0,483	Valid
21	Mudah	0	KJ	TE	TE	TE	TE	∞	Tidak Valid
22	Mudah	0,2	TE	E	E	TE	KJ	0,283	Tidak Valid
23	Mudah	0,5	E	KJ	E	TE	TE	0,480	Valid
24	Sedang	0,4	E	KJ	TE	E	E	0,324	Tidak Valid
25	Sedang	0,4	KJ	E	E	E	E	0,552	Valid
26	Sedang	0,3	E	E	KJ	E	E	0,625	Valid
27	Sukar	0,3	E	E	E	KJ	TE	0,579	Valid
28	Sukar	-0,1	TE	E	E	E	KJ	-0,236	Tidak Valid
29	Sedang	0,3	E	KJ	E	E	E	0,477	Valid
30	Mudah	0,1	KJ	E	TE	E	TE	0,084	Tidak Valid
31	Mudah	0,1	TE	E	TE	TE	KJ	0,127	Tidak Valid
32	Mudah	0,2	TE	TE	KJ	TE	E	0,257	Tidak Valid
33	Mudah	0,4	TE	E	TE	KJ	E	0,463	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
34	Sedang	0,5	KJ	E	E	TE	E	0,603	Valid
35	Sedang	0,4	E	KJ	TE	E	E	0,692	Valid
36	Mudah	0,4	E	E	E	TE	KJ	0,555	Valid
37	Sedang	0,4	TE	TE	KJ	E	E	0,470	Valid
38	Sedang	0,3	E	KJ	E	E	TE	0,524	Valid
39	Sedang	-0,3	KJ	E	E	E	TE	-0,413	Tidak Valid
40	Sukar	-0,1	E	E	E	KJ	E	-0,103	Tidak Valid
41	Sukar	0,3	E	E	KJ	E	E	0,489	Valid
42	Sedang	0,2	E	E	E	E	KJ	0,467	Valid
43	Sedang	0,4	E	KJ	E	E	E	0,537	Valid
44	Sedang	0,4	KJ	E	E	E	E	0,514	Valid
45	Sedang	0,3	E	E	KJ	TE	E	0,483	Valid

4.1.4 Hasil Analisis Butir Soal Mata Kuliah Kriptografi Tahap III

Analisis butir soal mata kuliah kriptografi tahap III dilakukan pada tanggal 10 Juni 2015. Butir soal yang dibuat dibagi menjadi 4 paket soal yaitu paket soal 1, paket soal 2, paket soal 3, dan paket soal 4. Setiap paket soal yang diujikan berisi 40 soal pilihan ganda. Setiap paket soal diujikan kepada 20 mahasiswa Prodi PTIK UNJ yang sedang mengambil mata kuliah kriptografi. Materi yang diujikan mulai dari perbedaan DES dan AES sampai dengan penggunaan kriptografi dalam kehidupan sehari-hari. Berikut ini merupakan hasil analisis butir

soal mata kuliah kriptografi untuk paket soal 1, paket soal 2, paket soal 3, dan paket soal 4. Kisi-kisi instrumen untuk pengujian tahap III akan dilampirkan pada Lampiran 27.

1. Paket Soal 1

Validitas butir paket soal 1 oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 28. Butir soal pada paket soal 1 akan dilampirkan pada Lampiran 29. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 30. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal 1 akan ditunjukkan oleh Tabel 4.10 di bawah ini.

Tabel 4.10 Hasil Analisis Butir Soal untuk Paket Soal 1

No.	**Taraf Kesukaran**	**Daya Beda**	**Efektivitas Pengecoh**					**Validitas**	**Ket**
			A	**B**	**C**	**D**	**E**		
1	Mudah	0,2	KJ	TE	E	E	E	0,188	Tidak Valid
2	Sedang	-0,4	TE	KJ	E	E	E	-0,307	Tidak Valid
3	Sedang	0,6	E	E	E	KJ	E	0,473	Valid
4	Sedang	0	E	E	E	E	KJ	-0,141	Tidak Valid
5	Mudah	0,5	E	KJ	E	E	TE	0,575	Valid
6	Sedang	0,5	KJ	E	E	E	E	0,568	Valid
7	Mudah	0,5	E	E	KJ	E	E	0,575	Valid
8	Mudah	0,4	E	KJ	E	E	TE	0,512	Valid
9	Sedang	0,5	E	E	E	KJ	E	0,588	Valid
10	Sedang	0,3	KJ	E	E	E	E	0,456	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
11	Sedang	0,4	E	E	KJ	E	E	0,499	Valid
12	Sukar	0	TE	KJ	TE	E	E	-0,110	Tidak Valid
13	Sedang	0,5	E	E	KJ	E	E	0,666	Valid
14	Sedang	0,4	TE	E	KJ	E	E	0,512	Valid
15	Sedang	0,6	E	TE	E	E	KJ	0,657	Valid
16	Mudah	0,4	E	E	TE	KJ	E	0,512	Valid
17	Mudah	0,4	KJ	TE	E	E	E	0,458	Valid
18	Sukar	0,3	E	KJ	E	E	E	0,487	Valid
19	Sedang	0,1	E	E	KJ	TE	TE	0,043	Tidak Valid
20	Sedang	0,4	KJ	E	E	E	E	0,549	Valid
21	Mudah	0,4	E	E	E	E	KJ	0,471	Valid
22	Sedang	0,6	E	E	E	KJ	E	0,545	Valid
23	Sedang	0,4	E	KJ	E	E	E	0,499	Valid
24	Sedang	0,5	E	E	KJ	E	E	0,551	Valid
25	Sukar	0,4	E	E	E	KJ	TE	0,485	Valid
26	Sedang	0,7	KJ	TE	E	TE	E	0,588	Valid
27	Sedang	0,4	E	E	E	KJ	E	0,473	Valid
28	Sedang	0,4	E	KJ	E	E	E	0,562	Valid
29	Sedang	0,6	E	TE	E	TE	KJ	0,567	Valid
30	Sedang	0,4	E	E	KJ	E	E	0,473	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
31	Sedang	0,5	E	E	E	KJ	E	0,569	Valid
32	Sedang	0,3	E	KJ	E	E	E	0,538	Valid
33	Mudah	0,4	KJ	TE	E	E	E	0,526	Valid
34	Sedang	-0,2	E	KJ	TE	E	TE	-0,115	Tidak Valid
35	Sedang	0,4	E	E	E	TE	KJ	0,470	Valid
36	Mudah	0,3	KJ	E	TE	TE	E	0,513	Valid
37	Mudah	0,4	E	E	E	KJ	TE	0,579	Valid
38	Mudah	0,4	TE	TE	KJ	E	TE	0,454	Valid
39	Mudah	0,4	E	TE	TE	TE	KJ	0,470	Valid
40	Mudah	0,4	E	KJ	TE	TE	TE	0,454	Valid

2. Paket Soal 2

Validitas butir paket soal 2 oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 31. Butir soal pada paket soal 2 akan dilampirkan pada Lampiran 32. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 33. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal 2 akan ditunjukkan oleh Tabel 4.11 di bawah ini.

Tabel 4.11 Hasil Analisis Butir Soal untuk Paket Soal 2

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Sedang	0,4	E	KJ	E	TE	E	0,451	Valid
2	Sedang	0,3	E	TE	TE	TE	KJ	0,503	Valid
3	Sukar	0,4	E	E	KJ	E	E	0,519	Valid
4	Sedang	0,3	E	KJ	TE	E	E	0,465	Valid
5	Mudah	0,4	TE	E	E	KJ	E	0,535	Valid
6	Sukar	0,3	KJ	E	E	E	E	0,519	Valid
7	Mudah	0,4	E	TE	E	TE	KJ	0,542	Valid
8	Sedang	0,5	E	KJ	TE	E	E	0,626	Valid
9	Sedang	0,6	KJ	E	E	E	E	0,527	Valid
10	Sedang	0,5	E	E	KJ	E	E	0,488	Valid
11	Mudah	0,4	TE	E	E	KJ	E	0,509	Valid
12	Sedang	0,4	TE	E	TE	E	KJ	0,589	Valid
13	Sukar	0,3	E	E	E	KJ	E	0,508	Valid
14	Sukar	0,4	KJ	E	E	E	E	0,592	Valid
15	Sedang	0,3	E	KJ	TE	E	E	0,525	Valid
16	Mudah	0	E	TE	KJ	TE	E	0,019	Tidak Valid
17	Sedang	0,6	E	E	E	KJ	E	0,546	Valid
18	Mudah	0,1	TE	E	E	KJ	E	-0,005	Tidak Valid
19	Sedang	0,5	KJ	E	E	E	TE	0,665	Valid
20	Sedang	0,4	E	E	TE	E	KJ	0,465	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
21	Sedang	0,4	E	KJ	E	E	E	0,609	Valid
22	Sukar	-0,3	E	E	KJ	TE	E	-0,499	Tidak Valid
23	Sedang	0,4	E	E	E	KJ	E	0,530	Valid
24	Sedang	-0,1	E	E	E	TE	KJ	-0,124	Tidak Valid
25	Sedang	0,5	KJ	E	E	E	E	0,488	Valid
26	Sedang	0,2	E	KJ	TE	E	E	0,451	Valid
27	Sedang	0,2	E	E	KJ	TE	E	0,265	Tidak Valid
28	Sukar	0,5	E	E	KJ	E	E	0,535	Valid
29	Sukar	0,3	KJ	E	E	E	E	0,476	Valid
30	Sedang	0,5	E	KJ	E	E	E	0,465	Valid
31	Mudah	0,2	E	TE	TE	KJ	E	0,191	Tidak Valid
32	Sedang	-0,1	E	E	E	E	KJ	0,036	Tidak Valid
33	Sedang	0,4	KJ	E	TE	E	TE	0,549	Valid
34	Mudah	0,2	E	TE	KJ	E	TE	0,497	Valid
35	Mudah	0,1	TE	E	E	KJ	E	0,059	Tidak Valid
36	Mudah	-0,1	TE	E	E	KJ	TE	-0,262	Tidak Valid
37	Mudah	0	TE	KJ	E	TE	TE	0,089	Tidak Valid
38	Mudah	-0,1	TE	TE	E	TE	KJ	-0,272	Tidak Valid
39	Mudah	0,4	KJ	E	TE	TE	TE	0,535	Valid
40	Sedang	0	E	E	KJ	E	E	0,023	Tidak Valid

3. Paket Soal 3

Validitas butir paket soal 3 oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 34. Butir soal pada paket soal 3 akan dilampirkan pada Lampiran 35. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 36. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal 3 akan ditunjukkan oleh Tabel 4.12 di bawah ini.

Tabel 4.12 Hasil Analisis Butir Soal untuk Paket Soal 3

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Mudah	0,2	E	E	KJ	E	TE	0,446	Valid
2	Sedang	0,4	KJ	E	TE	E	E	0,462	Valid
3	Mudah	0,3	TE	KJ	E	E	E	0,371	Tidak Valid
4	Sedang	0,4	E	TE	E	KJ	TE	0,641	Valid
5	Mudah	0,1	TE	E	KJ	E	TE	0,292	Tidak Valid
6	Sukar	0,3	E	E	E	TE	KJ	0,532	Valid
7	Sedang	0,5	E	KJ	E	E	E	0,524	Valid
8	Sedang	0,3	KJ	E	E	E	E	0,545	Valid
9	Mudah	0,4	E	KJ	E	E	E	0,446	Valid
10	Sukar	0,4	E	E	KJ	E	E	0,540	Valid
11	Mudah	0,3	KJ	E	E	TE	TE	0,450	Valid
12	Sedang	0,6	E	E	E	KJ	E	0,654	Valid
13	Sukar	0,2	TE	E	E	E	KJ	0,497	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
14	Sukar	0,3	E	E	E	E	KJ	0,539	Valid
15	Mudah	0,3	TE	KJ	TE	E	E	0,470	Valid
16	Mudah	0,1	KJ	TE	TE	TE	E	0,155	Tidak Valid
17	Sedang	0,4	TE	E	KJ	E	E	0,514	Valid
18	Sukar	0,3	E	E	E	KJ	TE	0,508	Valid
19	Sedang	0	E	E	TE	E	KJ	-0,098	Tidak Valid
20	Sedang	0,2	E	KJ	E	E	E	0,462	Valid
21	Sukar	0,2	KJ	E	E	E	E	0,488	Valid
22	Mudah	0,1	TE	E	KJ	E	E	0,114	Tidak Valid
23	Sukar	0,4	KJ	E	E	E	E	0,497	Valid
24	Sedang	0,4	E	E	E	KJ	E	0,483	Valid
25	Sedang	0,5	E	E	E	TE	KJ	0,461	Valid
26	Sedang	-0,2	E	KJ	E	E	TE	-0,115	Tidak Valid
27	Sukar	0,2	E	E	E	E	KJ	0,460	Valid
28	Sedang	0,2	E	E	E	KJ	E	0,497	Valid
29	Sukar	0,3	E	E	KJ	E	TE	0,556	Valid
30	Sedang	0,5	E	E	E	E	KJ	0,697	Valid
31	Mudah	0	KJ	E	E	TE	E	0,017	Tidak Valid
32	Sukar	-0,1	E	KJ	E	E	E	-0,272	Tidak Valid
33	Sedang	0,3	E	E	TE	KJ	E	0,216	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
34	Mudah	0,2	TE	KJ	E	E	TE	0,452	Valid
35	Mudah	0	TE	TE	KJ	E	TE	-0,174	Tidak Valid
36	Mudah	0	TE	TE	TE	E	KJ	-0,146	Tidak Valid
37	Mudah	0	KJ	TE	TE	E	TE	-0,174	Tidak Valid
38	Mudah	0,2	E	KJ	TE	TE	TE	0,146	Tidak Valid
39	Mudah	0	TE	E	TE	KJ	TE	0,026	Tidak Valid
40	Mudah	0,2	E	E	KJ	E	E	0,331	Tidak Valid

4. Paket Soal 4

Validitas butir paket soal 4 oleh dosen pengampu mata kuliah kriptografi akan dilampirkan pada Lampiran 37. Butir soal pada paket soal 4 akan dilampirkan pada Lampiran 38. Hasil perhitungan taraf kesukaran, daya beda, efektifitas pengecoh dan validitas butir soal akan dilampirkan pada Lampiran 39. Hasil analisis butir soal mata kuliah kriptografi untuk paket soal 4 akan ditunjukkan oleh Tabel 4.13 di bawah ini.

Tabel 4.13 Hasil Analisis Butir Soal untuk Paket Soal 4.

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
1	Sedang	0,4	E	TE	E	KJ	E	0,475	Valid
2	Sukar	0,4	TE	E	KJ	E	E	0,657	Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
3	Sedang	0,4	KJ	E	E	E	E	0,475	Valid
4	Mudah	0,4	TE	E	TE	E	KJ	0,522	Valid
5	Mudah	0	E	KJ	TE	E	E	0,055	Tidak Valid
6	Mudah	0,5	TE	KJ	TE	TE	E	0,503	Valid
7	Sedang	0,4	KJ	E	E	E	E	0,511	Valid
8	Sedang	0,3	E	E	E	KJ	E	0,504	Valid
9	Sedang	0,3	E	E	KJ	E	E	0,499	Valid
10	Sedang	0,3	E	E	E	E	KJ	0,520	Valid
11	Sedang	0,5	TE	KJ	E	E	TE	0,649	Valid
12	Sedang	0,5	KJ	E	E	E	E	0,549	Valid
13	Sedang	0,1	E	E	E	KJ	E	-0,015	Tidak Valid
14	Sedang	0,5	KJ	E	E	E	TE	0,577	Valid
15	Sukar	0,3	E	E	KJ	E	E	0,552	Valid
16	Sedang	0,4	E	KJ	E	E	TE	0,494	Valid
17	Sedang	0,3	E	E	E	E	KJ	0,450	Valid
18	Sedang	0,4	KJ	E	E	E	TE	0,494	Valid
19	Sedang	0,5	E	E	E	KJ	E	0,566	Valid
20	Sukar	0,3	E	E	KJ	TE	E	0,521	Valid
21	Sedang	0,4	TE	TE	KJ	E	E	0,462	Valid
22	Sedang	0,4	E	KJ	E	E	E	0,523	Valid
23	Mudah	0,2	KJ	E	TE	E	TE	0,194	Tidak Valid

No.	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas	Ket
			A	B	C	D	E		
24	Sedang	0,6	E	E	KJ	E	TE	0,511	Valid
25	Sedang	-0,1	E	E	E	E	KJ	0,043	Tidak Valid
26	Sedang	0,4	E	E	E	KJ	E	0,588	Valid
27	Sedang	0,7	E	E	KJ	E	E	0,616	Valid
28	Sedang	0,4	KJ	E	E	E	E	0,556	Valid
29	Sukar	-0,1	E	KJ	E	TE	E	0,009	Tidak Valid
30	Sedang	0,1	KJ	E	TE	E	E	-0,048	Tidak Valid
31	Mudah	-0,2	TE	E	TE	KJ	E	-0,359	Tidak Valid
32	Mudah	0,2	E	E	KJ	TE	TE	0,451	Valid
33	Sedang	0,5	E	E	E	TE	KJ	0,529	Valid
34	Mudah	0	KJ	TE	E	TE	TE	∞	Tidak Valid
35	Mudah	0,1	E	KJ	TE	TE	TE	0,171	Tidak Valid
36	Mudah	0	TE	TE	KJ	TE	TE	∞	Tidak Valid
37	Sedang	-0,2	E	E	E	KJ	E	-0,233	Tidak Valid
38	Mudah	0,1	E	E	KJ	TE	TE	0,113	Tidak Valid
39	Mudah	-0,1	E	TE	E	TE	KJ	-0,192	Tidak Valid
40	Sedang	0,2	E	E	KJ	E	E	-0,107	Tidak Valid

4.1.5 Hasil Analisis Butir Soal untuk Bank Soal Mata Kuliah Kriptografi

Setelah dilakukan pengujian analisis butir soal mata kuliah kriptografi pada tahap I, II, dan III, butir soal tersebut dipilih sesuai dengan parameter uji taraf kesukaran, uji daya beda, uji efektivitas pengecoh, dan uji validitas butir soal. Bank soal mata kuliah kriptografi memiliki jumlah butir soal yang valid yaitu sebanyak 284 soal dengan memenuhi 40 indikator mata kuliah kriptografi. Soal-soal yang bersifat tidak valid yaitu sebanyak 175 soal dari 460 soal yang telah diuji tidak digunakan pada bank soal mata kuliah kriptografi. Selain itu, terdapat pula 1 soal yang bersifat valid namun memiliki daya beda dengan nilai 0. Soal tersebut tidak digunakan pada bank soal mata kuliah kriptografi karena soal tersebut tidak dapat membedakan mahasiswa yang memiliki pengetahuan tinggi dengan mahasiswa yang memeuliki pengetahuan rendah.

Bank soal mata kuliah kriptografi terdiri dari minimal 5 butir soal setiap indikatornya. Kisi-kisi instrumen untuk bank soal mata kuliah kriptografi akan dilampirkan pada Lampiran 40. Bank soal mata kuliah kriptografi akan dilampirkan pada Lampiran 41. Berikut merupakan hasil analisis butir soal untuk bank soal mata kuliah kriptografi yang akan ditunjukkan pada Tabel 4.14 di bawah ini.

Tabel 4.14 Hasil Analisis Butir Soal untuk Bank Soal Mata Kuliah Kriptografi

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
Terminologi Kriptografi	1	Mudah	0,4	E	KJ	TE	E	TE	Valid
	2	Mudah	0,2	KJ	E	TE	TE	E	Valid
	3	Mudah	0,2	TE	TE	E	E	KJ	Valid
	4	Sedang	0,4	E	E	KJ	E	E	Valid
	5	Sedang	0,4	KJ	TE	TE	E	E	Valid
	6	Mudah	0,4	E	TE	E	TE	KJ	Valid
Tujuan Kriptografi	1	Mudah	0,3	E	TE	TE	E	KJ	Valid
	2	Sedang	0,6	E	E	E	KJ	E	Valid
	3	Mudah	0,2	KJ	E	TE	TE	E	Valid
	4	Sedang	0,5	E	KJ	E	E	E	Valid
	5	Sedang	0,4	E	E	KJ	TE	E	Valid
	6	Sedang	0,4	E	E	E	KJ	E	Valid
Sejarah Kriptografi	1	Mudah	0,4	E	KJ	E	E	E	Valid
	2	Sedang	0,7	KJ	E	TE	TE	E	Valid
	3	Sedang	0,4	E	E	KJ	E	TE	Valid
	4	Sedang	0,5	E	E	E	E	KJ	Valid
	5	Sedang	0,5	KJ	TE	TE	E	E	Valid
	6	Sukar	0,3	E	TE	KJ	E	E	Valid
	7	Sukar	0,4	KJ	E	E	E	TE	Valid
	8	Sedang	0,5	TE	KJ	E	E	E	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
Kriptanalisis	1	Sukar	0,3	E	TE	KJ	E	TE	Valid
	2	Sedang	0,4	E	TE	KJ	E	E	Valid
	3	Sukar	0,4	E	E	KJ	TE	E	Valid
	4	Sedang	0,5	E	TE	KJ	TE	E	Valid
	5	Sukar	0,3	KJ	E	TE	E	E	Valid
	6	Mudah	0,3	TE	E	TE	KJ	TE	Valid
Kunci simetris dan asimetris	1	Mudah	0,4	TE	E	TE	KJ	E	Valid
	2	Sedang	0,5	E	KJ	E	E	E	Valid
	3	Sedang	0,5	E	E	KJ	TE	E	Valid
	4	Sedang	0,4	KJ	E	E	TE	E	Valid
	5	Sukar	0,3	E	E	E	E	KJ	Valid
	6	Sedang	0,5	TE	TE	E	KJ	E	Valid
Keamanan algoritma kriptografi	1	Sukar	0,4	E	E	KJ	E	E	Valid
	2	Sedang	0,3	E	KJ	E	E	E	Valid
	3	Sedang	0,3	E	KJ	TE	E	E	Valid
	4	Sedang	0,3	E	E	KJ	E	E	Valid
	5	Sedang	0,5	E	E	E	E	KJ	Valid
Serangan terhadap kriptografi	1	Sukar	0,3	E	E	E	E	KJ	Valid
	2	Sedang	0,6	TE	KJ	E	E	TE	Valid
	3	Sedang	0,7	E	E	E	KJ	E	Valid
	4	Sedang	0,4	E	E	KJ	E	E	Valid
	5	Sedang	0,4	KJ	E	E	E	E	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
Kompleksitas serangan terhadap kriptografi	1	Sedang	0,5	TE	E	TE	KJ	E	Valid
	2	Sedang	0,5	KJ	E	E	TE	TE	Valid
	3	Sedang	0,5	E	E	E	KJ	E	Valid
	4	Sedang	0,2	E	KJ	E	E	E	Valid
	5	Sedang	0,5	KJ	E	TE	E	E	Valid
	6	Sedang	0,3	TE	E	E	KJ	TE	Valid
Fungsi matematika	1	Mudah	0,3	KJ	E	E	E	TE	Valid
	2	Sedang	0,3	E	TE	KJ	E	E	Valid
	3	Sedang	0,5	E	E	E	KJ	TE	Valid
	4	Sedang	0,6	E	E	E	KJ	E	Valid
	5	Sedang	0,4	E	TE	KJ	E	TE	Valid
	6	Sedang	0,7	E	KJ	E	E	TE	Valid
Fungsi permutasi	1	Sedang	0,5	E	E	TE	KJ	E	Valid
	2	Sedang	0,6	E	KJ	E	E	E	Valid
	3	Mudah	0,4	E	E	KJ	E	E	Valid
	4	Mudah	0,6	KJ	E	E	E	E	Valid
	5	Sedang	0,5	KJ	TE	E	E	TE	Valid
	6	Mudah	0,3	E	E	E	KJ	E	Valid
	7	Mudah	0,3	TE	E	KJ	E	E	Valid
	8	Mudah	0,4	TE	TE	E	E	KJ	Valid
Fungsi Kombinasi	1	Mudah	0,6	TE	E	KJ	E	E	Valid
	2	Sedang	0,6	E	KJ	E	TE	E	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	3	Mudah	0,2	KJ	E	E	E	TE	Valid
	4	Mudah	0,4	TE	E	E	E	KJ	Valid
	5	Sedang	0,6	TE	E	KJ	E	E	Valid
	6	Sedang	0,5	TE	E	E	KJ	E	Valid
	7	Sedang	0,3	E	E	E	E	KJ	Valid
Teori peluang	1	Sukar	0,3	E	E	E	KJ	E	Valid
	2	Sedang	0,6	E	E	E	E	KJ	Valid
	3	Sedang	0,4	KJ	E	E	E	E	Valid
	4	Sukar	0,3	KJ	E	TE	E	E	Valid
	5	Sedang	0,7	E	KJ	E	E	E	Valid
	6	Sedang	0,3	E	E	KJ	E	E	Valid
	7	Sukar	0,5	E	E	KJ	E	E	Valid
Teori bilangan	1	Sedang	0,4	E	E	KJ	E	TE	Valid
	2	Mudah	0,5	E	E	E	KJ	TE	Valid
	3	Mudah	0,1	TE	KJ	E	E	TE	Valid
	4	Sedang	0,5	E	E	KJ	E	E	Valid
	5	Sedang	0,4	KJ	E	E	E	TE	Valid
Algoritma *cipher* substitusi	1	Mudah	0,2	TE	E	E	KJ	TE	Valid
	2	Mudah	0,2	E	TE	KJ	E	TE	Valid
	3	Sedang	0,4	E	E	E	TE	KJ	Valid
	4	Mudah	0,3	KJ	E	TE	TE	E	Valid
	5	Mudah	0,2	TE	KJ	E	E	TE	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	6	Mudah	0,4	TE	TE	KJ	E	TE	Valid
Algoritma *cipher* transposisi	1	Mudah	0,3	KJ	TE	E	E	TE	Valid
	2	Mudah	0,5	E	KJ	E	TE	TE	Valid
	3	Sedang	0,4	E	TE	KJ	TE	TE	Valid
	4	Mudah	0,4	TE	TE	KJ	E	TE	Valid
	5	Mudah	0,4	KJ	E	TE	TE	TE	Valid
	6	Mudah	0,4	E	TE	TE	TE	KJ	Valid
	7	Mudah	0,4	E	KJ	TE	TE	TE	Valid
Algoritma *affine cipher*	1	Mudah	0,4	E	E	KJ	TE	E	Valid
	2	Sedang	0,4	E	E	TE	E	KJ	Valid
	3	Sukar	0,2	E	KJ	E	E	E	Valid
	4	Mudah	0,6	KJ	E	E	E	E	Valid
	5	Sedang	0,4	KJ	E	E	E	E	Valid
	6	Sedang	0,3	E	E	KJ	E	E	Valid
	7	Sedang	0,3	TE	E	E	KJ	E	Valid
	8	Sukar	0,3	KJ	E	E	E	E	Valid
	9	Sedang	0,5	E	KJ	E	TE	E	Valid
Algoritma *vigenere*	1	Sedang	0,4	E	KJ	E	E	E	Valid
	2	Sedang	0,6	E	E	KJ	E	E	Valid
	3	Sedang	0,4	E	E	E	E	KJ	Valid
	4	Sedang	0,3	KJ	E	E	E	TE	Valid
	5	Sedang	0,6	E	TE	E	KJ	E	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
Algoritma *playfair*	1	Sedang	0,7	TE	E	E	KJ	E	Valid
	2	Sedang	0,7	E	E	KJ	E	E	Valid
	3	Sedang	0,4	KJ	E	E	E	E	Valid
	4	Sedang	0,4	E	E	KJ	E	E	Valid
	5	Sukar	0,3	E	E	E	KJ	TE	Valid
	6	Sukar	0,4	KJ	E	E	E	E	Valid
Algoritma *one-time pad*	1	Sedang	0,4	TE	KJ	E	E	E	Valid
	2	Sedang	0,2	E	TE	E	E	KJ	Valid
	3	Sedang	0,6	KJ	E	E	E	E	Valid
	4	Sedang	0,6	E	E	E	KJ	E	Valid
	5	Sukar	0,5	KJ	E	E	E	TE	Valid
	6	Sedang	0,3	E	KJ	E	E	E	Valid
Rangkaian bit dan operasinya	1	Sedang	0,4	TE	E	KJ	E	E	Valid
	2	Sedang	0,3	E	E	TE	KJ	E	Valid
	3	Mudah	0,3	E	KJ	E	TE	E	Valid
	4	Mudah	0,2	E	E	KJ	TE	E	Valid
	5	Mudah	0,4	E	TE	E	KJ	TE	Valid
Algoritma enkripsi dengan XOR sederhana	1	Mudah	0,4	KJ	E	E	E	TE	Valid
	2	Mudah	0,3	E	KJ	TE	E	E	Valid
	3	Mudah	0,3	KJ	TE	E	TE	E	Valid
	4	Mudah	0,3	KJ	E	TE	TE	TE	Valid
	5	Mudah	0,4	TE	E	TE	KJ	E	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	6	Mudah	0,4	TE	E	E	TE	KJ	Valid
Manajemen kunci	1	Sukar	0,2	E	E	E	KJ	E	Valid
	2	Sukar	0,3	E	KJ	E	E	E	Valid
	3	Sedang	0,5	E	KJ	E	TE	E	Valid
	4	Sedang	0,4	E	E	TE	E	KJ	Valid
	5	Sedang	0,5	KJ	E	E	TE	E	Valid
	6	Sedang	0,2	E	E	KJ	E	E	Valid
	7	Sedang	0,3	TE	E	TE	KJ	E	Valid
DES dan AES	1	Sedang	0,3	TE	E	KJ	TE	E	Valid
	2	Mudah	0,3	E	E	E	TE	KJ	Valid
	3	Sukar	0,4	KJ	E	E	E	E	Valid
	4	Sedang	0,4	E	KJ	E	TE	E	Valid
	5	Mudah	0,2	E	E	KJ	E	TE	Valid
	6	Sedang	0,4	E	TE	E	KJ	E	Valid
	7	Sedang	0,3	E	TE	TE	TE	KJ	Valid
	8	Sedang	0,4	KJ	E	TE	E	E	Valid
	9	Sukar	0,4	TE	E	KJ	E	E	Valid
RC4 dan A5	1	Sedang	0,4	E	KJ	TE	E	E	Valid
	2	Sedang	0,4	KJ	E	TE	TE	E	Valid
	3	Sedang	0,5	E	E	E	E	KJ	Valid
	4	Sedang	0,5	TE	TE	E	KJ	E	Valid
	5	Sedang	0,6	E	E	KJ	TE	TE	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
Cipher aliran	1	Mudah	0,3	E	KJ	E	E	TE	Valid
	2	Sedang	0,3	KJ	E	E	E	E	Valid
	3	Sedang	0,3	E	E	E	KJ	E	Valid
	4	Mudah	0,4	E	E	E	TE	KJ	Valid
	5	Sedang	0,4	TE	TE	KJ	E	E	Valid
Serangan terhadap *cipher* aliran	1	Sedang	0,5	KJ	E	E	E	E	Valid
	2	Sukar	0,4	E	E	TE	E	KJ	Valid
	3	Sedang	0,3	E	KJ	E	E	TE	Valid
	4	Sukar	0,5	E	E	KJ	TE	E	Valid
	5	Sedang	0,4	KJ	E	E	E	E	Valid
	6	Sukar	0,4	E	E	KJ	E	E	Valid
	7	Sedang	0,6	E	E	E	KJ	E	Valid
	8	Mudah	0,4	TE	E	TE	E	KJ	Valid
	9	Sedang	0,4	E	TE	E	KJ	TE	Valid
	10	Sedang	0,3	E	KJ	TE	E	E	Valid
Cipher blok	1	Sedang	0,3	E	E	E	KJ	E	Valid
	2	Sedang	0,3	E	KJ	E	E	E	Valid
	3	Sedang	0,4	E	E	E	E	KJ	Valid
	4	Sedang	0,4	TE	E	KJ	E	E	Valid
	5	Mudah	0,4	TE	E	E	KJ	E	Valid
	6	Sukar	0,3	E	E	E	TE	KJ	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	7	Sukar	0,3	KJ	E	E	E	E	Valid
	8	Mudah	0,5	E	KJ	E	E	TE	Valid
	9	Mudah	0,5	TE	KJ	TE	TE	E	Valid
Prinsip perancangan *cipher* blok	1	Sedang	0,3	TE	E	E	E	KJ	Valid
	2	Sedang	0,5	TE	KJ	E	E	E	Valid
	3	Sedang	0,6	KJ	E	E	E	E	Valid
	4	Sedang	0,3	E	E	KJ	E	E	Valid
	5	Sedang	0,5	KJ	E	E	E	E	Valid
	6	Sedang	0,5	E	KJ	E	E	E	Valid
	7	Mudah	0,5	E	E	KJ	E	E	Valid
	8	Sedang	0,4	KJ	E	E	E	E	Valid
	9	Sedang	0,3	E	E	E	KJ	E	Valid
	10	Mudah	0,4	E	TE	E	TE	KJ	Valid
	11	Sedang	0,5	E	KJ	TE	E	E	Valid
Konsep kriptografi kunci publik	1	Sukar	0,3	E	E	KJ	E	E	Valid
	2	Sedang	0,2	E	E	E	E	KJ	Valid
	3	Mudah	0,3	KJ	E	E	E	E	Valid
	4	Sukar	0,3	TE	E	E	KJ	TE	Valid
	5	Sedang	0,6	TE	KJ	TE	TE	E	Valid
Algoritma RSA	1	Sedang	0,4	E	KJ	E	E	E	Valid
	2	Sedang	0,3	E	E	TE	KJ	TE	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	3	Sukar	0,3	KJ	E	E	E	E	Valid
	4	Sedang	0,5	E	E	E	E	KJ	Valid
	5	Mudah	0,4	E	KJ	E	E	TE	Valid
	6	Sedang	0,3	KJ	E	E	E	E	Valid
	7	Sedang	0,3	E	E	KJ	E	E	Valid
	8	Sedang	0,3	E	E	E	E	KJ	Valid
	9	Sedang	0,5	E	E	E	KJ	E	Valid
	10	Sedang	0,6	KJ	E	E	E	E	Valid
	11	Sedang	0,5	E	E	KJ	E	E	Valid
	12	Mudah	0,4	E	KJ	E	E	E	Valid
Algoritma *ElGamal*	1	Sedang	0,4	TE	E	E	KJ	E	Valid
	2	Sedang	0,4	KJ	E	E	E	E	Valid
	3	Sedang	0,3	E	E	KJ	TE	E	Valid
	4	Sedang	0,3	E	KJ	E	E	E	Valid
	5	Sedang	0,4	E	E	E	E	KJ	Valid
Algoritma *Rabin*	1	Mudah	0,5	E	KJ	E	E	E	Valid
	2	Sedang	0,6	E	E	E	TE	KJ	Valid
	3	Sukar	0,2	E	E	KJ	E	E	Valid
	4	Sedang	0,3	KJ	E	E	E	E	Valid
	5	Sedang	0,6	E	E	E	KJ	E	Valid
	6	Sedang	0,4	E	E	KJ	E	E	Valid
	7	Sedang	0,5	TE	KJ	E	E	TE	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	8	Mudah	0,4	TE	E	E	KJ	E	Valid
	9	Sedang	0,4	TE	E	TE	E	KJ	Valid
	10	Sedang	0,5	KJ	E	E	E	E	Valid
	11	Sukar	0,4	E	E	KJ	E	E	Valid
Pembangkit bilangan prima	1	Sedang	0,4	E	E	E	KJ	E	Valid
	2	Sedang	0,4	KJ	E	E	E	E	Valid
	3	Sedang	0,4	E	KJ	E	E	E	Valid
	4	Sukar	0,2	E	E	E	E	KJ	Valid
	5	Sukar	0,5	E	E	KJ	E	E	Valid
Pembangkit bilangan acak semu	1	Sedang	0,3	E	KJ	TE	E	E	Valid
	2	Mudah	0,3	KJ	E	E	TE	TE	Valid
	3	Sukar	0,3	E	E	KJ	E	E	Valid
	4	Sukar	0,2	TE	E	E	E	KJ	Valid
	5	Sukar	0,4	KJ	E	E	E	E	Valid
	6	Sedang	0,5	E	E	KJ	E	E	Valid
	7	Sedang	0,4	TE	E	KJ	E	E	Valid
	8	Sedang	0,5	KJ	E	E	E	TE	Valid
	9	Sukar	0,3	E	E	E	E	KJ	Valid
	10	Sukar	0,3	E	E	E	KJ	E	Valid
Fungsi *hash* satu arah	1	Sedang	0,6	E	TE	E	E	KJ	Valid
	2	Mudah	0,3	TE	KJ	TE	E	E	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	3	Mudah	0,4	E	E	TE	KJ	E	Valid
	4	Sedang	0,4	KJ	E	E	E	TE	Valid
	5	Sedang	0,4	E	KJ	E	E	TE	Valid
	6	Sedang	0,4	TE	E	KJ	E	E	Valid
	7	Sedang	0,6	E	E	E	KJ	E	Valid
	8	Sedang	0,3	E	E	E	E	KJ	Valid
	9	Mudah	0,4	KJ	TE	E	E	E	Valid
Algoritma MD5	1	Sedang	0,4	TE	TE	KJ	E	E	Valid
	2	Sedang	0,5	KJ	E	E	E	TE	Valid
	3	Sukar	0,3	E	KJ	E	E	E	Valid
	4	Sedang	0,5	E	E	E	KJ	E	Valid
	5	Sedang	0,4	E	E	TE	E	KJ	Valid
	6	Sedang	0,4	KJ	E	E	E	E	Valid
	7	Sedang	0,4	E	KJ	E	E	E	Valid
	8	Sedang	0,2	E	KJ	E	E	E	Valid
	9	Sukar	0,3	E	E	E	KJ	TE	Valid
	10	Sukar	0,3	E	E	KJ	TE	E	Valid
Algoritma MAC	1	Sedang	0,2	E	E	E	KJ	E	Valid
	2	Sukar	0,3	E	E	KJ	E	TE	Valid
	3	Sukar	0,3	KJ	E	E	E	E	Valid
	4	Sedang	0,6	E	TE	E	TE	KJ	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
	5	Sedang	0,5	E	KJ	E	E	E	Valid
	6	Sedang	0,4	E	E	KJ	E	E	Valid
	7	Sedang	0,5	E	E	E	E	KJ	Valid
	8	Sedang	0,5	E	E	E	KJ	E	Valid
Konsep tanda tangan digital	1	Mudah	0,4	E	E	E	E	KJ	Valid
	2	Sedang	0,6	E	E	E	KJ	E	Valid
	3	Sukar	0,2	KJ	E	E	E	E	Valid
	4	Sedang	0,4	E	KJ	E	E	E	Valid
	5	Sedang	0,4	E	KJ	E	E	E	Valid
	6	Sedang	0,6	E	E	KJ	E	TE	Valid
	7	Sedang	0,4	E	E	E	KJ	E	Valid
	8	Sukar	0,4	KJ	E	E	E	E	Valid
Protokol kriptografi	1	Sedang	0,4	E	E	E	KJ	E	Valid
	2	Sedang	0,5	KJ	E	E	E	E	Valid
	3	Sedang	0,5	E	E	KJ	E	E	Valid
	4	Sedang	0,2	E	KJ	TE	E	E	Valid
	5	Sukar	0,4	E	E	E	KJ	TE	Valid
	6	Sedang	0,7	KJ	TE	E	TE	E	Valid
	7	Sedang	0,7	E	E	KJ	E	E	Valid
	8	Sedang	0,4	E	E	E	KJ	E	Valid
	9	Sedang	0,5	E	E	E	TE	KJ	Valid

Materi	Nomor Soal	Taraf Kesukaran	Daya Beda	Efektivitas Pengecoh					Validitas
				A	B	C	D	E	
Penggunaan kriptografi dalam kehidupan sehari-hari	1	Sedang	0,3	E	KJ	E	E	E	Valid
	2	Mudah	0,4	KJ	TE	E	E	E	Valid
	3	Mudah	0,2	E	E	KJ	TE	TE	Valid
	4	Sedang	0,5	E	E	E	TE	KJ	Valid
	5	Sedang	0,4	KJ	E	TE	E	TE	Valid

4.2 Pembahasan

Berdasarkan hasil penelitian di atas, dapat ditarik kesimpulan bahwa nilai daya beda yang berada di bawah 0 atau minus sudah pasti soal tersebut tidak valid. Jumlah daya beda yang bernilai kurang dari sama dengan 0 adalah sebanyak 98 dari 460 soal yang diuji. 98 butir soal ini bersifat tidak valid, sehingga butir soal harus diperbaiki/diganti. Daya beda yang memiliki nilai minus berarti jumlah mahasiswa di kelompok bawah yang menjawab soal dengan benar lebih banyak daripada jumlah mahasiswa di kelompok atas yang menjawab soal dengan benar. Butir soal tersebut dapat dikatakan tidak baik karena tidak dapat membedakan mahasiswa yang memiliki pengetahuan tinggi dengan mahasiswa yang memiliki pengetahuan rendah. Nilai validitasnya pun sudah pasti memiliki nilai di bawah r tabel atau dapat dikatakan bahwa soal tersebut tidak valid.

Kesimpulan lainnya adalah apabila seluruh mahasiswa dapat menjawab soal dengan benar, taraf kesukaran dari soal tersebut akan bernilai 1. Nilai 1 menunjukkan bahwa soal tersebut termasuk kategori mudah. Seluruh mahasiswa

menjawab soal dengan benar berarti distraktor pada soal tersebut tidak ada yang efektif. Nilai validitasnya pun sudah pasti memiliki nilai di bawah r tabel atau dapat dikatakan bahwa soal tersebut tidak valid.

Pada pengujian validitas butir soal, butir soal pada sebuah indikator perlu diuji berulang kali. Apabila sebuah soal bersifat tidak valid, soal tersebut dapat diperbaiki kalimatnya atau diganti dengan butir soal yang baru. Setelah itu, butir soal dapat diujikan kembali kepada mahasiswa untuk mengetahui nilai validitasnya. Jumlah soal yang valid adalah 285 soal dari 460 soal yang diuji.

Setelah melalui uji validitas, terdapat satu soal yang valid namun memiliki daya beda yang bernilai 0, sehingga soal tersebut tidak digunakan pada bank soal mata kuliah kriptografi.

Jumlah persentase pengecoh jawaban pada bank soal mata kuliah kriptografi yang bersifat efektif adalah sebesar 79,75%. Nilai ini didapat dari jumlah pengecoh efektif yaitu 906 dibagi dengan jumlah jawaban pengecoh yaitu 1136. Jumlah soal yang bersifat mudah pada bank soal mata kuliah kriptografi adalah 64 soal, sedangkan soal yang bersifat sukar sebanyak 45 soal. Soal yang bersifat sedang pada bank soal mata kuliah kriptografi adalah 175 soal.

BAB V

Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan, maka kesimpulan yang diambil sebagai berikut:

1. Untuk membuat sebuah bank soal, butir soal harus terlebih dahulu dilakukan uji taraf kesukaran, daya beda, efektivitas pengecoh, dan validitas butir soal. Hasil uji taraf kesukaran pada bank soal mata kuliah kriptografi adalah 64 soal bersifat mudah, 45 soal bersifat sukar, dan 175 soal bersifat sedang. Sebuah soal sebaiknya bersifat sedang. Jumlah persentase soal yang bersifat sedang pada bank soal mata kuliah kriptografi adalah 61,6 %. Dalam beberapa situasi, taraf kesukaran soal yang bersifat sedang tidak selalu harus digunakan. Contohnya adalah penggunaan soal yang bersifat mudah dan sukar digunakan untuk mengukur tingkat pengetahuan mahasiswa pada sebuah materi.
2. Hasil uji daya beda pada bank soal mata kuliah kriptografi adalah 284 soal memiliki daya beda positif. Jumlah daya beda yang bernilai kurang dari sama dengan 0 adalah sebanyak 98 soal yang terdiri dari 44 soal memiliki daya beda yang bernilai minus dan 54 soal memiliki daya beda yang bernilai 0.

3. Persentase pengecoh soal yang bersifat efektif pada bank soal mata kuliah kriptografi adalah 79,75%. Jumlah pengecoh soal yang bersifat efektif pada bank soal mata kuliah kriptografi adalah 906 soal, sedangkan jumlah keseluruhan jawaban pengecoh adalah 1136 soal.
4. Berdasarkan uji validitas, terdapat 285 soal yang bersifat valid. Setelah dilakukan pengecekan, terdapat 1 soal valid dengan daya beda yang bernilai 0. Soal tersebut tidak digunakan pada bank soal mata kuliah kriptografi karena soal tersebut tidak dapat membedakan mahasiswa yang memiliki pengetahuan tinggi dengan mahasiswa yang memiliki pengetahuan rendah.

5.2 Saran

Berdasarkan pembahasan dan simpulan di atas, maka perumusan saran adalah sebagai berikut:

1. Jumlah sampel mahasiswa untuk pengujian taraf kesukaran, daya beda, efektivitas pengecoh, dan validitas butir soal sebaiknya ditambah.
2. Apabila terdapat perubahan materi ajar pada mata kuliah kriptografi, bank soal perlu diperbaharui kembali sesuai materi ajar yang berlaku.
3. Bank soal mata kuliah kriptografi dapat dikembangkan lagi menjadi bank soal pada ujian online kriptografi. Untuk itu, diperlukan aplikasi yang dapat menunjang proses belajar yang baik dengan melakukan evaluasi hasil belajar menggunakan bank soal mata kuliah kriptografi

DAFTAR PUSTAKA

Anastasia, A. dan Urbina, S. 1997. *Tes Psikologi, Edisi Bahasa Indonesia*. Jakarta: PT Prenhalindo.

Arikunto, Suharsimi. 2002. *Dasar-Dasar Evaluasi Pendidikan (Edisi Revisi)*. Jakarta: PT Bumi Aksara

Crocker, Linda dan Algina, James. 1986. *Introduction to Classical and Modern Test Theory*. USA: Cengage Learning.

Darminto, Dwi Prastowo dan Julianty, Rifka. 2002. *Analisis Laporan Keuangan*. Yogyakarta: YKPN.

Departemen Pendidikan Nasional. 2005. *Kamus Besar Bahasa Indonesia Edisi Ketiga*. Jakarta: Balai Pustaka

Kromodimoeljo, Sentot. 2010. *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consulting

Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A. 1996. *Handbook of Applied Cryptography*. USA: Press, Inc.

Purwanto. 2009. *Evaluasi Hasil Belajar*. Yogyakarta: Pustaka Pelajar

Schneier, Bruce. 1996. *Applied Cryptography, Second Edition*. USA: Wiley Computer Publishing, John Wiley & Sons, Inc.

Stallings, William. 2006. *Cryptography and Network Security Principles and Practice Fifth Edition*. New York: Pearson Education, Inc.

Sudjana, Nana. 1990. *Dasar-dasar Proses Belajar Mengajar*. Bandung: Sinar Baru.

Tim Redaksi Kanisius. 2010. *Paradigma Pedagogi Reflektif*. Bekasi: Kanisius.

Tynan, Bernadette. 2004. *Melatih Anak Berpikir seperti Jenius*. Jakarta: Gramedia Pustaka Utama

Usman, Husaini dan Setiady Akbar, Purnomo. 1996. *Metodologi Penelitian Sosial*. Jakarta: PT Bumi Aksara

Lampiran 1: Kisi-kisi Instrumen Pengujian Tahap I

Universitas : Universitas Negeri Jakarta

Mata Kuliah : Kriptografi

Alokasi Waktu: 60 menit

Jumlah Soal : 30

Bentuk Soal : Pilihan Ganda

No.	Materi Pokok	Indikator	Paket Soal	Nomor Soal	Taksonomi Bloom
1	Pengantar kriptografi	Mahasiswa dapat mendeskripsikan terminologi kriptografi	A	1, 2	C1
			B	1	
			C	1	
			D	1, 2	
		Mahasiswa dapat mengidentifikasikan tujuan kriptografi	A	3	C1
			B	2	
			C	2, 3	
			D	3	
		Mahasiswa dapat menyebutkan sejarah kriptografi	A	4	C1
			B	3, 4	
			C	4, 5	
			D	4	
		Mahasiswa dapat mendefinisikan pengertian dari kriptanalisis	A	5	C1
			B	5, 6	
			C	6	
			D	5	
		Mahasiswa dapat mengidentifikasikan perbedaan antara kriptografi kunci simetris dengan kriptografi kunci asimetris	A	6	C1
			B	7	
			C	7	
			D	6, 7	
2	Serangan terhadap kriptografi	Mahasiswa dapat menjelaskan fungsi keamanan algoritma kriptografi	A	7, 8	C2
			B	8	
			C	8	
			D	8	
		Mahasiswa dapat menyebutkan jenis-jenis serangan terhadap kriptografi	A	9	C1
			B	9, 10	
			C	9, 10	
			D	9	
		Mahasiswa dapat mengidentifikasikan kompleksitas serangan terhadap kriptografi	A	10, 11	C1
			B	11	
			C	11	
			D	10	

No.	Materi Pokok	Indikator	Paket Soal	Nomor Soal	Taksonomi Bloom
3	Landasan matematika pada kriptografi	Mahasiswa dapat menerapkan penggunaan fungsi matematika pada kriptografi	A	12	C3
			B	12	
			C	12	
			D	11, 12	
		Mahasiswa dapat menghitung fungsi permutasi	A	13	C3
			B	13	
			C	13	
			D	13, 14	
		Mahasiswa dapat menghitung fungsi kombinasi	A	14, 15	C3
			B	14	
			C	14	
			D	15	
		Mahasiswa dapat menerapkan teori peluang	A	16	C3
			B	15	
			C	15, 16	
			D	16	
		Mahasiswa dapat menerapkan teori bilangan	A	17	C3
			B	16, 17	
			C	17	
			D	17	
4	Algoritma kriptografi klasik	Mahasiswa dapat mengplikasikan algoritma *cipher* subtitusi	A	18	C3
			B	18, 19	
			C	18, 19	
			D	18	
		Mahasiswa dapat mengplikasikan algoritma *cipher* transposisi	A	19, 20	C3
			B	20	
			C	20	
			D	19, 20	
		Mahasiswa dapat mengplikasikan algoritma *affine cipher*	A	21	C3
			B	21	
			C	21	
			D	21, 22	
		Mahasiswa dapat mengplikasikan algoritma *vigenere*	A	22	C3
			B	22, 23	
			C	22, 23	
			D	23	
		Mahasiswa dapat mengplikasikan algoritma *playfair*	A	23, 24	C3
			B	24	
			C	24	
			D	24	

No.	Materi Pokok	Indikator	Paket Soal	Nomor Soal	Taksonomi Bloom
		Mahasiswa dapat mengaplikasikan algoritma *one-time pad*	A	25	C3
			B	25, 26	
			C	25	
			D	25	
5	Algoritma kriptografi modern	Mahasiswa dapat menerapkan rangkaian bit dan operasinya	A	26	C3
			B	27	
			C	26	
			D	26, 27	
		Mahasiswa dapat menerapkan algoritma enkripsi dengan XOR sederhana	A	27, 28	C3
			B	28	
			C	27, 28	
			D	28	
		Mahasiswa dapat mengoperasikan pembangkitan kunci	A	29	C3
			B	29	
			C	29, 30	
			D	29	
		Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	A	30	C1
			B	30	
			C	-	
			D	30	

Lampiran 2: Validitas Butir Paket Soal A

Indikator	Soal	Validitas Butir
Mahasiswa dapat mendeskripsikan terminologi kriptografi	Pesan berupa teks, gambar, audio, video dalam kriptografi disebut... a. Cipherteks d. Dekripsi b. Plainteks e. Kunci algoritma c. Enkripsi	
	Pesan yang telah disandikan sehingga tidak memiliki makna disebut.. a. Cipherteks d. Dekripsi b. Plainteks e. Kunci algoritma c. Enkripsi	
Mahasiswa dapat mengidentifikasikan tujuan kriptografi	Layanan yang berhubungan dengan penjagaan dari perubahan data secara tidak sah mendefinisikan tujuan kriptografi berupa... a. Kerahasiaan d. Non-repudiasi b. Integritas data e.Ketepatan waktu c. Autentikasi	
Mahasiswa dapat menyebutkan sejarah kriptografi	Buku yang berisikan tentang penjelasan teknik analisis frekuensi kriptanalisis yang pertama kalinya pada abad 9 M berjudul... a. *Scytale* d. *Al-Kindi* b. *Hieroglyphics* e. *Steganografi* c. *Risalah fi Istikhraj al-Mu'amma*	
Mahasiswa dapat mendefinisikan pengertian dari kriptanalisis	Istilah yang digunakan untuk mempelajari metode untuk memperoleh arti dari informasi enkripsi tanpa mengakses sandi secara normal yang dibutuhkan untuk melakukannya adalah.. a. Kriptografi d. Kriptanalis b. Kriptografer e. Kriptologi c. Kriptanalisis	
Mahasiswa dapat mengidentifikasikan perbedaan antara kriptografi kunci simetris dengan kriptografi kunci asimetris	Termasuk jenis kunci manakah apabila kunci yang digunakan pada proses enkripsi dan dekripsi berbeda... a. Kunci simetris d. Kunci asimetris b. Kunci substitusi e. Kunci kombinasi c. Kunci transposisi	
Mahasiswa dapat menjelaskanfungsi keamanan algoritma kriptografi	Menurut Lars Knudsen, kriptanalis menemukan kunci K sehingga Dekripsi $D_K(C)=P$ termasuk ke dalam hasil kriptanalisis kategori... a. Induksi parsial d. Deduksi total b. Deduksi informasi e. Pemecahan total c. Deduksi global	

Indikator	Soal	Validitas Butir
	Sebuah algoritma kriptografi dikatakan aman mutlak tanpa syarat (*unconditionally secure*) apabila... a. Cipherteks yang dihasilkan tidak mengandung cukup informasi untuk menentukan plainteksnya b. Kunci yang digunakan pada proses enkripsi bersifat privat dan hanya diketahui oleh pengirim pesan c. Kunci yang digunakan pada proses dekripsi bersifat privat dan hanya diketahui oleh penerima pesan d. Hasil cipherteks lebih panjang dan rumit dari plainteks sebelumnya e. Data algortima pada proses enkripsi dan dekripsi tidak mudah untuk dipecahkan	
Mahasiswa dapat menyebutkan jenis-jenis serangan terhadap kriptografi	Di bawah ini yang termasuk *passive attack* menurut William Stallings adalah... a. *Masquerade* d. *Modification of Message* b. *Replay* e. *Denial of Service* c. *Release of Message Content*	
Mahasiswa dapat mengidentifikasikan kompleksitas serangan terhadap kriptografi	Semakin lama waktu yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut merupakan kompleksitas serangan yang diukur berdasarkan... a. Kompleksitas memori d. Kompleksitas waktu b. Kompleksitas kunci e. Kompleksitas cipherteks c. Kompleksitas data	
	Semakin banyak memori yang dibutuhkan untuk melakukan serangan berarti semakin bagus sistem kriptografi tersebut merupakan kompleksitas serangan yang diukur berdasarkan... a. Kompleksitas memori d. Kompleksitas waktu b. Kompleksitas kunci e. Kompleksitas cipherteks c. Kompleksitas data	
Mahasiswa dapat menerapkan penggunaan fungsi matematika pada kriptografi	Fungsi matematika untuk plainteks Caesar Cipher yang digeser 3 ke kiri adalah... a. E(P-3) d. E(C+3) b. D(C-3) e. D(E) c. D(C+3)	
Mahasiswa dapat menghitung fungsi permutasi	Hasil dari P_3^7 adalah... a. 210 d. 60 b. 30 e. 120 c. 12	
Mahasiswa dapat menghitung fungsi kombinasi	Hasil dari C_4^8 adalah... a. 84 d. 28 b. 210 e. 70 c. 120	
	Hasil dari C_7^{10} adalah... a. 84 d. 28 b. 210 e. 70 c. 120	

Indikator	Soal	Validitas Butir
Mahasiswa dapat menerapkan teori peluang	Apabila terdapat sebuah kunci yang berisikan 2 huruf (huruf boleh sama dan tidak) dari jumlah alfabet, peluang untuk mendapatkan kunci yang benar adalah... a. 0,01331 d. 0,001479 b. 0,01775 e. 0,004438 c. 0,01479	
Mahasiswa dapat menerapkan teori bilangan	Hasil pembulatan dari bilangan 9,1706 dengan 2 angka penting adalah... a. 9 d. 9,18 b. 9,2 e. 9,1 c. 9,17	
Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi	Plainteks dari "XEVCGBTENSV" yang menggunakan aturan ROT 13 adalah... a. KRIPTOGRAFI d. INFORMATIKA b. TRANSPOSISI e. CIPHERTEKS c. PENDIDIKAN	
Mahasiswa dapat mengaplikasikan algoritma *cipher* transposisi	Cipherteks dari " 5 TEKNIK DASAR KRIPTOGRAFI" yang menggunakan aturan *blocking* berupa 7 blok adalah... a. 5G_KKTIPGOIFRO_TDRDSA_AAEKII b. GK5DS_KPIOTFRSA__EDNKIIDRAKR c. IFAKROTIDRAS5__EKKRN_GRTIPAT d. KG5__KTRARDIAET_ANIPSKFIORT e. 5K_G__KRTDRAEAIFKSPINAT_IRO_	
	Cipherteks dari " PROGRAM STUDI S1 PTIK UNJ" yang menggunakan aturan *blocking* berupa 6 blok adalah... a. MIPRJTI__OKSS_T_G1R_UU_NAPD__I b. IPKTJNU__DSTPGO__MA1_S_UIRR__O c. PMITJR__I_OSSK_GT1__RU_U_ADPN_ d. ITUDUJNS1S_TKPRMA_IK___GMR_O_ e. RMP_ROGN_J1US__TIDS_ASPIK_T__AI	
Mahasiswa dapat mengaplikasikan algoritma *affine cipher*	Cipherteks dari "TRANSISI" yang menggunakan algoritma *affine cipher* dengan kunci a = 5 dan b = 6 adalah... a. DEHYXSQK d. XNGTSUSU b. JMHFECIL e. CVBNMJHG c. VFRUXWSG	
Mahasiswa dapat mengaplikasikan algoritma *vigenere*	Cipherteks dari "PLAINTEKS" yang menggunakan algoritma *vigenere* dengan kuci "ILMU" adalah... a. XWMCVEQEA d. PNMEIGKCX b. LITBNRGQX e. STXPLOQYV c. RIKRSNMWZ	

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengaplikasikan algoritma *playfair*	Cipherteks dari "ALGORITMA PLAYFAIR" yang menggunakan algoritma *playfair* dengan kunci "KOMPUTER" adalah... a. GANLPTILMTQKEKFARGSV b. EQDPTNRKGAQEXGTQBX c. MTQKEKFARGVTQEILUV d. DALFLCVTRQCVOKQL e. ERMIVTLQDMFRBEVTBY	
	Cipherteks dari "KRIPTOGRAFI KLASIK" yang menggunakan algoritma *playfair* dengan kunci "KOMPUTER" adalah... a. GANLPTILMTQKEKFARGSV b. EQDPTNRKGAQEXGTQBX c. MTQKEKFARGVTQEILUV d. DALFLCVTRQCVOKQL e. ERMIVTLQDMFRBEVTBY	
Mahasiswa dapat mengaplikasikan algoritma *one-time pad*	Cipherteks dari "KOMUNIKASI" yang menggunakan algoritma *one-time pad* dengan kunci "ASDFGHJKLP" adalah... a. FTBWIPMFRT d. IOMNFRDCAZ b. DKOTRVFCHU e. LHQAUQULEG c. TRBNJGFWQK	
Mahasiswa dapat menerapkan rangkaian bit dan operasinya	Plainteks "101101101101" yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu... a. A 6 5 d. 8 6 D b. E 5 C e. 1 7 9 c. 7 3 8	
Mahasiswa dapat menerapkan algoritma enkripsi dengan XOR sederhana	Cipherteks dari 11010 dengan kunci 11100 adalah... a. 11011 d. 01011 b. 00001 e. 01101 c. 00110	
	Cipherteks dari 00110 dengan kunci 01101 adalah... a. 11011 d. 01011 b. 00001 e. 01101 c. 00110	
Mahasiswa dapat mengoperasikan pembangkitan kunci	Salah satu masalah pembangkitan kunci pada algoritma kunci publik adalah... a. Membutuhkan perhitungan matematis yang rumit b. Membutuhkan memori yang besar c. Membutuhkan data yang beragam d. Membutuhkan waktu yang lama e. Membutuhkan kriptanalis yang handal	

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	1) 56 bit 2) 128 bit 3) 192 bit 4) 256 bit Dari jumlah bit di atas, jumlah bit yang dapat digunakan oleh kunci DES adalah... a. 3) d. 3) dan 4) b. 1) dan 2) e. 2), 3), dan 4) c. 1)	

Dosen Pengampu

Prasetyo Wibowo Yunanto, M.Eng

Lampiran 1: Paket Soal A

1. Pesan berupa teks, gambar, audio, video dalam kriptografi disebut...
   a. Cipherteks
   b. Plainteks
   c. Enkripsi
   d. Dekripsi
   e. Kunci algoritma
2. Pesan yang telah disandikan sehingga tidak memiliki makna disebut..
   a. Cipherteks
   b. Plainteks
   c. Enkripsi
   d. Dekripsi
   e. Kunci algoritma
3. Layanan yang berhubungan dengan penjagaan dari perubahan data secara tidak sah mendefinisikan tujuan kriptografi berupa...
   a. Kerahasiaan
   b. Integritas data
   c. Autentikasi
   d. Non-repudiasi
   e. Ketepatan waktu
4. Buku yang berisikan tentang penjelasan teknik analisis frekuensi kriptanalisis yang pertama kalinya pada abad 9 M berjudul...
   a. *Scytale*
   b. *Hieroglyphics*
   c. *Risalah fi Istikhraj al-Mu'amma*
   d. *Al-Kindi*
   e. *Steganografi*
5. Istilah yang digunakan untuk mempelajari metode untuk memperoleh arti dari informasi enkripsi tanpa mengakses sandi secara normal yang dibutuhkan untuk melakukannya adalah..
   a. Kriptografi
   b. Kriptografer
   c. Kriptanalisis
   d. Kriptanalis
   e. Kriptologi
6. Termasuk jenis kunci manakah apabila kunci yang digunakan pada proses enkripsi dan dekripsi berbeda...
   a. Kunci simetris
   b. Kunci substitusi
   c. Kunci transposisi
   d. Kunci asimetris
   e. Kunci kombinasi
7. Menurut Lars Knudsen, kriptanalis menemukan kunci K sehingga Dekripsi $D_K(C)=P$ termasuk ke dalam hasil kriptanalisis kategori...
   a. Induksi parsial
   b. Deduksi informasi
   c. Deduksi global
   d. Deduksi total
   e. Pemecahan total
8. Sebuah algoritma kriptografi dikatakan aman mutlak tanpa syarat (*unconditionally secure*) apabila...
   a. Cipherteks yang dihasilkan tidak mengandung cukup informasi untuk menentukan plainteksnya
   b. Kunci yang digunakan pada proses enkripsi bersifat privat dan hanya diketahui oleh pengirim pesan
   c. Kunci yang digunakan pada proses dekripsi bersifat privat dan hanya diketahui oleh penerima pesan

d. Hasil cipherteks lebih panjang dan rumit dari plainteks sebelumnya
e. Data algortima pada proses enkripsi dan dekripsi tidak mudah untuk dipecahkan

9. Di bawah ini yang termasuk *passive attack* menurut William Stallings adalah...
   a. *Masquerade*
   b. *Replay*
   c. *Release of Message Content*
   d. *Modification of Message*
   e. *Denial of Service*
10. Semakin lama waktu yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut merupakan kompleksitas serangan yang diukur berdasarkan...
    a. Kompleksitas memori
    b. Kompleksitas kunci
    c. Kompleksitas data
    d. Kompleksitas waktu
    e. Kompleksitas cipherteks
11. Semakin banyak memori yang dibutuhkan untuk melakukan serangan berarti semakin bagus sistem kriptografi tersebut merupakan kompleksitas serangan yang diukur berdasarkan...
    a. Kompleksitas memori
    b. Kompleksitas kunci
    c. Kompleksitas data
    d. Kompleksitas waktu
    e. Kompleksitas cipherteks
12. Fungsi matematika untuk plainteks Caesar Cipher yang digeser 3 ke kiri adalah...
    a. E(P-3)
    b. D(C-3)
    c. D(C+3)
    d. E(C+3)
    e. D(E)
13. Hasil dari P_3^7 adalah...
    a. 210
    b. 30
    c. 12
    d. 60
    e. 120
14. Hasil dari C_4^8 adalah...
    a. 84
    b. 210
    c. 120
    d. 28
    e. 70
15. Hasil dari C_7^{10} adalah...
    a. 84
    b. 210
    c. 120
    d. 28
    e. 70
16. Apabila terdapat sebuah kunci yang berisikan 2 huruf (huruf boleh sama dan tidak) dari jumlah alfabet, peluang untuk mendapatkan kunci yang benar adalah...
    a. 0,01331
    b. 0,01775
    c. 0,01479
    d. 0,001479
    e. 0,004438

17. Hasil pembulatan dari bilangan 9,1706 dengan 2 angka penting adalah...
    a. 9
    b. 9,2
    c. 9,17
    d. 9,18
    e. 9,1
18. Plainteks dari "XEVCGBTENSV" yang menggunakan aturan ROT 13 adalah...
    a. KRIPTOGRAFI
    b. TRANSPOSISI
    c. PENDIDIKAN
    d. INFORMATIKA
    e. CIPHERTEKS
19. Cipherteks dari " 5 TEKNIK DASAR KRIPTOGRAFI" yang menggunakan aturan *blocking* berupa 7 blok adalah...
    a. 5G_KKTIPGOIFRO_TDRDSA_AAEKII
    b. GK5DS_KPIOTFRSA__EDNKIIDRAKR
    c. IFAKROTIDRAS5__EKKRN_GRTIPAT
    d. KG5__KTRARDIAET_ANIPSKFIORT
    e. 5K_G__KRTDRAEAIFKSPINAT_IRO_
20. Cipherteks dari " PROGRAM STUDI S1 PTIK UNJ" yang menggunakan aturan *blocking* berupa 6 blok adalah...
    a. MIPRJTI__OKSS_T_G1R_UU_NAPD__I
    b. IPKTJNU__DSTPGO__MA1_S_UIRR__O
    c. PMITJR__I_OSSK_GT1__RU_U_ADPN_
    d. ITUDUJNS1S_TKPRMA_IK___GMR_O_
    e. RMP_ROGN_J1US__TIDS_ASPIK_T__AI
21. Cipherteks dari "TRANSISI" yang menggunakan algoritma *affine cipher* dengan kunci a = 5 dan b = 6 adalah...
    a. DEHYXSQK
    b. JMHFECIL
    c. VFRUXWSG
    d. XNGTSUSU
    e. CVBNMJHG
22. Cipherteks dari "PLAINTEKS" yang menggunakan algoritma *vigenere* dengan kuci "ILMU" adalah...
    a. XWMCVEQEA
    b. LITBNRGQX
    c. RIKRSNMWZ
    d. PNMEIGKCX
    e. STXPLOQYV
23. Cipherteks dari "ALGORITMA PLAYFAIR" yang menggunakan algoritma *playfair* dengan kunci "KOMPUTER" adalah...
    a. GANLPTILMTQKEKFARGSV
    b. EQDPTNRKGAQEXGTQBX
    c. MTQKEKFARGVTQEILUV
    d. DALFLCVTRQCVOKQL
    e. ERMIVTLQDMFRBEVTBY
24. Cipherteks dari "KRIPTOGRAFI KLASIK" yang menggunakan algoritma *playfair* dengan kunci "KOMPUTER" adalah...
    a. GANLPTILMTQKEKFARGSV
    b. EQDPTNRKGAQEXGTQBX
    c. MTQKEKFARGVTQEILUV

d. DALFLCVTRQCVOKQL
e. ERMIVTLQDMFRBEVTBY

25. Cipherteks dari “KOMUNIKASI” yang menggunakan algoritma *one-time pad* dengan kunci “ASDFGHJKLP” adalah...
    a. FTBWIPMFRT
    b. DKOTRVFCHU
    c. TRBNJGFWQK
    d. IOMNFRDCAZ
    e. LHQAUQULEG
26. Plainteks “101101101101” yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu...
    a. A 6 5
    b. E 5 C
    c. 7 3 8
    d. 8 6 D
    e. 1 7 9
27. Cipherteks dari 11010 dengan kunci 11100 adalah...
    a. 11011
    b. 00001
    c. 00110
    d. 01011
    e. 01101
28. Cipherteks dari 00110 dengan kunci 01101 adalah...
    a. 11011
    b. 00001
    c. 00110
    d. 01011
    e. 01101
29. Salah satu masalah pembangkitan kunci pada algoritma kunci publik adalah...
    a. Membutuhkan perhitungan matematis yang rumit
    b. Membutuhkan memori yang besar
    c. Membutuhkan data yang beragam
    d. Membutuhkan waktu yang lama
    e. Membutuhkan kriptanalis yang handal
30. 1) 56 bit
    2) 128 bit
    3) 192 bit
    4) 256 bit
    Dari jumlah bit di atas, jumlah bit yang dapat digunakan oleh kunci DES adalah...
    a. 3)
    b. 1) dan 2)
    c. 1)
    d. 3) dan 4)
    e. 2), 3), dan 4)

Lampiran 4: Perhitungan Hasil Analisis Butir Soal untuk Paket A

VALIDITAS BUTIR SOAL PILIHAN GANDA dengan Korelasi Produk Moment

Taraf Signifikan = 5%

NO	Nama	Butir Soal																													Skor Total (Y)	Y2	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	Vina Sepnani	1	1	0	1	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	23	529	
2	M. Elmodio Maldini	1	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	0	0	1	0	0	1	13	169	
3	M. Rayhan Haroki	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	25	625	
4	Ilyas Rahmanda	1	1	1	1	1	1	0	0	1	0	0	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	1	21	441	
5	Gatis Lestiana	1	0	1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1	22	484	
6	Moctar Afendi	1	1	0	0	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	0	1	21	441	
7	Nurul Indah Prabawati	1	1	0	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	0	1	1	1	0	0	1	1	0	1	18	324	
8	Nur M. Nabil	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	1	0	1	0	0	1	1	0	1	18	324	
9	Mohammad Dwi F.	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	0	0	0	1	1	1	1	0	0	15	225	
10	Mentari Diyah Utami	0	1	1	0	1	1	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	12	144	
11	Silka Nayah	0	0	1	0	0	1	0	0	0	1	1	0	1	1	1	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0	13	169	
12	Sarah Lutfiah	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0	1	1	1	0	0	19	361	
13	Muhamad Syahrizal	1	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	1	1	1	1	15	225	
14	Iis Sumarni	0	1	0	1	1	1	0	0	1	1	1	0	1	1	1	0	1	1	1	1	0	0	1	1	0	0	1	0	0	0	17	289	
15	Humairoh Desreini	1	1	0	0	0	1	0	0	0	1	1	0	1	1	1	0	0	1	1	1	1	1	0	0	0	0	1	1	1	0	16	256	
16	Reva Siti Ardhita	0	1	0	0	0	1	0	0	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	0	1	0	0	1	1	0	15	225	
17	Reza Ridwansyah	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1	1	0	0	1	1	15	225	
18	R. Andi Rahmadi	1	1	0	0	0	0	1	0	1	0	0	1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1	1	0	14	196	
19	Much Ade T. Oktora	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	0	0	0	1	1	1	0	0	11	121	
20	Rizky Swandani	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	1	0	1	1	0	0	1	1	0	0	10	100	
	Benar (∑X)	14	17	7	6	10	16	6	3	6	11	11	8	14	13	14	3	10	20	20	20	12	11	6	9	8	9	17	14	7	11	333	5873	110889
	Salah	6	3	13	14	10	4	14	17	14	9	9	12	6	7	6	17	10	0	0	0	8	9	14	11	12	11	3	6	13	9			
	∑XY	255	288	120	123	188	285	109	55	118	204	204	135	253	225	250	65	162	333	333	333	203	189	101	175	157	172	281	233	120	204			
	rxy	0,590	0,171	0,089	0,622	0,530	0,574	0,245	0,174	0,487	0,517	0,517	0,045	0,536	0,221	0,455	0,520	-0,111	#DIV/0!	#DIV/0!	#DIV/0!	0,081	0,145	0,030	0,624	0,599	0,549	-0,071	-0,003	0,089	0,517			
	R Tabel	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444			
	Keterangan	Valid	Tidak Vali	Tidak Vali	Valid	Valid	Valid	Tidak Vali	Tidak Vali	Valid	Valid	Valid	Tidak Vali	Valid	Tidak Vali	Valid	Valid	Tidak Vali	#DIV/0!	#DIV/0!	#DIV/0!	Tidak Vali	Tidak Vali	Tidak Vali	Valid	Valid	Valid	Tidak Vali	Tidak Vali	Tidak Vali	Valid			
	Tingkat Kesukaran	0,7	0,85	0,35	0,3	0,5	0,8	0,3	0,15	0,3	0,55	0,55	0,4	0,7	0,65	0,7	0,15	0,5	1	1	1	0,6	0,55	0,3	0,45	0,4	0,45	0,85	0,7	0,35	0,55			
	Indeks	Mudah	Mudah	Sedang	Sedang	Sedang	Mudah	Sedang	Sukar	Sedang	Sedang	Sedang	Sedang	Mudah	Sedang	Mudah	Sukar	Sedang	Mudah	Mudah	Mudah	Sedang	Sedang	Sedang	Sedang	Sedang	Sedang	Mudah	Mudah	Sedang	Sedang			

DATA KELOMPOK ATAS

NO	Nama	Butir Soal																													Skor Total (Y)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
1	M. Rayhan Haroki	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	25
2	Vina Sepnani	1	1	0	1	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	1	23
3	Gatis Lestiana	1	0	1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	1	1	22
4	Ilyas Rahmanda	1	1	1	1	1	1	0	0	1	0	0	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	0	1	21
5	Moctar Afendi	1	1	0	0	1	1	0	0	1	1	1	0	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	0	1	21
6	Sarah Lutfiah	1	1	1	0	1	1	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0	1	1	1	0	0	19
7	Nurul Indah Prabawati	1	1	0	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	0	1	1	1	0	0	1	1	0	1	18
8	Nur M. Nabil	1	1	1	0	0	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	1	0	1	0	0	1	1	0	1	18
9	Iis Sumarni	0	1	0	1	1	1	0	0	1	1	1	0	1	1	1	0	1	1	1	1	0	0	1	1	0	0	1	0	0	0	17
10	Humairoh Desreini	1	1	0	0	0	1	0	0	0	1	1	0	1	1	1	0	0	1	1	1	1	1	0	0	0	0	1	1	1	0	16
	Total Benar	9	9	4	5	7	10	3	1	5	8	8	4	10	8	10	3	5	10	10	10	6	6	4	8	5	6	9	7	3	7	200

DATA KELOMPOK BAWAH

NO	Nama	Butir Soal																													Skor Total
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
1	Reva Siti Ardhita	0	1	0	0	0	1	0	0	0	1	1	1	1	1	1	0	0	1	1	1	1	0	0	0	1	0	0	1	1	0	15
2	Mohammad Dwi F.	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	1	1	1	1	1	0	0	0	1	1	1	1	0	0	15
3	Muhamad Syahrizal	1	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1	0	1	0	0	0	0	1	1	1	1	15
4	Reza Ridwansyah	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	1	1	0	0	1	1	15
5	R. Andi Rahmadi	1	1	0	0	0	0	1	0	1	0	0	1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	1	1	1	0	14
6	M. Elmodio Maldini	1	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	0	0	1	0	0	1	13
7	Silka Nayah	0	0	1	0	0	1	0	0	0	1	1	0	1	1	1	0	0	1	1	1	0	0	0	0	0	0	1	1	0	1	13
8	Mentari Diyah Utami	0	1	1	0	1	1	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	12
9	Much Ade T. Oktora	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	1	1	1	1	0	0	0	1	1	1	0	0	11
10	Rizky Swandani	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	1	0	1	1	0	0	1	1	0	0	10
	Total Benar	5	8	3	1	3	6	3	2	1	3	3	4	4	5	4	0	5	10	10	10	6	5	2	1	3	3	8	7	4	4	133
	Daya Beda	0,4	0,1	0,1	0,4	0,4	0,4	0	-0,1	0,4	0,5	0,5	0	0,6	0,3	0,6	0,3	0	0	0	0	0	0,1	0,2	0,7	0,2	0,3	0,1	0	-0,1	0,3			

Butir Soal Nomor 1

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	9	0	1	0	0	10
Kelompok Bawah	3	5	0	2	0	0	10
Jumlah	3	14	0	3	0	0	20

Butir Soal Nomor 2

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	9	0	1	0	0	0	10
Kelompok Bawah	8	2	0	0	0	0	10
Jumlah	17	2	1	0	0	0	20

Butir Soal Nomor 3

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	3	4	2	1	0	0	10
Kelompok Bawah	5	3	2	0	0	0	10
Jumlah	8	7	4	1	0	0	20

Butir Soal Nomor 4

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	1	5	0	3	0	10
Kelompok Bawah	2	2	1	1	4	0	10
Jumlah	3	3	6	1	7	0	20

Butir Soal Nomor 5

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	3	0	7	0	0	0	10
Kelompok Bawah	2	0	3	2	3	0	10
Jumlah	5	0	10	2	3	0	20

Butir Soal Nomor 6

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	10	0	0	10
Kelompok Bawah	0	2	0	6	2	0	10
Jumlah	0	2	0	16	2	0	20

Butir Soal Nomor 7

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	3	2	0	1	4	0	10
Kelompok Bawah	3	3	0	1	3	0	10
Jumlah	6	5	0	2	7	0	20

Butir Soal Nomor 8

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	2	2	1	1	4	0	10
Kelompok Bawah	2	0	3	0	5	0	10
Jumlah	4	2	4	1	9	0	20

Butir Soal Nomor 9

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	1	5	2	1	0	10
Kelompok Bawah	2	1	1	4	2	0	10
Jumlah	3	2	6	6	3	0	20

Butir Soal Nomor 10

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	1	0	8	1	0	10
Kelompok Bawah	0	5	0	3	2	0	10
Jumlah	0	6	0	11	3	0	20

Butir Soal Nomor 11

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	1	1	0	0	0	10
Kelompok Bawah	3	1	6	0	0	0	10
Jumlah	11	2	7	0	0	0	20

Butir Soal Nomor 12

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	7	3	0	0	0	0	10
Kelompok Bawah	2	4	2	2	0	0	10
Jumlah	9	7	2	2	0	0	20

Butir Soal Nomor 13

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	10	0	0	0	0	0	10
Kelompok Bawah	4	1	1	2	2	0	10
Jumlah	14	1	1	2	2	0	20

Butir Soal Nomor 14

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	2	0	0	0	8	0	10
Kelompok Bawah	0	2	1	2	5	0	10
Jumlah	2	2	1	2	13	0	20

Butir Soal Nomor 15

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	10	0	0	0	10
Kelompok Bawah	0	2	4	2	2	0	10
Jumlah	0	2	14	2	2	0	20

Butir Soal Nomor 16

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	1	4	3	1	0	10
Kelompok Bawah	1	1	4	0	4	0	10
Jumlah	2	2	8	3	5	0	20

Butir Soal Nomor 17

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	5	4	0	1	0	10
Kelompok Bawah	0	5	2	3	0	0	10
Jumlah	0	10	6	3	1	0	20

Butir Soal Nomor 18

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	10	0	0	0	0	0	10
Kelompok Bawah	10	0	0	0	0	0	10
Jumlah	20	0	0	0	0	0	20

Butir Soal Nomor 19

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	0	0	10	0	10
Kelompok Bawah	0	0	0	0	10	0	10
Jumlah	0	0	0	0	20	0	20

Butir Soal Nomor 20

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	10	0	0	0	10
Kelompok Bawah	0	0	10	0	0	0	10
Jumlah	0	0	20	0	0	0	20

Butir Soal Nomor 21

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	1	3	6	0	0	10
Kelompok Bawah	1	1	1	6	1	0	10
Jumlah	1	2	4	12	1	0	20

Butir Soal Nomor 22

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	3	1	0	0	0	10
Kelompok Bawah	5	1	2	2	0	0	10
Jumlah	11	4	3	2	0	0	20

Butir Soal Nomor 23

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	2	4	1	1	2	0	10
Kelompok Bawah	3	2	4	1	0	0	10
Jumlah	5	6	5	2	2	0	20

Butir Soal Nomor 24

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	1	8	0	1	0	10
Kelompok Bawah	1	2	1	4	2	0	10
Jumlah	1	3	9	4	3	0	20

Butir Soal Nomor 25

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	0	2	2	5	0	10
Kelompok Bawah	3	0	2	2	3	0	10
Jumlah	4	0	4	4	8	0	20

Butir Soal Nomor 26

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	3	0	6	0	0	10
Kelompok Bawah	3	3	0	3	1	0	10
Jumlah	4	6	0	9	1	0	20

Butir Soal Nomor 27

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	0	9	0	0	0	10
Kelompok Bawah	0	1	8	0	1	0	10
Jumlah	1	1	17	0	1	0	20

Butir Soal Nomor 28

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	2	0	0	7	1	0	10
Kelompok Bawah	3	0	1	6	0	0	10
Jumlah	5	0	1	13	1	0	20

Butir Soal Nomor 29

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	3	1	4	1	1	0	10
Kelompok Bawah	4	1	3	2	0	0	10
Jumlah	7	2	7	3	1	0	20

Butir Soal Nomor 30

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	1	7	0	2	0	10
Kelompok Bawah	0	2	4	0	4	0	10
Jumlah	0	3	11	0	6	0	20

Lampiran 5: Validitas Butir Paket Soal B

Indikator	Soal	Validitas Butir
Mahasiswa dapat mendeskripsikan terminologi kriptografi	Proses menyandikan plainteks menjadi cipherteks disebut... a. Cipherteks d. Dekripsi b. Plainteks e. Kunci algoritma c. Enkripsi	
Mahasiswa dapat mengidentifikasikan tujuan kriptografi	Di bawah ini yang bukan merupakan tujuan dari kriptografi adalah... a. Kerahasiaan d. Non-repudiasi b. Integritas data e. Ketepatan waktu c. Autentikasi	
Mahasiswa dapat menyebutkan sejarah kriptografi	Ukiran rahasia yang digunakan bangsa mesir untuk menyampaikan pesan kepada orang-orang yang berhak disebut... a. *Scytale* d. *Al-Kindi* b. *Hieroglyphics* e. *Steganografi* c. *Risalah fi Istikhraj al-Mu'amma*	
	Pita panjang berbahan daun *papyrus* yang dibaca dengan cara digulungkan ke sebatang silinder merupakan kriptografi bangsa yunani yang disebut.. a. *Scytale* d. *Al-Kindi* b. *Hieroglyphics* e. *Steganografi* c. *Risalah fi Istikhraj al-Mu'amma*	
Mahasiswa dapat mendefinisikan pengertian dari kriptanalisis	Orang yang melakukan kriptanalisis disebut... a. Kriptografi d. Kriptanalis b. Kriptografer e. Kriptologi c. Kriptanalisis	
	Ilmu yang mempelajari cara untuk memecahkan algoritma enkripsi atau implementasinya disebut.. a. Kriptografi d. Kriptanalis b. Kriptografer e. Kriptologi c. Kriptanalisis	
Mahasiswa dapat mengidentifikasikan perbedaan antara kriptografi kunci simetris dengan kriptografi kunci asimetris	1) DES dan AES 2) *Blowfish* and *Twofish* 3) 3DES 4) RSA dan ECC Pada algoritma di atas yang termasuk contoh kunci asimetris adalah... a. 1) dan 3) d. 4) b. 2) dan 3) e. 2) dan 4) c. 1)	

Indikator	Soal	Validitas Butir
Mahasiswa dapat menjelaskanfungsi keamanan algoritma kriptografi	Menurut Lars Knudsen, kriptanalis menemukan algoritma alternatif A yang ekivalen dengan $D_K(C)$ tapi tidak mengetahui kunci K termasuk ke dalam hasil kriptanalis kategori... a. Induksi parsial d. Deduksi total b. Deduksi informasi e. Pemecahan total c. Deduksi global	
Mahasiswa dapat menyebutkan jenis-jenis serangan terhadap kriptografi	**1) *Release of Message Content*** **2) *Traffic Analysis*** **3) *Masquerade*** **4) *Replay*** **5) *Modification of Message*** **Dari jenis serangan di. Pemecahan total**	

Lampiran 31: Validitas Butir Paket Soal 2

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	AES merupakan salah satu algoritma kriptografi *cipher block* dengan ukuran blok yaitu... a. 56 bit b. 128 bit c. 192 bit d. 255 bit e. 256 bit	
	Algoritma *Lucifer* telah diperbaharui menjadi algoritma DES yang kemudian digantikan kembali karena faktor keamanan yang kurang baik oleh algoritma... a. 3DES b. RC4 c. A5 d. RSA e. AES	
Mahasiswa dapat mengidentifikasikan serangan terhadap *cipher* aliran	*Keystream* yang samadigunakandua kali terhadap potongan plainteks yang berbeda dapat mengakibatkan terjadinya serangan... a. *Known-plaintext attack* b. *Known-ciphertext attack* c. *Ciphertext-only attack* d. *Plaintext-only attack* e. *Flip-bit attack*	
	Penggunaan bit-aliran-kunci yang tidak dapat diprediksi pada cipher aliran dimaksudkan untuk... a. Menghasilkan cipherteks yang sulit didekripsi b. Menghindarkan kemungkinan kriptanalis mendeduksi bit-aliran-kunci c. Membuat beberapa cipherteks yang sulit dipecahkan d. Menghasilkan kunci-kunci dengan bilangan prima acak semu e. Menghindarkan kemungkinan kriptanalis mendapatkan plainteks	
Mahasiswa dapat mengidentifikasikan *cipher* blok	1) Substitusi 2) Transposisi 3) Faktorisasi 4) Diferensiasi Teknik di atas yang **bukan** merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah... a. 1) dan 3) b. 1) dan 2) c. 2) dan 4) d. 3) dan 4) e. 4)	

Indikator	Soal	Validitas Butir
	1) *Electronic Code Book* (*ECB*) 2) *Cipher Block Chaining* (*CBC*) 3) *Cipher Feedback* (*CFC*) 4) *Output Feedback* (*OFB*) 5) *Input Feedback* (IFB) Pada mode di atas yang **bukan** merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah... a. 5) d. 2) b. 4) e. 1) c. 3)	
Mahasiswa dapat mendeskripsikan prinsip perancangan *cipher* blok	Prinsip perancangan *cipher* blok berupa *s-box* berarti... a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks c. Mengubah plainteks menjadi cipherteks diulang beberapa kali d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain	
	Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi merupakan prinsip perancangan *cipher* blok yaitu... a. *Strong key* d. *Short key* b. *Weak key* e. *Low key* c. *Long key*	
Mahasiswa dapat mengidentifikasikan algoritma RSA	$M = C^d$ mod n merupakan fungsi pada algoritma RSA untuk melakukan proses... a. Dekripsi b. Pembangkitan kunci c. Faktorisasi bilangan prima d. Enkripsi e. Pencarian bilangan prima	
	Cipherteks pada algoritma RSA bersifat... a. Simetris d. Sementara b. Privat e. Tetap c. Publik	
Mahasiswa dapat mengidentifikasikan algoritma *rabin*	Kunci dekripsi pada algoritma *Rabin* bersifat... a. Simetris d. Privat b. Sementara e. Publik c. Tetap	

Indikator	Soal	Validitas Butir
	Kunci enkripsi pada algoritma *Rabin* bersifat... a. Simetris d. Privat b. Sementara e. Publik c. Tetap	
Mahasiswa dapat menjelaskan pembangkit bilangan acak semu	Pembangkit bilangan acak yang cocok untuk kriptografi dinamakan... a. *Blum Blum Shut* b. *CryptographicallySecurePseudorandomGenerator* c. *Chaos* d. *Pseudo-RandomNumber Generator* e. *LinearCongruentialGenerator*	
	1) Nilai bilangan harus non-prima 2) Data algoritma memiliki kompleksitas yang tinggi 3) Memori yang dibutuhkan tidak terlalu besar 4) Tahan terhadap serangan yang serius Salah satu syarat sebagai pembangkit bilangan acak yang cocok untuk kriptografi ditunjukkan oleh nomor.. a. 1) d. 4) b. 2) e. Semua Benar c. 3)	
	Salah satu contoh penggunaan pembangkit bilangan acak semu yaitu untukpembangkitan parameter kuncipada... a. Algoritma kunci publik b. Algoritma kunci private c. Algoritma *cipher* transposisi d. Algoritma *cipher* substitusi e. Algoritma kunci asimetris	
	Keunggulan *Linear Congruential Generator* (LCG) terletak pada... a. Algoritmanya sulit ditembus oleh kriptanalis b. Kecepatannya dan hanya membutuhkan sedikit operasi bit c. Menggunakan algoritma operasi byte d. Tidak membutuhkan memori yang besar e. Data algoritma pada proses enkripsi tidak rumit	
Mahasiswa dapat mengidentifikasikan fungsi *hash* satu arah	Keamanan pada fungsi *hash* satu arah terletak pada... a. Logaritma diskrit yang sulit dipecahkan b. Diferensial bilangannya memiliki nilai yang besar c. Sifat satu arah dari fungsi *hash* itu sendiri d. Kerumitan algoritma pada proses enkripsi e. Penggunaan pembangkit kunci acak	

Indikator	Soal	Validitas Butir
	Salah satu contoh dari fungsi *hash* satu arah adalah... a. RC4 d. MD5 b. RSA e. AES c. A5	
Mahasiswa dapat menyebutkan algoritma MD5	Pada algoritma MD5, pengolahan pesan dilakukan dalam blok berukuran... a. 512 bit d. 64 bit b. 256 bit e. 32 bit c. 128 bit	
	Pada pengolahan pesan dalam algoritma MD5, proses H_{MD5} memiliki putaran sebanyak... a. 5 putaran d. 8 putaran b. 3 putaran e. 4 putaran c. 2 putaran	
	Total panjang penyangga pada inisialisasi penyangga MD dalam algoritma MD5 adalah... a. 512 bit d. 32 bit b. 128 bit e. 64 bit c. 256 bit	
Mahasiswa dapat mengidentifikasikan konsep tanda tangan digital	Tanda tangan digital menggunakan sistem... a. Kriptografi simetri b. Cipher alira c. Kriptografi asimetri d. Cipher blok e. Kunci privat	
	Penegasan merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti... a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya	

Indikator	Soal	Validitas Butir
	Efisiensi merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti... a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya	
Mahasiswa dapat mengidentifikasikan protokol kriptografi	Di bawah ini yang bukan kegunaan protokol kriptografi adalah... a. Pengiriman hasil cipherteks kepada penerima pesan b. Berbagi komponen rahasia untuk menghitung sebuah nilai c. Membangkitkan rangkaian bilangan acak d. Proses otentikasi identitas e. Membangkitkan rangkaian bilangan prima	
	Dalam mendesain protokol kriptografi dua langkah penting yang harus diperhatikan adalah... a. Proses otentikasi pada pengirim dan penerima pesan b. Identifikasi semua asumsi yang digunakan dan tentukan pengaruhnya terhadap tujuan keamanan jika asumsi itu dilanggar c. Penggunaan setiap kunci yang akan digunakan pada setiap proses enkripsi dan dekripsi d. Proses enkripsi dan dekripsi yang terjamin keamanan algoritmanya e. Setiap pembangkitan kunci bilangan prima dan acak semu harus bersifat *private* atau rahasia	
	Dua gabungan sistem kriptografi yang digunakan pada sebuah protokol disebut... a. *Double Cryptosystem* b. *Second Cryptosystem* c. *Hybrid Cryptosystem* d. *First Cryptosystem* e. *Cryptosystem Engineering*	

Indikator	Soal	Validitas Butir
Mahasiswa dapat menjelaskan pembangkit bilangan prima	Dalam pembangkit bilangan prima, menggunakan pembagi yang jauh lebih sedikit memiliki kelemahan yaitu... a. Memakan waktu yang lama pada saat pengujian b. Data algoritma yang dihasilkan memiliki banyak bilangan prima c. Bergantung pada media penyimpanan bilangan prima yang pernah dihasilkan d. Membutuhkan biaya tambahan untuk penggunaan perangkat khusus e. Data pengujian tidak akurat untuk menemukan nilai bilangan prima	
Mahasiswa dapat mengidentifikasikan algoritma MAC	Algoritma MAC berbasiskan pada... a. Cipher blok b. Cipher substitusi c. Caesar cipher d. Cipher aliran e. Ekspansi cipher	
	Algoritma MAC tidak memiliki fungsi tanda tangan digital, tetapi menyediakan... a. Kerahasiaan data pengirim pesan b. Otentikasi pengirim dan otentikasi pesan c. Dokumentasi proses pengiriman dan penerimaan pesan d. Efisiensi waktu pada proses pemgiriman pesan e. Kerahasiaan data penerima pesan	
	Otentikasi arsip yang digunakan oleh dua atau lebih pengguna merupakan salah satu contoh peangaplikasian algoritma... a. RSA b. MD5 c. MD4 d. MAC e. RC4	
Mahasiswa dapat menganalisis penggunaan kriptografi dalam kehidupan sehari-hari	1) Kartu kredit 2) Pemancar radio 3) Pay TV 4) Kartu cerdas 5) Satelit TV Pada contoh di atas, yang bukan contoh penggunaan kriptografi dalam kehidupan sehari-hari adalah... a. 1) dan 2) b. 2) dan 3) c. 4) dan 5) d. 1) dan 5) e. 2) dan 5)	
	Dua kebutuhan keamanan pada GSM *mobile phone* dipenuhi dengan penggunaan... a. SIM *card* b. *Base station* c. Sinyal radio d. Gelombang mikro e. Antena	

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi	Cipherteks dari "HARI INI AKAN DIADAKAN UAS KRIPTOGRAFI" dengan menggunakan aturan Caesar Cipher adalah... a. KDUL LQL DNDQ GLDGONDQ XDV NULSWRJUDIL b. KDUL LQL DNDQ GLOGDNDQ XDV NULSWRJUDIL c. KDUL LQL DNDQ GLDGDNDQ XDV NULSWRJUDIL d. KDUL LQL DNOQ GLDGDNDQ XDT NULSWRJUDIL e. KDUL LQL DNOQ GLOGDNDQ XDV NULSWRJUDIL	
	Cipherteks dari "MATERI KRIPTOGRAFI YANG DIUJIKAN DIMULAI DARI DES" dengan menggunakan aturan Caesar Cipher adalah... a. PDWHUL NULSWRJUDIL BDQJ GLXMLNOQ GLPXODL GDUL GHV b. PDWHUL NULSWRJUDIL BDQJ GLXMLNRQ GLPXODL GDUL GHV c. PDWHUL NULSWRJUDIL BDQJ GLWMLNDQ GLPXODL GDUL GHV d. PDWHUL NULSWRJUDIL BDQJ GLXMLNDQ GLPXODL GDUL GHV e. PDWHUL NULSWRJUDIL BDQJ GLWMLNOQ GLPXODL GDUL GHV	
	Cipherteks dari "MATA KULIAH KRIPTOGRAFI ADALAH MATA KULIAH PILIHAN" dengan menggunakan aturan Caesar Cipher adalah... a. PDWD NXOLDK NULSWRJUDIL DGDODK PDWD NXOLBK SLOLKDO b. PDWD NXOLDK NULSWRJUDIL DGDOOK PDWD NXOLDK SLOLKDQ c. PDWD NXOLDK NULSWRJUDIL DGOODK PDWD NXOLDK SLOLKDO d. PDWD NXOLDK NULSWRJUDIL DGDODK PDWD NXOLDK SLOLKDQ e. PDWD NXOLDK NULSWRJUDIL DGDODR PDWD NXOLOK SLOLKDO	

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengaplikasikan algoritma *cipher* transposisi	Cipherteks dari "ALGORITMA KRIPTOGRAFI MODERN LEBIH RUMIT DARI PADA KLASIK" dengan menggunakan aturan *blocking* berupa 3 blok adalah... a. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B__RPALIGIATRIORLIRIDIA_AK b. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_RPALIGIARTRIORLIRIDIA_AK c. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_MPALIGIARTRIORLIRIDIAAK d. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_RPALIGIARTRORLIRIDIA_AK e. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_RPALIGARTRIORLIRIDIA_AK	
	Cipherteks dari "UJIAN AKHIR SEMESTER MATA KULIAH KRIPTOGRAFI" dengan menggunakan aturan *blocking* berupa 4 blok adalah... a. UNHSS_AL_PRJ_IETM_IKTAIARMEAKAROFAK_ERTUHIGI_ b. UNHSS_AL_PRJ_IETM_IKTAARMEAKAROFAK_ERTUHIGI c. UNHSS_AL_PRJ_IETM_IKTAIARMEAKASOFAK_ERTUHIGI d. UNHSS_AL_PRJ_IETM_IKTAARMEAKUROFAK_ERTUHIGI_ e. UNHSS_AL_PRJ_IETM_IKTAIARMEAKAROFAK_ERTUHIGI	
	Cipherteks dari "HARI INI HARI RABU TANGGAL SEPULUH JUNI" dengan menggunakan aturan *blocking* berupa 2 blok adalah... a. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN_ b. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN c. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPNHJN_ d. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTHGLSPLHJN e. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTGLSPLHJN_	
Mahasiswa dapat menjelaskan *cipher* aliran	Mengenkripsikan data pada saluran yang menghubungkan antara dua buah komputer merupakan contoh penggunaan kriptografi... a. Caesar Cipher b. Cipher blok c. Cipher aliran d. Cipher ekspansi e. Cipher subtitusi	

Dosen Pengampu

Prasetyo Wibowo Yunanto, M.Eng

Lampiran 32: Paket Soal 2

1. AES merupakan salah satu algoritma kriptografi *cipher block* dengan ukuran blok yaitu...
   a. 56 bit
   b. 128 bit
   c. 192 bit
   d. 255 bit
   e. 256 bit
2. Algoritma *Lucifer* telah diperbaharui menjadi algoritma DES yang kemudian digantikan kembali karena faktor keamanan yang kurang baik oleh algoritma...
   a. 3DES
   b. RC4
   c. A5
   d. RSA
   e. AES
3. *Keystream* yang sama digunakan dua kali terhadap potongan plainteks yang berbeda dapat mengakibatkan terjadinya serangan...
   a. *Known-plaintext attack*
   b. *Known-ciphertext attack*
   c. *Ciphertext-only attack*
   d. *Plaintext-only attack*
   e. *Flip-bit attack*
4. Penggunaan bit-aliran-kunci yang tidak dapat diprediksi pada cipher aliran dimaksudkan untuk...
   a. Menghasilkan cipherteks yang sulit didekripsi
   b. Menghindarkan kemungkinan kriptanalis mendeduksi bit-aliran-kunci
   c. Membuat beberapa cipherteks yang sulit dipecahkan
   d. Menghasilkan kunci-kunci dengan bilangan prima acak semu
   e. Menghindarkan kemungkinan kriptanalis mendapatkan plainteks
5. 1) Substitusi
   2) Transposisi
   3) Faktorisasi
   4) Diferensiasi
   Teknik di atas yang **bukan** merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah...
   a. 1) dan 3)
   b. 1) dan 2)
   c. 2) dan 4)
   d. 3) dan 4)
   e. 4)
6. 1) *Electronic Code Book* (*ECB*)
   2) *Cipher Block Chaining* (*CBC*)
   3) *Cipher Feedback* (*CFC*)
   4) *Output Feedback* (*OFB*)
   5) *Input Feedback* (IFB)
   Pada mode di atas yang **bukan** merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah...
   a. 5)
   b. 4)
   c. 3)
   d. 2)
   e. 1)

7. Prinsip perancangan *cipher* blok berupa *s-box* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks
   c. Mengubah plainteks menjadi cipherteks diulang beberapa kali
   d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
   e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain
8. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi merupakan prinsip perancangan *cipher* blok yaitu...
   a. *Strong key*
   b. *Weak key*
   c. *Long key*
   d. *Short key*
   e. *Low key*
9. $M = C^d \bmod n$ merupakan fungsi pada algoritma RSA untuk melakukan proses...
   a. Dekripsi
   b. Pembangkitan kunci
   c. Faktorisasi bilangan prima
   d. Enkripsi
   e. Pencarian bilangan prima
10. Cipherteks pada algoritma RSA bersifat...
    a. Simetris
    b. Privat
    c. Publik
    d. Sementara
    e. Tetap
11. Kunci dekripsi pada algoritma *Rabin* bersifat...
    a. Simetris
    b. Sementara
    c. Tetap
    d. Privat
    e. Publik
12. Kunci enkripsi pada algoritma *Rabin* bersifat...
    a. Simetris
    b. Sementara
    c. Tetap
    d. Privat
    e. Publik
13. 1) Nilai bilangan harus non-prima
    2) Data algoritma memiliki kompleksitas yang tinggi
    3) Memori yang dibutuhkan tidak terlalu besar
    4) Tahan terhadap serangan yang serius

    Salah satu syarat sebagai pembangkit bilangan acak yang cocok untuk kriptografi ditunjukkan oleh nomor..
    a. 1)
    b. 2)
    c. 3)
    d. 4)
    e. Semua Benar
14. Salah satu contoh penggunaan pembangkit bilangan acak semu yaitu untuk pembangkitan parameter kunci pada...
    a. Algoritma kunci publik
    b. Algoritma kunci privat
    d. Algoritma *cipher* substitusi
    e. Algoritma kunci asimetris

c. Algoritma *cipher* transposisi

15. Keunggulan *Linear Congruential Generator* (LCG) terletak pada...
    a. Algoritmanya sulit ditembus oleh kriptanalis
    b. Kecepatannya dan hanya membutuhkan sedikit operasi bit
    c. Menggunakan algoritma operasi byte
    d. Tidak membutuhkan memori yang besar
    e. Data algoritma pada proses enkripsi tidak rumit
16. Keamanan pada fungsi *hash* satu arah terletak pada...
    a. Logaritma diskrit yang sulit dipecahkan
    b. Diferensial bilangannya memiliki nilai yang besar
    c. Sifat satu arah dari fungsi *hash* itu sendiri
    d. Kerumitan algoritma pada proses enkripsi
    e. Penggunaan pembangkit kunci acak
17. Kolisi adalah...
    a. Nilai variabel pada *hash* bersifat bilangan prima
    b. Keadaan dimana nilai *hash* dapat didekripsi kembali
    c. Keadaan dimana nilai *hash* dapat dienkripsi kembali
    d. Kondisi dua *string* sembarang memiliki nilai *hash* yang sama
    e. Nilai variabel pada *hash* bersifat bilangan non-prima
18. Salah satu contoh dari fungsi *hash* satu arah adalah...
    a. RC4
    b. RSA
    c. A5
    d. MD5
    e. AES
19. Pada algoritma MD5, pengolahan pesan dilakukan dalam blok berukuran...
    a. 512 bit
    b. 256 bit
    c. 128 bit
    d. 64 bit
    e. 32 bit
20. Pada pengolahan pesan dalam algoritma MD5, proses H_{MD5} memiliki putaran sebanyak...
    a. 5 putaran
    b. 3 putaran
    c. 2 putaran
    d. 8 putaran
    e. 4 putaran
21. Total panjang penyangga pada inisialisasi penyangga MD dalam algoritma MD5 adalah...
    a. 512 bit
    b. 128 bit
    c. 256 bit
    d. 32 bit
    e. 64 bit
22. Tanda tangan digital menggunakan sistem...
    a. Kriptografi simetri
    b. Cipher aliran
    c. Kriptografi asimetri
    d. Cipher blok
    e. Kunci privat

23. Penegasan merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti...
    a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
    b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
    c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
    d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
    e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya
24. Efisiensi merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti...
    a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
    b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
    c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
    d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
    e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya
25. Di bawah ini yang bukan kegunaan protokol kriptografi adalah...
    a. Pengiriman hasil cipherteks kepada penerima pesan
    b. Berbagi komponen rahasia untuk menghitung sebuah nilai
    c. Membangkitkan rangkaian bilangan acak
    d. Proses otentikasi identitas
    e. Membangkitkan rangkaian bilangan prima
26. Dalam mendesain protokol kriptografi dua langkah penting yang harus diperhatikan adalah...
    a. Proses otentikasi pada pengirim dan penerima pesan
    b. Identifikasi semua asumsi yang digunakan dan tentukan pengaruhnya terhadap tujuan keamanan jika asumsi itu dilanggar
    c. Penggunaan setiap kunci yang akan digunakan pada setiap proses enkripsi dan dekripsi
    d. Proses enkripsi dan dekripsi yang terjamin keamanan algoritmanya
    e. Setiap pembangkitan kunci bilangan prima dan acak semu harus bersifat *private* atau rahasia
27. Dua gabungan sistem kriptografi yang digunakan pada sebuah protokol disebut...
    a. *Double Cryptosystem*
    b. *Second Cryptosystem*
    c. *Hybrid Cryptosystem*
    d. *First Cryptosystem*
    e. *Cryptosystem Engineering*

28. Dalam pembangkit bilangan prima, menggunakan pembagi yang jauh lebih sedikit memiliki kelemahan yaitu...
    a. Memakan waktu yang lama pada saat pengujian
    b. Data algoritma yang dihasilkan memiliki banyak bilangan prima
    c. Bergantung pada media penyimpanan bilangan prima yang pernah dihasilkan
    d. Membutuhkan biaya tambahan untuk penggunaan perangkat khusus
    e. Data pengujian tidak akurat untuk menemukan nilai bilangan prima
29. Algoritma MAC berbasiskan pada...
    a. Cipher blok
    b. Cipher substitusi
    c. Caesar cipher
    d. Cipher aliran
    e. Ekspansi cipher
30. Algoritma MAC tidak memiliki fungsi tanda tangan digital, tetapi menyediakan...
    a. Kerahasiaan data pengirim pesan
    b. Otentikasi pengirim dan otentikasi pesan
    c. Dokumentasi proses pengiriman dan penerimaan pesan
    d. Efisiensi waktu pada proses pemgiriman pesan
    e. Kerahasiaan data penerima pesan
31. Otentikasi arsip yang digunakan oleh dua atau lebih pengguna merupakan salah satu contoh peangaplikasian algoritma...
    a. RSA
    b. MD5
    c. MD4
    d. MAC
    e. RC4
32. 1) Kartu kredit
    2) Pemancar radio
    3) Pay TV
    4) Kartu cerdas
    5) Satelit TV

    Pada contoh di atas, yang bukan contoh penggunaan kriptografi dalam kehidupan sehari-hari adalah...
    a. 1) dan 2)
    b. 2) dan 3)
    c. 4) dan 5)
    d. 1) dan 5)
    e. 2) dan 5)
33. Dua kebutuhan keamanan pada GSM *mobile phone* dipenuhi dengan penggunaan...
    a. SIM *card*
    b. *Base station*
    c. Sinyal radio
    d. Gelombang mikro
    e. Antena
34. Cipherteks dari “HARI INI AKAN DIADAKAN UAS KRIPTOGRAFI” dengan menggunakan aturan Caesar Cipher adalah...
    a. KDUL LQL DNDQ GLDGONDQ XDV NULSWRJUDIL
    b. KDUL LQL DNDQ GLOGDNDQ XDV NULSWRJUDIL
    c. KDUL LQL DNDQ GLDGDNDQ XDV NULSWRJUDIL
    d. KDUL LQL DNOQ GLDGDNDQ XDT NULSWRJUDIL
    e. KDUL LQL DNOQ GLOGDNDQ XDV NULSWRJUDIL

35. Cipherteks dari “MATERI KRIPTOGRAFI YANG DIUJIKAN DIMULAI DARI DES” dengan menggunakan aturan Caesar Cipher adalah...
    a. PDWHUL NULSWRJUDIL BDQJ GLXMLNOQ GLPXODL GDUL GHV
    b. PDWHUL NULSWRJUDIL BDQJ GLXMLNRQ GLPXODL GDUL GHV
    c. PDWHUL NULSWRJUDIL BDQJ GLWMLNDQ GLPXODL GDUL GHV
    d. PDWHUL NULSWRJUDIL BDQJ GLXMLNDQ GLPXODL GDUL GHV
    e. PDWHUL NULSWRJUDIL BDQJ GLWMLNOQ GLPXODL GDUL GHV
36. Cipherteks dari “MATA KULIAH KRIPTOGRAFI ADALAH MATA KULIAH PILIHAN” dengan menggunakan aturan Caesar Cipher adalah...
    a. PDWD NXOLDK NULSWRJUDIL DGDODK PDWD NXOLBK SLOLKDO
    b. PDWD NXOLDK NULSWRJUDIL DGDOOK PDWD NXOLDK SLOLKDQ
    c. PDWD NXOLDK NULSWRJUDIL DGOODK PDWD NXOLDK SLOLKDO
    d. PDWD NXOLDK NULSWRJUDIL DGDODK PDWD NXOLDK SLOLKDQ
    e. PDWD NXOLDK NULSWRJUDIL DGDODR PDWD NXOLOK SLOLKDO
37. Cipherteks dari “ALGORITMA KRIPTOGRAFI MODERN LEBIH RUMIT DARI PADA KLASIK” dengan menggunakan aturan *blocking* berupa 3 blok adalah...
    a. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B__RPALIGIATRIORLIRIDIA_AK
    b. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_RPALIGIARTRIORLIRIDIA_AK
    c. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_MPALIGIARTRIORLIRIDIAAK
    d. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_RPALIGIARTRORLIRIDIA_AK
    e. AOT_IOA_DNEHUTA_DKSLRMKPGFME_B_M_RPALIGARTRIORLIRIDIA_AK
38. Cipherteks dari “UJIAN AKHIR SEMESTER MATA KULIAH KRIPTOGRAFI” dengan menggunakan aturan *blocking* berupa 4 blok adalah...
    a. UNHSS_AL_PRJ_IETM_IKTAIARMEAKAROFAK_ERTUHIGI_
    b. UNHSS_AL_PRJ_IETM_IKTAARMEAKAROFAK_ERTUHIGI
    c. UNHSS_AL_PRJ_IETM_IKTAIARMEAKASOFAK_ERTUHIGI
    d. UNHSS_AL_PRJ_IETM_IKTAARMEAKUROFAK_ERTUHIGI_
    e. UNHSS_AL_PRJ_IETM_IKTAIARMEAKAROFAK_ERTUHIGI
39. Cipherteks dari “HARI INI HARI RABU TANGGAL SEPULUH JUNI” dengan menggunakan aturan *blocking* berupa 2 blok adalah...
    a. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN_
    b. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN
    c. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPNHJN_

d. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTHGLSPLHJN
e. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTGLSPLHJN_

40. Mengenkripsikan data pada saluran yang menghubungkan antara dua buah komputer merupakan contoh penggunaan kriptografi...
    a. Caesar Cipher
    b. Cipher blok
    c. Cipher aliran
    d. Cipher ekspansi
    e. Cipher subtitusi

VALIDITAS BUTIR SOAL PILIHAN GANDA dengan Korelasi Produk Moment
Taraf Signifikan = 5%

NO	Nama	Butir Soal																																				Skor Total (Y)	Y2	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40			
1	Mohammad Dwi Fachriansyah	0	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	19	361	
2	Desik Budi Pramesti	1	1	1	1	1	0	1	0	0	1	0	0	1	1	1	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	31	961	
3	Nurul Indah Prabawati	0	0	0	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	1	0	1	1	1	0	0	1	1	1	1	1	1	1	1	0	1	0	29	841	
4	Hafiez Arief Raharjo	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	32	1024	
5	Hendrik Praditya	0	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	1	1	24	576	
6	Muchtar Efendi	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	0	1	0	0	1	1	0	1	1	0	0	1	1	0	30	900	
7	Ilyas Rahmanda	1	1	0	1	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	0	1	1	0	1	0	0	1	1	1	1	1	1	1	1	1	0	29	841	
8	Ruby Eka Prawira	1	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	1	1	1	0	19	361	
9	Fitri Setiadewi	0	0	0	1	1	0	1	1	0	0	1	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	0	0	0	0	0	1	0	1	1	1	1	1	1	19	361	
10	Mentari Diyah Utami	1	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1	1	1	1	1	0	23	529	
11	Anggilina Ningsih	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	9	81	
12	Rahmawati Miftahul Fauziah	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0	1	1	1	1	1	0	1	14	196	
13	Nasiha Sakina	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	1	0	1	1	1	0	27	729	
14	Randi Satria	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	0	1	1	0	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1	1	1	20	400	
15	Purwati Septyaningrum	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	14	196	
16	Ibnu Prahadiwibowo	1	0	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	1	1	14	196	
17	Putri Ghanim Septia Habiba	0	1	0	0	1	0	0	0	0	1	1	0	0	0	1	1	0	1	0	0	0	0	0	0	1	1	0	0	0	1	1	1	0	1	1	1	1	1	0	1	18	324	
18	Rahma Qonita	1	1	0	0	1	0	1	0	0	0	1	0	0	1	1	1	1	1	0	1	0	0	0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	23	529	
19	Annisa Nurul Sabilla	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	1	1	1	0	0	0	1	0	1	1	1	1	1	1	1	0	15	225	
20	Muhammad Iswahyudi	0	0	0	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	1	0	1	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1	1	0	0	16	256	
	Benar (∑X)	10	9	3	11	16	3	14	9	10	9	14	10	5	4	13	16	12	17	11	11	6	5	8	7	9	10	8	4	3	11	16	7	9	18	17	17	18	19	16	10	425	9887	180625
	Salah	10	11	17	9	4	17	6	11	10	11	6	10	15	16	7	4	8	3	9	9	14	15	12	13	11	10	12	16	17	9	4	13	11	2	3	3	2	1	4	10			
	∑XY	242	224	88	264	368	88	330	232	247	223	328	251	135	116	309	341	290	361	277	264	164	78	204	141	223	242	187	113	86	264	350	151	227	402	364	349	386	396	368	214			
	rxy	0,451	0,503	0,519	0,465	0,535	0,519	0,542	0,626	0,527	0,488	0,509	0,589	0,508	0,592	0,525	0,019	0,546	-0,005	0,665	0,465	0,609	-0,499	0,530	-0,124	0,488	0,451	0,265	0,535	0,476	0,465	0,191	0,036	0,549	0,497	0,059	-0,262	0,089	-0,272	0,535	0,023			
	R Tabel	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444			
	Keterangan	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Tidak Vali	Valid	Tidak Vali	Valid	Valid	Valid	Tidak Vali	Valid	Tidak Vali	Valid	Valid	Tidak Vali	Valid	Valid	Valid	Tidak Vali	Valid	Valid	Tidak Vali	Tidak Vali	Valid	Valid	Tidak Vali	Tidak Vali	Tidak Vali	Valid	Tidak Valid			
	Tingkat Kesukaran	0,5	0,45	0,15	0,55	0,8	0,15	0,7	0,45	0,5	0,45	0,7	0,5	0,25	0,2	0,65	0,8	0,6	0,85	0,55	0,55	0,3	0,25	0,4	0,35	0,45	0,5	0,4	0,2	0,15	0,55	0,8	0,35	0,45	0,9	0,85	0,85	0,9	0,95	0,8	0,5			
	Indeks	Sedang	Sedang	Sukar	Sedang	Mudah	Sukar	Mudah	Sedang	Sedang	Sedang	Mudah	Sedang	Sukar	Sukar	Sedang	Mudah	Sedang	Mudah	Sedang	Sedang	Sedang	Sukar	Sedang	Sedang	Sedang	Sedang	Sedang	Sukar	Sukar	Sedang	Mudah	Sedang	Sedang	Mudah	Mudah	Mudah	Mudah	Mudah	Mudah	Sedang			

DATA KELOMPOK ATAS

NO	Nama	Butir Soal																																								Skor Total (Y)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
1	Hafiez Arief Raharjo	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	32
2	Desik Budi Pramesti	1	1	1	1	1	0	1	0	0	1	0	0	1	1	1	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	31
3	Nurul Indah Prabawati	0	0	0	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	0	30
4	Muchtar Efendi	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	0	1	1	0	1	0	1	1	0	1	1	0	0	1	1	1	0	30
5	Ilyas Rahmanda	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	0	1	1	0	1	0	0	1	1	0	1	1	1	1	1	1	0	29
6	Nasiha Sakina	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	0	1	1	0	0	0	1	1	1	0	0	1	1	0	1	1	1	0	27
7	Hendrik Praditya	0	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	1	1	24
8	Rahma Qonita	1	1	0	0	1	0	1	0	0	0	1	1	0	0	1	1	1	1	1	0	1	0	0	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	23
9	Mentari Diyah Utami	1	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1	1	1	1	0	22
10	Randi Satria	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	0	1	1	0	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	1	1	1	20
	Total Benar	7	6	4	7	10	3	9	7	8	7	9	7	4	4	8	8	9	9	8	7	5	1	6	3	7	6	5	5	3	8	9	3	6	10	9	8	9	9	10	5	268

DATA KELOMPOK BAWAH

NO	Nama	Butir Soal																																								Skor Total
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
1	Mohammad Dwi Fachriansyah	0	0	0	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	19
2	Ruby Eka Prawira	1	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	1	1	1	0	19
3	Fitri Setiadewi	0	0	0	1	1	0	1	1	0	0	1	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	19
4	Putri Ghanim Septia Habiba	0	1	0	0	1	0	0	0	0	1	1	0	0	0	1	1	0	1	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1	0	1	1	18
5	Muhammad Iswahyudi	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1	0	1	0	1	0	1	0	0	0	0	0	1	1	0	0	1	1	1	1	0	0	16
6	Annisa Nurul Sabilla	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	1	1	1	0	0	0	1	0	0	1	0	1	1	1	1	0	15
7	Ibnu Prahadiwibowo	1	0	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	1	1	14
8	Rahmawati Miftahul Fauziah	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	1	0	0	1	1	1	1	1	0	1	14
9	Purwati Septyaningrum	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	14
10	Anggilina Ningsih	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	9
	Total Benar	3	3	0	4	6	0	5	2	2	2	5	3	1	0	5	8	3	8	3	3	1	4	2	4	2	4	3	0	0	3	7	4	2	8	8	9	9	10	6	5	157
	Daya Beda	0,4	0,3	0,4	0,3	0,4	0,3	0,4	0,5	0,6	0,5	0,4	0,4	0,3	0,4	0,3	0	0,6	0,1	0,5	0,4	0,4	-0,3	0,4	-0,1	0,5	0,2	0,2	0,5	0,3	0,5	0,2	-0,1	0,4	0,2	0,1	-0,1	0	-0,1	0,4	0			

Butir Soal Nomor 1

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	7	1	0	1	1	10
Kelompok Bawah	2	3	2	0	3	0	10
Jumlah	2	10	3	0	4	1	20

Butir Soal Nomor 2

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	4	0	0	0	6	0	10
Kelompok Bawah	7	0	0	0	3	0	10
Jumlah	11	0	0	0	9	0	20

Butir Soal Nomor 3

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	2	1	4	1	2	0	10
Kelompok Bawah	4	3	0	2	1	0	10
Jumlah	6	4	4	3	3	0	20

Butir Soal Nomor 4

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	7	0	1	2	0	10
Kelompok Bawah	2	4	0	0	4	0	10
Jumlah	2	11	0	1	6	0	20

Butir Soal Nomor 5

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	10	0	0	10
Kelompok Bawah	0	1	2	6	1	0	10
Jumlah	0	1	2	16	1	0	20

Butir Soal Nomor 6

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	3	2	2	1	1	1	10
Kelompok Bawah	0	1	1	3	5	0	10
Jumlah	3	3	3	4	6	1	20

Butir Soal Nomor 7

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	0	0	0	9	0	10
Kelompok Bawah	2	0	3	0	5	0	10
Jumlah	3	0	3	0	14	0	20

Butir Soal Nomor 8

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	2	7	0	0	1	0	10
Kelompok Bawah	2	2	0	2	4	0	10
Jumlah	4	9	0	2	5	0	20

Butir Soal Nomor 9

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	0	0	1	1	0	10
Kelompok Bawah	2	4	2	0	1	1	10
Jumlah	10	4	2	1	2	1	20

Butir Soal Nomor 10

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	2	7	0	0	0	10
Kelompok Bawah	4	1	2	1	2	0	10
Jumlah	5	3	9	1	2	0	20

Butir Soal Nomor 11

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	9	1	0	10
Kelompok Bawah	0	1	3	5	1	0	10
Jumlah	0	1	3	14	2	0	20

Butir Soal Nomor 12

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	0	3	7	0	10
Kelompok Bawah	0	3	0	4	3	0	10
Jumlah	0	3	0	7	10	0	20

Butir Soal Nomor 13

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	1	0	4	4	0	10
Kelompok Bawah	0	2	1	1	6	0	10
Jumlah	1	3	1	5	10	0	20

Butir Soal Nomor 14

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	4	2	0	0	4	0	10
Kelompok Bawah	0	2	3	1	4	0	10
Jumlah	4	4	3	1	8	0	20

Butir Soal Nomor 15

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	2	8	0	0	0	0	10
Kelompok Bawah	3	5	0	1	1	0	10
Jumlah	5	13	0	1	1	0	20

Butir Soal Nomor 16

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	0	8	0	1	0	10
Kelompok Bawah	2	0	8	0	0	0	10
Jumlah	3	0	16	0	1	0	20

Butir Soal Nomor 17

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	9	1	0	10
Kelompok Bawah	3	1	2	3	1	0	10
Jumlah	3	1	2	12	2	0	20

Butir Soal Nomor 18

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	9	1	0	10
Kelompok Bawah	0	1	1	8	0	0	10
Jumlah	0	1	1	17	1	0	20

Butir Soal Nomor 19

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	0	1	1	0	0	10
Kelompok Bawah	3	2	4	1	0	0	10
Jumlah	11	2	5	2	0	0	20

Butir Soal Nomor 20

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	0	3	7	0	10
Kelompok Bawah	1	1	0	5	3	0	10
Jumlah	1	1	0	8	10	0	20

Butir Soal Nomor 21

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	5	1	3	1	0	10
Kelompok Bawah	4	1	0	4	1	0	10
Jumlah	4	6	1	7	2	0	20

Butir Soal Nomor 22

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	3	1	1	0	4	1	10
Kelompok Bawah	1	2	4	0	3	0	10
Jumlah	4	3	5	0	7	1	20

Butir Soal Nomor 23

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	2	0	2	6	0	0	10
Kelompok Bawah	4	2	1	2	1	0	10
Jumlah	6	2	3	8	1	0	20

Butir Soal Nomor 24

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	1	5	0	3	0	10
Kelompok Bawah	0	4	2	0	4	0	10
Jumlah	1	5	7	0	7	0	20

Butir Soal Nomor 25

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	7	2	1	0	0	0	10
Kelompok Bawah	2	3	0	3	2	0	10
Jumlah	9	5	1	3	2	0	20

Butir Soal Nomor 26

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	6	0	3	1	0	10
Kelompok Bawah	1	4	0	2	3	0	10
Jumlah	1	10	0	5	4	0	20

Butir Soal Nomor 27

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	4	0	5	0	1	0	10
Kelompok Bawah	6	1	3	0	0	0	10
Jumlah	10	1	8	0	1	0	20

Butir Soal Nomor 28

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	3	2	5	0	0	0	10
Kelompok Bawah	3	3	0	2	2	0	10
Jumlah	6	5	5	2	2	0	20

Butir Soal Nomor 29

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	3	1	0	6	0	0	10
Kelompok Bawah	0	1	1	6	2	0	10
Jumlah	3	2	1	12	2	0	20

Butir Soal Nomor 30

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	8	1	1	0	0	10
Kelompok Bawah	2	3	2	2	1	0	10
Jumlah	2	11	3	3	1	0	20

Butir Soal Nomor 31

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	9	1	0	10
Kelompok Bawah	1	0	0	7	2	0	10
Jumlah	1	0	0	16	3	0	20

Butir Soal Nomor 32

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	1	5	1	3	0	10
Kelompok Bawah	1	3	2	0	4	0	10
Jumlah	1	4	7	1	7	0	20

Butir Soal Nomor 33

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	2	0	2	0	0	10
Kelompok Bawah	2	3	0	5	0	0	10
Jumlah	8	5	0	7	0	0	20

Butir Soal Nomor 34

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	10	0	0	0	10
Kelompok Bawah	1	0	8	1	0	0	10
Jumlah	1	0	18	1	0	0	20

Butir Soal Nomor 35

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	1	0	9	0	0	10
Kelompok Bawah	0	0	1	8	1	0	10
Jumlah	0	1	1	17	1	0	20

Butir Soal Nomor 36

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	2	0	8	0	0	10
Kelompok Bawah	0	0	1	9	0	0	10
Jumlah	0	2	1	17	0	0	20

Butir Soal Nomor 37

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	9	1	0	0	0	10
Kelompok Bawah	0	9	0	0	0	1	10
Jumlah	0	18	1	0	0	1	20

Butir Soal Nomor 38

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	1	0	9	0	10
Kelompok Bawah	0	0	0	0	10	0	10
Jumlah	0	0	1	0	19	0	20

Butir Soal Nomor 39

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	10	0	0	0	0	0	10
Kelompok Bawah	6	4	0	0	0	0	10
Jumlah	16	4	0	0	0	0	20

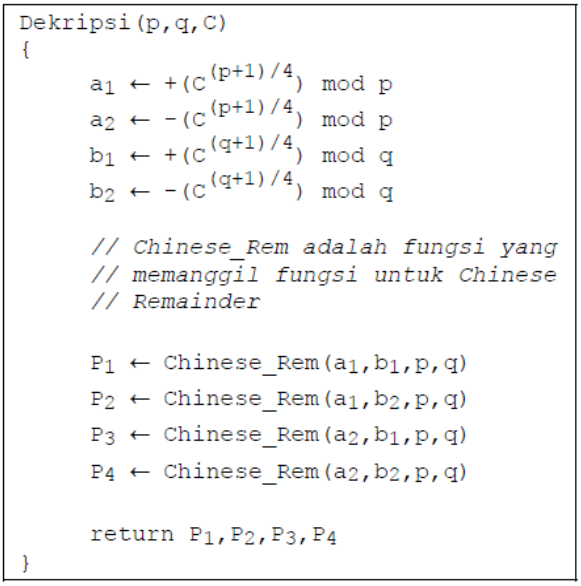
Butir Soal Nomor 40

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	1	5	2	1	0	10
Kelompok Bawah	1	0	5	3	0	1	10
Jumlah	2	1	10	5	1	1	20

Lampiran 34: Validasi Butir Paket Soal 3

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	Dalam proses *enchiper* pada algoritma DES, blok plainteks terbagi menjadi dua bagian yaitu bagian kiri (L) dan bagian kanan (R), yang masing-masing memilki panjang yaitu... a. 8 bit d. 64 bit b. 16 bit e. 128 bit c. 32 bit	
	1) 10 putaran 2) 12 putaran 3) 14 putaran 4) 16 putaran Jumlah putaran yang digunakan setiap blok pada AES-128 adalah... a. 1) d. 4) b. 2) e. Semua jawaban benar c. 3)	
Mahasiswa dapat mengidentifikasikan serangan terhadap *cipher* aliran	Pengubahan pada *flip-bit attack* dilakukan dengan cara... a. Mengubah kunci acak semu menggunakan bilangan prima b. Membalikkan bit tertentu (0 menjadi 1 atau 1 menjadi 0) c. Mengubah kunci acak dengan biner tertentu d. Membuat sebuah kunci baru untuk menggantikan kunci sebenarnya e. Melakukan pencurian bit-bit kunci untuk menghasilkan cipherteks	
	Agar dapat terhindar dari serangan seorang kriptanalis, penggunaan cipher aliran harus mempunyai... a. *Keystream generator* yang tidak menghasilkan kunci yang sama b. Beberapa cipherteks yang sulit dipecahkan c. Kunci yang rumit agar mendapatkan cipherteks yang sulit didekripsi d. Bit-aliran-kunci yang tidak dapat diprediksi e. Kunci yang mengandung bilangan prima acak semu	
Mahasiswa dapat mengidentifikasikan *cipher* blok	Di bawah ini yang merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah... a. Diferensiasi d. *Padding bit* b. *Flip-bit* e. Faktorisasi c. Ekspansi	

Indikator	Soal	Validitas Butir
	Di bawah ini merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher*, **kecuali**... a. *Electronic Code Book* (*ECB*) b. *Cipher Block Chaining (CBC*) c. *Cipher Feedback (CFC*) d. *Output Feedback* (*OFB*) e. *Input Feedback* (IFB)	
Mahasiswa dapat mendeskripsikan prinsip perancangan *cipher* blok	Prinsip perancangan *cipher* blok berupa *diffusion* berarti... a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks c. Mengubah plainteks menjadi cipherteks diulang beberapa kali d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain	
Mahasiswa dapat mengidentifikasikan algoritma RSA	1) *p* dan *q* bilangan prima 2) *PK* (kunci enkripsi) 3) *SK* (kunci dekripsi) 4) *X* (plainteks) 5) *Y* (cipherteks) Besaran di atas yang bersifat rahasia pada algoritma RSA adalah... a. 1), 3), dan 4) d. 2), 3), dan 4) b. 1), 2), dan 5) e. 1), 3), dan 5) c. 2), 3), dan 5)	
	Kunci dekripsi pada algoritma RSA bersifat... a. Simetris d. Sementara b. Privat e. Tetap c. Publik	
Mahasiswa dapat mengidentifikasikan algoritma *rabin*	Proses enkripsi pada algoritma *Rabin* dapat dilakukan dalam waktu yang relatif singkat sehingga memiliki keuntungan yaitu... a. Memudahkan pengirim pesan untukmengenkripsi plainteks dengan cepat b. Dapat mengefisienkan waktu yang digunakan dalam proses enkripsi c. Menghadapi keterbatasan *resource* yang ada pada media kriptografi d. Tidak mudah untuk dilakukan *hijacking* oleh kriptanalis e. Tidak membutuhkan kunci yang rumit pada proses enkripsi	

Indikator	Soal	Validitas Butir
Mahasiswa dapat menjelaskan pembangkit bilangan acak semu	*Linear Congruential Generator* (LCG) tidak dapat digunakan untuk kriptografi karena... a. Bilangan acaknya dapat diprediksi urutan kemunculannya b. Faktor bilangan terlalu rumit c. Logaritma diskritnya dapat diprediksi nilainya d. Membutuhkan memori yang besar e. Tidak lulus uji keacakan statistik	
Mahasiswa dapat mengidentifikasikan algoritma *rabin*	 Potongan program di atas merupakan proses dekripsi pada algoritma... a. MD5 d. Rabin b. A5 e. RSA c. RC4	
Mahasiswa dapat menjelaskan pembangkit bilangan acak semu	Pembangkit bilangan acak *Blum Blum Shub* (BBS) berbasis pada... a. Biner b. Teori peluang c. Bit d. Byte e. Teori bilangan	

Indikator	Soal	Validitas Butir
	1)*Blum Blum Shut* 2) *Chaos* 3) *InitializationVector* 4) *LinearCongruentialGenerator* 5) *Keystream Generator* Contoh di atas yang bukan termasuk dalam contoh pembangkit bilangan acak semu adalah... a. 1) dan 3) d. 4) dan 5) b. 2) dan 4) e. 3) dan 5) c. 3) dan 4)	
Mahasiswa dapat mengidentifikasikan fungsi *hash* satu arah	Salah satu contoh dari fungsi *hash* satu arah, **kecuali**... a. MD2 d. MD5 b. RSA e. SHA c. MD4	
	Pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula disebut... a. Fungsi hash satu arah b. Algoritma RSA c. Fungsi Digital Signature d. Algoritma RC4 e. Fungsi pesan acak	
	Di bawah ini yang bukan merupakan keuntungan penggunaan fungsi *hash* satu arah adalah... a. Peka terhadap perubahan 1 bit pada pesan b. Menormalkan panjang data yang beraneka ragam c. Algoritma tidak mudah diserang d. Menghemat waktu pengiriman e. Menjaga integritas data	
Mahasiswa dapat menyebutkan algoritma MD5	Kriptanalisis yang dapat dilakukan pada algoritma MD5 adalah... a. Destruksi d. Kolisi b. *Padding bits* e. *Chaos* c. *Message digest*	
	Pesan yang telah diberi bit-bit penganjal pada algoritma MD5 akan ditambahkan lagi dengan... a. 512 bit d. 32 bit b. 128 bit e. 64 bit c. 256 bit	
	Panjang proses H_{MD5} pada algoritma MD5 adalah... a. 512 bit d. 32 bit b. 128 bit e. 64 bit c. 256 bit	

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengidentifikasikan konsep tanda tangan digital	Di bawah ini merupakan unsur-unsur yang paling penting pada proses pembentukan dan verifikasi tanda tangan digital, **kecuali**... a. Integritas data b. Otentikasi penandatangan c. Otentikasi Dokumen d. Penegasan e. Efisiensi	
	Proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan disebut... a. Pembuatan tanda tangan digital b. Otentikasi penandatangan c. Verifikasi tanda tangan digital d. Otentikasi dokumen e. Integritas data	
	Proses pembentukan tanda tangan digital pada penggunaan tanda tangan digital berarti... a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya	
Mahasiswa dapat mengidentifikasikan protokol kriptografi	Protokol kriptografi digunakan untuk... a. Proses enkripsi pada algoritma kriptografi b. Proses dekripsi pada algoritma kriptografi c. Mencari sebuah kunci pada setiap proses enkripsi d. Berbagi komponen rahasia untuk menghitung sebuah nilai e. Pengiriman hasil cipherteks kepada penerima pesan	

Indikator	Soal	Validitas Butir
	Session key adalah... a. Kunci yang digunakan pada protokol komunikasi sebuah sistem kriptografi b. Kunci pada sebuah protokol yang menerapkan sistem kriptografi simetri c. Kunci pada sebuah protokol yang menerapkan sistem kriptografi kunci publik d. Kriptanalis berhasil mengetahui kunci yang digunakan pada protokol sebuah sistem kriptografi e. Sebuah kunci yang dipertukarkan antara pengirim dan penerima pesan pada protokol kriptografi	
	Masalah pada protokol komunikasi dengan sistem kriptografi simetri dapat dipecahkan dengan protokol komunikasi dengan sistem... a. Kriptografi kunci privat b. Kriptografi kunci publik c. Kriptografi klasik d. Kriptografi *stream cipher* e. Kriptografi *cipher* blok	
Mahasiswa dapat menjelaskan pembangkit bilangan prima	Salah satu metode dalam pembangkit bilangan prima yaitu menggunakan teknik yang mirip dengan *brute force* yang memiliki perbedan pada... a. Pemfaktoran bilangan prima dengan bilangan besar b. Logaritma diskrit yang digunakan lebih sedikit c. Menggunakan setiap kemungkinan diferensial bilangan d. Menggunakan pembagi bilangan yang bernilai besar e. Menggunakan pembagi yang jauh lebih sedikit	
Mahasiswa dapat mengidentifikasikan algoritma MAC	Fungsi satu arah yang menggunakan kunci rahasia dalam pembangkitan nilai *hash* disebut... a. RSA d. MAC b. RC4 e. MD5 c. A5	
	Kegunaan algoritma MAC adalah... a. Untuk melakukan pembangkitan kunci bilangan acak semu b. Untuk melakukan pembangkitan kunci bilangan prima c. Untuk otentikasi tanpa perlu merahasiakan pesan d. Untuk menentukan jumlah cipher blok yang digunakan e. Untuk memudahkan pemfaktoran bilangan prima	
Indikator	**Soal**	**Validitas Butir**

	Algoritma MAC mempunyai 2 basis yaitu... a. Berbasis *cipher* aliran dan *cipher* blok b. Berbasis *cipher* aliran dan fungsi *hash* c. Berbasis kriptografi simetri dan asimetri d. Berbasis kriptografi asimetri dan *cipher* blok e. Berbasis *cipher* blok dan fungsi *hash* satu arah	
Mahasiswa dapat menganalisis penggunaan kriptografi dalam kehidupan sehari-hari	Di bawah ini contoh penggunaan kriptografi dalam kehidupan sehari-hari, **kecuali**... a. Pemancar radio b. Pay TV c. Kartu cerdas d. Transaksi ATM e. Pengamanan e-mail dengan PGP	
	Penggunaan kriptografi dalam komunikasi pesan melalui GSM *mobile phone* berupa... a. Kunci privat yang dimiliki setiap pelanggan pengguna GSM *mobile phone* b. Pesan dienkripsi selama transmisi dari ponsel ke BST terdekat c. Penggunaan sistem kriptografi simetri pada pengiriman pesan d. Otentikasi data menggunakan sistem kriptografi kunci publik e. Kunci publik yang dimiliki setiap pelanggan pengguna GSM *mobile phone*	
	Sistem kriptografi yang terdapat dalam SIM *card* adalah... a. Simetri b. Asimetri c. *Caesar cipher* d. *Stream cipher* e. Kunci publik	
Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi	Cipherteks dari "UAS KRIPTOGRAFI AKAN DISELENGGARAKAN HARI INI" dengan menggunakan aturan Caesar Cipher adalah... a. XDV NULSWRJUDIL DNDQ GLVHOHQJDUDNDQ KDUL LQL b. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDNDQ KDUL LQL c. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUONDQ KDUL LQL d. XDV NULSWRJUDIL DNDQ GLVNOHQJJDUDNDQ KDUL LQL e. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDHDQ KDUL LQL	

Indikator	Soal	Validitas Butir
	Cipherteks dari "ISILAH SEMUA SOAL DENGAN BENAR" dengan menggunakan aturan Caesar Cipher adalah... a. LVLODK VHPXD VRDO GHQTDQ EHQDU b. LVLODK VHPXD VRDO GHQJDQ EHNDU c. LVLODK VHPXD VRDO GHQJDQ EHQDU d. LVLODK VHPXD VSDO GHQJDQ EHQDU e. LVLODK VHPXD VRDO GHOJDQ EHNDU	
	Cipherteks dari "FAKULTAS TEKNIK UNIVERSITAS NEGERI JAKARTA" dengan menggunakan aturan Caesar Cipher adalah... a. IDNXOWDV WHNQLN XQLYHUVLWDV QHJHUL MDNDUWO b. IDNXOWDV WHNQLN XQLYHUVLWDV QHJNUL MDNDUWD c. IDNXOWDV WHNQLN XQLYNUVLWDV QHJHUL MDNDUWO d. IDNXOWDV WNNOLN XQLYHUVLWDV QHJNUL MDNDUWD e. IDNXOWDV WHNQLN XQLYHUVLWDV QHJHUL MDNDUWD	
Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi	Cipherteks dari "CUACA HARI INI SANGAT TIDAK MENENTU" dengan menggunakan aturan *blocking* berupa 2 blok adalah... a. CAAHR_N_AGTTDKMNNUUC_AIIISNA_IA_EET_ b. CAAHR_H_AGTTDKMNNUUC_AIIISNA_IA_EES_ c. CAANR_N_AGTTDKMNNUUC_AIIISHA_IA_EET_ d. CAAHR_H_AGTTDKMNNUUC_AIIISNA_IA_EES_ e. CAAHR_N_AGTTRKMNNUUC_AIIISNA_IA_EET_	
	Cipherteks dari "UAS KRIPTOGRAFI AKAN DISELENGGARAKAN HARI INI" dengan menggunakan aturan *blocking* berupa 4 blok adalah... a. UKTAA_EGA_IIAROFKDLGKH__SIGIAIEAAI_PR_NSNRNRN b. UKTAA_EGA_IIAROFKDLGKH__SIGIAIEAAI__PR_NSNRNRN_ c. UKTAA_EGA_IIAROFKDLGKH_SIGIAIEAAI_PR_NSNRNRN d. UKTAA_EGA_IIAROFKDLGKH_SIGIAIEAAI_PR_NSNRNRN_ e. UKTAA_EGA_IIAROFKDLGKH_SIGIAIEAAI__PR_NSNRNRN	

Indikator	Soal	Validitas Butir
	Cipherteks dari "PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER" dengan menggunakan aturan *blocking* berupa 4 blok adalah... a. PIAEKFAANMEEDNK_OT_PRNI_NIRIDKU_DK TINMKAOT b. PIAEKFAANMEEDNK_OT__PRNI_NIRIDKU_D KTINMKAOT c. PIAEKFAANMEEDNK_OT_PRNI_NIRIDKU_DK TINMKAOT_ d. PIAEKFAANMEEDNK_OT__PRNI_NIRIDKU_D KTINMKAOT_ e. PIAEKFAANMEEDNK_OT__PRNI_NIRIDKU_D KTNMKAOT	
Mahasiswa dapat menjelaskan *cipher* aliran	Aliran-bit-kunci (*runningkey*) di-XOR-kan dengan aliran bit-bit plainteks untuk menghasilkan aliran bit-bit cipherteks merupakan proses enkripsi pada kriptografi... a. Caesar Cipher b. Cipher blok c. Cipher aliran d. Cipher ekspansi e. Cipher subtitusi	

Dosen Pengampu

Prasetyo Wibowo Yunanto, M.Eng

Lampiran 35: Paket Soal 3

1. Dalam proses *enchiper* pada algoritma DES, blok plainteks terbagi menjadi dua bagian yaitu bagian kiri (L) dan bagian kanan (R), yang masing-masing memilki panjang yaitu...
   a. 8 bit
   b. 16 bit
   c. 32 bit
   d. 64 bit
   e. 128 bit
2. 1) 10 putaran
   2) 12 putaran
   3) 14 putaran
   4) 16 putaran
   Jumlah putaran yang digunakan setiap blok pada AES-128 adalah...
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. Semua jawaban benar
3. Pengubahan pada *flip-bit attack* dilakukan dengan cara...
   a. Mengubah kunci acak semu menggunakan bilangan prima
   b. Membalikkan bit tertentu (0 menjadi 1 atau 1 menjadi 0)
   c. Mengubah kunci acak dengan biner tertentu
   d. Membuat sebuah kunci baru untuk menggantikan kunci sebenarnya
   e. Melakukan pencurian bit-bit kunci untuk menghasilkan cipherteks
4. Agar dapat terhindar dari serangan seorang kriptanalis, penggunaan cipher aliran harus mempunyai...
   a. *Keystream generator* yang tidak menghasilkan kunci yang sama
   b. Beberapa cipherteks yang sulit dipecahkan
   c. Kunci yang rumit agar mendapatkan cipherteks yang sulit didekripsi
   d. Bit-aliran-kunci yang tidak dapat diprediksi
   e. Kunci yang mengandung bilangan prima acak semu
5. Di bawah ini yang merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah...
   a. Diferensiasi
   b. *Flip-bit*
   c. Ekspansi
   d. *Padding bit*
   e. Faktorisasi
6. Di bawah ini merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher*, **kecuali**...
   a. *Electronic Code Book* (*ECB*)
   b. *Cipher Block Chaining* (*CBC*)
   c. *Cipher Feedback* (*CFC*)
   d. *Output Feedback* (*OFB*)
   e. *Input Feedback* (IFB)
7. Prinsip perancangan *cipher* blok berupa *diffusion* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks

c. Mengubah plainteks menjadi cipherteks diulang beberapa kali
d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

8. 1) *p* dan *q* bilangan prima
   2) *PK* (kunci enkripsi)
   3) *SK* (kunci dekripsi)
   4) *X* (plainteks)
   5) *Y* (cipherteks)

   Besaran di atas yang bersifat rahasia pada algoritma RSA adalah...
   a. 1), 3), dan 4)
   b. 1), 2), dan 5)
   c. 2), 3), dan 5)
   d. 2), 3), dan 4)
   e. 1), 3), dan 5)
9. Kunci dekripsi pada algoritma RSA bersifat...
   a. Simetris
   b. Privat
   c. Publik
   d. Sementara
   e. Tetap
10. Proses enkripsi pada algoritma *Rabin* dapat dilakukan dalam waktu yang relatif singkat sehingga memiliki keuntungan yaitu...
    a. Memudahkan pengirim pesan untuk mengenkripsi plainteks dengan cepat
    b. Dapat mengefisienkan waktu yang digunakan dalam proses enkripsi
    c. Menghadapi keterbatasan *resource* yang ada pada media kriptografi
    d. Tidak mudah untuk dilakukan *hijacking* oleh kriptanalis
    e. Tidak membutuhkan kunci yang rumit pada proses enkripsi
11. *Linear Congruential Generator* (LCG) tidak dapat digunakan untuk kriptografi karena...
    a. Bilangan acaknya dapat diprediksi urutan kemunculannya
    b. Faktor bilangan terlalu rumit
    c. Logaritma diskritnya dapat diprediksi nilainya
    d. Membutuhkan memori yang besar
    e. Tidak lulus uji keacakan statistik

12.
```
Dekripsi(p,q,C)
{
      a1 ← +(C^((p+1)/4)) mod p
      a2 ← -(C^((p+1)/4)) mod p
      b1 ← +(C^((q+1)/4)) mod q
      b2 ← -(C^((q+1)/4)) mod q

      // Chinese_Rem adalah fungsi yang
      // memanggil fungsi untuk Chinese
      // Remainder

      P1 ← Chinese_Rem(a1,b1,p,q)
      P2 ← Chinese_Rem(a1,b2,p,q)
      P3 ← Chinese_Rem(a2,b1,p,q)
      P4 ← Chinese_Rem(a2,b2,p,q)

      return P1,P2,P3,P4
}
```

Potongan program di atas merupakan proses dekripsi pada algoritma...

a. MD5
b. A5
c. RC4
d. Rabin
e. RSA

13. Pembangkit bilangan acak *Blum Blum Shub* (BBS) berbasis pada...
    a. Biner
    b. Teori peluang
    c. Bit
    d. Byte
    e. Teori bilangan

14. 1) *Blum Blum Shut*
2) *Chaos*
3) *InitializationVector*
4) *Linear Congruential Generator*
5) *Keystream Generator*

Contoh di atas yang bukan termasuk dalam contoh pembangkit bilangan acak semu adalah...

a. 1) dan 3)
b. 2) dan 4)
c. 3) dan 4)
d. 4) dan 5)
e. 3) dan 5)

15. Salah satu contoh dari fungsi *hash* satu arah, **kecuali**...
    a. MD2
    b. RSA
    c. MD4
    d. MD5
    e. SHA

16. Pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula disebut...
    a. Fungsi hash satu arah
    b. Algoritma RSA
    c. Fungsi Digital Signature

d. Algoritma RC4
e. Fungsi pesan acak

17. Di bawah ini yang bukan merupakan keuntungan penggunaan fungsi *hash* satu arah adalah...
    a. Peka terhadap perubahan 1 bit pada pesan
    b. Menormalkan panjang data yang beraneka ragam
    c. Algoritma tidak mudah diserang
    d. Menghemat waktu pengiriman
    e. Menjaga integritas data
18. Kriptanalisis yang dapat dilakukan pada algoritma MD5 adalah...
    a. Destruksi
    b. *Padding bits*
    c. *Message digest*
    d. Kolisi
    e. *Chaos*
19. Pesan yang telah diberi bit-bit penganjal pada algoritma MD5 akan ditambahkan lagi dengan...
    a. 512 bit
    b. 128 bit
    c. 256 bit
    d. 32 bit
    e. 64 bit
20. Panjang proses H_{MD5} pada algoritma MD5 adalah...
    a. 512 bit
    b. 128 bit
    c. 256 bit
    d. 32 bit
    e. 64 bit
21. Di bawah ini merupakan unsur-unsur yang paling penting pada proses pembentukan dan verifikasi tanda tangan digital, **kecuali**...
    a. Integritas data
    b. Otentikasi penandatangan
    c. Otentikasi Dokumen
    d. Penegasan
    e. Efisiensi
22. Proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan disebut...
    a. Pembuatan tanda tangan digital
    b. Otentikasi penandatangan
    c. Verifikasi tanda tangan digital
    d. Otentikasi dokumen
    e. Integritas data
23. Proses pembentukan tanda tangan digital pada penggunaan tanda tangan digital berarti...
    a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
    b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
    c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
    d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
    e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya
24. Protokol kriptografi digunakan untuk...
    a. Proses enkripsi pada algoritma kriptografi

b. Proses dekripsi pada algoritma kriptografi
c. Mencari sebuah kunci pada setiap proses enkripsi
d. Berbagi komponen rahasia untuk menghitung sebuah nilai
e. Pengiriman hasil cipherteks kepada penerima pesan

25. *Session key* adalah...
    a. Kunci yang digunakan pada protokol komunikasi sebuah sistem kriptografi
    b. Kunci pada sebuah protokol yang menerapkan sistem kriptografi simetri
    c. Kunci pada sebuah protokol yang menerapkan sistem kriptografi kunci publik
    d. Kriptanalis berhasil mengetahui kunci yang digunakan pada protokol sebuah sistem kriptografi
    e. Sebuah kunci yang dipertukarkan antara pengirim dan penerima pesan pada protokol kriptografi
26. Masalah pada protokol komunikasi dengan sistem kriptografi simetri dapat dipecahkan dengan protokol komunikasi dengan sistem...
    a. Kriptografi kunci privat
    b. Kriptografi kunci publik
    c. Kriptografi klasik
    d. Kriptografi *stream cipher*
    e. Kriptografi *cipher* blok
27. Salah satu metode dalam pembangkit bilangan prima yaitu menggunakan teknik yang mirip dengan *brute force* yang memiliki perbedan pada...
    a. Pemfaktoran bilangan prima dengan bilangan besar
    b. Logaritma diskrit yang digunakan lebih sedikit
    c. Menggunakan setiap kemungkinan diferensial bilangan
    d. Menggunakan pembagi bilangan yang bernilai besar
    e. Menggunakan pembagi yang jauh lebih sedikit
28. Fungsi satu arah yang menggunakan kunci rahasia dalam pembangkitan nilai *hash* disebut...
    a. RSA
    b. RC4
    c. A5
    d. MAC
    e. MD5
29. Kegunaan algoritma MAC adalah...
    a. Untuk melakukan pembangkitan kunci bilangan acak semu
    b. Untuk melakukan pembangkitan kunci bilangan prima
    c. Untuk otentikasi tanpa perlu merahasiakan pesan
    d. Untuk menentukan jumlah cipher blok yang digunakan
    e. Untuk memudahkan pemfaktoran bilangan prima
30. Algoritma MAC mempunyai 2 basis yaitu...
    a. Berbasis *cipher* aliran dan *cipher* blok
    b. Berbasis *cipher* aliran dan fungsi *hash*
    c. Berbasis kriptografi simetri dan asimetri
    d. Berbasis kriptografi asimetri dan *cipher* blok
    e. Berbasis *cipher* blok dan fungsi *hash* satu arah

31. Di bawah ini contoh penggunaan kriptografi dalam kehidupan sehari-hari, **kecuali**...
    a. Pemancar radio
    b. Pay TV
    c. Kartu cerdas
    d. Transaksi ATM
    e. Pengamanan e-mail dengan PGP
32. Penggunaan kriptografi dalam komunikasi pesan melalui GSM *mobile phone* berupa...
    a. Kunci privat yang dimiliki setiap pelanggan pengguna GSM *mobile phone*
    b. Pesan dienkripsi selama transmisi dari ponsel ke BST terdekat
    c. Penggunaan sistem kriptografi simetri pada pengiriman pesan
    d. Otentikasi data menggunakan sistem kriptografi kunci publik
    e. Kunci publik yang dimiliki setiap pelanggan pengguna GSM *mobile phone*
33. Sistem kriptografi yang terdapat dalam SIM *card* adalah...
    a. Simetri
    b. Asimetri
    c. *Caesar cipher*
    d. *Stream cipher*
    e. Kunci publik
34. Cipherteks dari "UAS KRIPTOGRAFI AKAN DISELENGGARAKAN HARI INI" dengan menggunakan aturan Caesar Cipher adalah...
    a. XDV NULSWRJUDIL DNDQ GLVHOHQJDUDNDQ KDUL LQL
    b. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDNDQ KDUL LQL
    c. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUONDQ KDUL LQL
    d. XDV NULSWRJUDIL DNDQ GLVNOHQJJDUDNDQ KDUL LQL
    e. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDHDQ KDUL LQL
35. Cipherteks dari "ISILAH SEMUA SOAL DENGAN BENAR" dengan menggunakan aturan Caesar Cipher adalah...
    a. LVLODK VHPXD VRDO GHQTDQ EHQDU
    b. LVLODK VHPXD VRDO GHQJDQ EHNDU
    c. LVLODK VHPXD VRDO GHQJDQ EHQDU
    d. LVLODK VHPXD VSDO GHQJDQ EHQDU
    e. LVLODK VHPXD VRDO GHOJDQ EHNDU
36. Cipherteks dari "FAKULTAS TEKNIK UNIVERSITAS NEGERI JAKARTA" dengan menggunakan aturan Caesar Cipher adalah...
    a. IDNXOWDV WHNQLN XQLYHUVLWDV QHJHUL MDNDUWO
    b. IDNXOWDV WHNQLN XQLYHUVLWDV QHJNUL MDNDUWD
    c. IDNXOWDV WHNQLN XQLYNUVLWDV QHJHUL MDNDUWO
    d. IDNXOWDV WNNOLN XQLYHUVLWDV QHJNUL MDNDUWD
    e. IDNXOWDV WHNQLN XQLYHUVLWDV QHJHUL MDNDUWD
37. Cipherteks dari "CUACA HARI INI SANGAT TIDAK MENENTU" dengan menggunakan aturan *blocking* berupa 2 blok adalah...
    a. CAAHR_N_AGTTDKMNNUUC_AIIISNA_IA_EET_
    b. CAAHR_H_AGTTDKMNNUUC_AIIISNA_IA_EES_
    c. CAANR_N_AGTTDKMNNUUC_AIIISHA_IA_EET_
    d. CAAHR_H_AGTTDKMNNUUC_AIIISNA_IA_EES_

e. CAAHR_N_AGTTRKMNNUUC_AIIISNA_IA_EET_

38. Cipherteks dari "UAS KRIPTOGRAFI AKAN DISELENGGARAKAN HARI INI" dengan menggunakan aturan *blocking* berupa 4 blok adalah...
    a. UKTAA_EGA_IIAROFKDLGKH__SIGIAIEAAI_PR_NSNRNRN
    b. UKTAA_EGA_IIAROFKDLGKH__SIGIAIEAAI__PR_NSNRNRN_
    c. UKTAA_EGA_IIAROFKDLGKH_SIGIAIEAAI_PR_NSNRNRN
    d. UKTAA_EGA_IIAROFKDLGKH_SIGIAIEAAI_PR_NSNRNRN_
    e. UKTAA_EGA_IIAROFKDLGKH_SIGIAIEAAI__PR_NSNRNRN
39. Cipherteks dari "PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER" dengan menggunakan aturan *blocking* berupa 4 blok adalah...
    a. PIAEKFAANMEEDNK_OT_PRNI_NIRIDKU_DKTINMKAOT
    b. PIAEKFAANMEEDNK_OT__PRNI_NIRIDKU_DKTINMKAOT
    c. PIAEKFAANMEEDNK_OT_PRNI_NIRIDKU_DKTINMKAOT_
    d. PIAEKFAANMEEDNK_OT__PRNI_NIRIDKU_DKTINMKAOT_
    e. PIAEKFAANMEEDNK_OT__PRNI_NIRIDKU_DKTNMKAOT
40. Aliran-bit-kunci (*running key*) di-XOR-kan dengan aliran bit-bit plainteks untuk menghasilkan aliran bit-bit cipherteks merupakan proses enkripsi pada kriptografi...
    a. Caesar Cipher
    b. Cipher blok
    c. Cipher aliran
    d. Cipher ekspansi
    e. Cipher subtitusi

VALIDITAS BUTIR SOAL PILIHAN GANDA dengan Korelasi Produk Moment
Taraf Signifikan = 5%

NO	Nama	Butir Soal																																					Skor Total (Y)	Y2	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40			
1	M. Rayhan Haroki	1	0	1	0	1	0	0	1	1	0	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	18	324	
2	Hanna Nurdianah	1	0	1	0	1	0	0	0	1	0	1	0	0	1	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	17	289	
3	Fickry Ibnu Saputra	1	0	1	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	19	361	
4	Gatis Lestiana	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	0	1	1	0	1	0	0	1	1	0	0	1	1	1	1	1	1	1	30	900	
5	R. M. Firzatullah	1	0	1	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	1	1	1	18	324	
6	Muhamad Prasetio Dwi Cahyo	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	0	1	0	1	0	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	30	900	
7	Nillam Kesuma	1	1	1	0	0	0	1	0	1	1	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	20	400	
8	Muhamad Syahrizal	1	0	1	1	1	0	0	1	1	0	0	1	0	1	1	1	1	0	0	1	0	1	0	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	26	676	
9	Faldy Alga Firman	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	0	0	0	30	900	
10	Cahyo Pramudita	1	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	1	1	1	1	0	0	1	0	1	1	0	0	1	1	1	1	1	1	1	29	841	
11	Tera Putri S.	1	1	1	0	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	18	324	
12	Riki Anggun Gumala	1	0	1	0	1	1	1	0	1	0	1	1	0	0	1	1	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	1	1	1	1	1	1	25	625	
13	Nida Aulia Hasanah	0	1	1	0	1	0	0	0	1	0	1	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	20	400	
14	Annisa Tri Ambareta	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	1	1	0	0	0	11	121	
15	R. Andi Rahmadi	0	0	1	0	1	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	0	1	0	1	1	1	0	1	0	0	0	1	1	1	1	1	0	1	0	0	18	324	
16	Dimas Agung Riansa	1	0	1	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	0	1	0	1	1	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	28	784	
17	Meyvi Lusandi	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	14	196	
18	Humairoh Desreini	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	1	1	0	15	225	
19	Silka Najah	1	1	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0	0	1	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	1	1	1	1	1	17	289	
20	Ivan Bagaskara A.	1	0	1	1	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	1	1	1	1	1	16	256	
	Benar (∑X)	16	8	15	6	15	3	9	7	16	4	15	8	4	5	15	19	8	3	8	8	2	15	4	12	13	8	2	8	3	9	16	5	11	17	18	18	18	16	18	14	419	9459	175561
	Salah	4	12	5	14	5	17	11	13	4	16	5	12	16	15	5	1	12	17	12	12	18	5	16	8	7	12	18	12	17	11	4	15	9	3	2	2	2	4	2	6			
	∑XY	356	194	333	160	329	85	219	177	356	109	337	205	107	132	338	402	197	84	162	194	59	320	107	279	298	161	58	196	86	229	336	91	243	375	371	372	371	342	378	311			
	rxy	0,446	0,462	0,371	0,641	0,292	0,532	0,524	0,545	0,446	0,540	0,450	0,654	0,497	0,539	0,470	0,155	0,514	0,508	-0,098	0,462	0,488	0,114	0,497	0,483	0,461	-0,115	0,460	0,497	0,556	0,697	0,017	-0,272	0,216	0,452	-0,174	-0,146	-0,174	0,146	0,026	0,331			
	R Tabel	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444			
	Keterangan	Valid	Valid	Idak Vali	Valid	Idak Vali	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Idak Vali	Valid	Valid	Idak Vali	Valid	Valid	Idak Vali	Valid	Valid	Valid	Idak Vali	Valid	Valid	Valid	Valid	Idak Vali	Idak Vali	Idak Vali	Valid	Idak Vali	Idak Vali	Idak Vali	Idak Vali	Idak Vali	Idak Vali			

Tingkat Kesukaran	0,8	0,4	0,75	0,3	0,75	0,15	0,45	0,35	0,8	0,2	0,75	0,4	0,2	0,25	0,75	0,95	0,4	0,15	0,4	0,4	0,1	0,75	0,2	0,6	0,65	0,4	0,1	0,4	0,15	0,45	0,8	0,25	0,55	0,85	0,9	0,9	0,9	0,8	0,9	0,7			
Indeks	Mudah	Sedang	Mudah	Sedang	Mudah	Sukar	Sedang	Sedang	Mudah	Sukar	Mudah	Sedang	Sukar	Sukar	Mudah	Mudah	Sedang	Sukar	Sedang	Sedang	Sukar	Mudah	Sukar	Sedang	Sedang	Sedang	Sukar	Sedang	Sukar	Sedang	Mudah	Sukar	Sedang	Mudah	Mudah	Mudah	Mudah	Mudah	Mudah	Mudah			

DATA KELOMPOK ATAS

NO	Nama	Butir Soal																																								Skor Total (Y)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
1	Gatis Lestiana	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	0	1	1	0	1	0	0	1	1	0	0	1	1	1	1	1	1	1	30
2	Faldy Alga Firman	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	30
3	Muhamad Prasetio Dwi Cahyo	1	1	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	0	1	0	1	0	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	30
4	Cahyo Pramudita	1	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	1	1	1	1	0	0	1	0	1	1	0	0	1	1	1	1	1	1	1	29
5	Dimas Agung Riansa	1	0	1	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	0	1	0	1	1	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	28
6	Muhamad Syahrizal	1	0	1	1	1	0	0	1	1	0	0	1	0	1	1	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	26
7	Riki Anggun Gumala	1	0	1	0	1	1	1	0	1	0	1	1	0	0	1	1	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	1	1	1	1	1	1	25
8	Nida Aulia Hasanah	0	1	1	0	1	0	0	0	1	0	1	0	0	0	1	1	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	20
9	Nillam Kesuma	1	1	1	0	0	0	1	0	1	1	1	1	0	0	0	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	20
10	Fickry Ibnu Saputra	1	0	1	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	1	1	1	1	1	1	1	1	19
	Total Benar	9	6	9	5	8	3	7	5	10	4	9	7	3	4	9	10	6	3	4	5	2	8	4	8	9	3	2	5	3	7	8	2	7	10	9	9	9	9	9	8	257

DATA KELOMPOK BAWAH

NO	Nama	Butir Soal																																								Skor Total
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
1	R. M. Firzatullah	1	0	1	0	0	0	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	1	1	1	18
2	Tera Putri S.	1	1	1	0	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1	1	18
3	M. Rayhan Haroki	1	0	1	0	1	0	1	1	1	0	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	1	1	1	0	1	1	18
4	R. Andi Rahmadi	0	0	1	0	1	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	0	1	0	1	1	1	0	1	0	1	0	0	0	1	1	1	1	0	1	0	18
5	Silka Najah	1	1	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0	0	1	0	1	0	0	1	0	0	1	0	0	1	0	0	0	1	0	1	1	1	1	17
6	Ivan Bagaskara A.	1	0	1	1	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	0	1	1	1	1	1	1	1	17
7	Hanna Nurdianah	1	0	1	0	1	0	0	0	1	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	17
8	Humairoh Desreini	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	1	1	0	15
9	Meyvi Lusandi	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	14
10	Annisa Tri Ambareta	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	1	0	0	1	1	1	0	0	0	11
	Total Benar	7	2	6	1	7	0	2	2	6	0	6	1	1	1	6	9	2	0	4	3	0	7	0	4	4	5	0	3	0	2	8	3	4	8	9	9	9	7	9	6	163

Daya Beda	0,2	0,4	0,3	0,4	0,1	0,3	0,5	0,3	0,4	0,4	0,3	0,6	0,2	0,3	0,3	0,1	0,4	0,3	0	0,2	0,2	0,1	0,4	0,4	0,5	-0,2	0,2	0,2	0,3	0,5	0	-0,1	0,3	0,2	0	0	0	0,2	0	0,2			

Butir Soal Nomor 1

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	0	9	0	0	0	10
Kelompok Bawah	0	1	7	2	0	0	10
Jumlah	1	1	16	2	0	0	20

Butir Soal Nomor 2

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	2	0	2	0	0	10
Kelompok Bawah	2	2	0	4	1	1	10
Jumlah	8	4	0	6	1	1	20

Butir Soal Nomor 3

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	9	0	0	1	0	10
Kelompok Bawah	0	6	2	1	0	1	10
Jumlah	0	15	2	1	1	1	20

Butir Soal Nomor 4

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	0	4	5	0	0	10
Kelompok Bawah	6	0	3	1	0	0	10
Jumlah	7	0	7	6	0	0	20

Butir Soal Nomor 5

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	8	2	0	0	10
Kelompok Bawah	0	1	7	2	0	0	10
Jumlah	0	1	15	4	0	0	20

Butir Soal Nomor 6

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	3	1	3	0	3	0	10
Kelompok Bawah	4	3	3	0	0	0	10
Jumlah	7	4	6	0	3	0	20

Butir Soal Nomor 7

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	1	6	1	0	2	0	10
Kelompok Bawah	5	2	1	2	0	0	10
Jumlah	6	8	2	2	2	0	20

Butir Soal Nomor 8

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	5	2	2	0	1	0	10
Kelompok Bawah	2	1	3	2	2	0	10
Jumlah	7	3	5	2	3	0	20

Butir Soal Nomor 9

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	10	0	0	0	0	10
Kelompok Bawah	1	6	1	1	1	0	10
Jumlah	1	16	1	1	1	0	20

Butir Soal Nomor 10

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	2	4	4	0	0	0	10
Kelompok Bawah	2	6	0	1	1	0	10
Jumlah	4	10	4	1	1	0	20

Butir Soal Nomor 11

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	9	0	1	0	0	0	10
Kelompok Bawah	6	1	3	0	0	0	10
Jumlah	15	1	4	0	0	0	20

Butir Soal Nomor 12

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	2	7	1	0	10
Kelompok Bawah	2	2	2	1	3	0	10
Jumlah	2	2	4	8	4	0	20

Butir Soal Nomor 13

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	6	0	1	3	0	10
Kelompok Bawah	0	5	3	1	1	0	10
Jumlah	0	11	3	2	4	0	20

Butir Soal Nomor 14

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	2	2	2	0	4	0	10
Kelompok Bawah	3	4	1	1	1	0	10
Jumlah	5	6	3	1	5	0	20

Butir Soal Nomor 15

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	9	0	1	0	0	10
Kelompok Bawah	0	6	0	2	2	0	10
Jumlah	0	15	0	3	2	0	20

Butir Soal Nomor 16

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	10	0	0	0	0	0	10
Kelompok Bawah	9	0	0	0	1	0	10
Jumlah	19	0	0	0	1	0	20

Butir Soal Nomor 17

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	6	3	1	0	10
Kelompok Bawah	0	1	2	6	1	0	10
Jumlah	0	1	8	9	2	0	20

Butir Soal Nomor 18

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	2	4	3	0	0	10
Kelompok Bawah	1	5	4	0	0	0	10
Jumlah	2	7	8	3	0	0	20

Butir Soal Nomor 19

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	3	0	1	4	1	10
Kelompok Bawah	1	2		3	4	0	10
Jumlah	2	5	0	4	8	1	20

Butir Soal Nomor 20

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	1	5	2	1	1	0	10
Kelompok Bawah	6	3	1	0	0	0	10
Jumlah	7	8	3	1	1	0	20

Butir Soal Nomor 21

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	2	1	0	3	4	0	10
Kelompok Bawah	0	0	1	4	5	0	10
Jumlah	2	1	1	7	9	0	20

Butir Soal Nomor 22

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	1	8	1	0	0	10
Kelompok Bawah	0	1	7	1	1	0	10
Jumlah	0	2	15	2	1	0	20

Butir Soal Nomor 23

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	4	5	0	1	0	0	10
Kelompok Bawah	0	3	2	4	1	0	10
Jumlah	4	8	2	5	1	0	20

Butir Soal Nomor 24

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	0	1	8	0	0	10
Kelompok Bawah	1	2	3	3	1	0	10
Jumlah	2	2	4	11	1	0	20

Butir Soal Nomor 25

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	1	0	0	9	0	10
Kelompok Bawah	3	1	2	0	4	0	10
Jumlah	3	2	2	0	13	0	20

Butir Soal Nomor 26

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	5	3	1	1	0	0	10
Kelompok Bawah	1	6	1	2	0	0	10
Jumlah	6	9	2	3	0	0	20

Butir Soal Nomor 27

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	3	2	3	0	2	0	10
Kelompok Bawah	4	3	2	1	0	0	10
Jumlah	7	5	5	1	2	0	20

Butir Soal Nomor 28

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	1	1	5	1	1	10
Kelompok Bawah	1	2	2	3	2	0	10
Jumlah	2	3	3	8	3	1	20

Butir Soal Nomor 29

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	3	1	3	3	0	0	10
Kelompok Bawah	7	2	0	1	0	0	10
Jumlah	10	3	3	4	0	0	20

Butir Soal Nomor 30

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	2	0	0	7	0	10
Kelompok Bawah	2	3	1	2	2	0	10
Jumlah	3	5	1	2	9	0	20

Butir Soal Nomor 31

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	0	1	0	1	0	10
Kelompok Bawah	8	1	1	0	0	0	10
Jumlah	16	1	2	0	1	0	20

Butir Soal Nomor 32

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	3	2	1	1	3	0	10
Kelompok Bawah	3	3	1	1	2	0	10
Jumlah	6	5	2	2	5	0	20

Butir Soal Nomor 33

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	2	0	7	0	1	10
Kelompok Bawah	2	2	0	4	2	0	10
Jumlah	2	4	0	11	2	1	20

Butir Soal Nomor 34

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	10	0	0	0	0	10
Kelompok Bawah	0	8	1	1	0	0	10
Jumlah	0	18	1	1	0	0	20

Butir Soal Nomor 35

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	9	0	0	1	10
Kelompok Bawah	0	0	9	1	0	0	10
Jumlah	0	0	18	1	0	1	20

Butir Soal Nomor 36

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	0	0	9	1	10
Kelompok Bawah	0	0	0	1	9	0	10
Jumlah	0	0	0	1	18	1	20

Butir Soal Nomor 37

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	9	0	0	0	0	1	10
Kelompok Bawah	9	0	0	1	0	0	10
Jumlah	18	0	0	1	0	1	20

Butir Soal Nomor 38

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	9	0	0	0	1	10
Kelompok Bawah	1	8	0	0	0	1	10
Jumlah	1	17	0	0	0	2	20

Butir Soal Nomor 39

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	0	0	9	0	1	10
Kelompok Bawah	0	1	0	9	0	0	10
Jumlah	0	1	0	18	0	1	20

Butir Soal Nomor 40

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	1	8	0	0	1	10
Kelompok Bawah	2	0	6	1	1	0	10
Jumlah	2	1	14	1	1	1	20

Lampiran 37: Validasi Butir Paket Soal 4

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	Algoritma *Lucifer* merupakan algoritma yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit. Algoritma ini telah dimodifikasi sehingga menghasilkan sebuah algortima baru bernama... a. AES d. DES b. RC4 e. RSA c. A5	
	1) 10 putaran 2) 12 putaran 3) 14 putaran 4) 16 putaran Jumlah putaran yang digunakan setiap blok pada AES-256 adalah... a. 1) d. 4) b. 2) e. Semua jawaban benar c. 3)	
Mahasiswa dapat mengidentifikasikan serangan terhadap *cipher* aliran	*Ciphertext-only attack* dapat terjadi apabila... a. *Keystream* yang samadigunakandua kali terhadappotonganplainteks yang berbeda b. *Keystream generator* menghasilkan kunci yang sama c. Cipherteks menggunakan sebuah kunci yang dihasilkan oleh *keystream generator* d. Plainteks menggunakan sebuah kunci yang dihasilkan oleh *keystream generator* e. Cipherteks dihasilkan oleh rangkaian bit kunci yang sudah diubah oleh kriptanalis	
	Pada *flip-bit attack*, kriptanalis yang akan melakukan pengubahan pesan tidak perlu mengetahui... a. Cipherteks d. Keystream generator b. Plainteks e. Kunci c. Cipherteks dan plainteks	
Mahasiswa dapat mengidentifikasikan *cipher* blok	1) Substitusi 2) Transposisi 3) Faktorisasi 4) Diferensiasi Teknik di atas yang merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah... a. 1) dan 3) d. 1) b. 1) dan 2) e. 2) c. 2) dan 4)	

Indikator	Soal	Validasi Butir
	1) *Plaintext Block Chaining* (PBC) 2) *Plaintext Feedback* (PFC) 3) *Electronic Feedback* (EFB) 4) *Cipher Block Chaining* (CBC) 5) *Input Feedback* (IFB) Pada mode di atas yang merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah... a. 5) d. 2) b. 4) e. 1) c. 3)	
Mahasiswa dapat mendeskripsikan prinsip perancangan *cipher* blok	Prinsip perancangan *cipher* blok berupa *feistel network* berarti... a. Model jaringan yang membuat algoritma kriptografi menjadi *reversible* b. Model jaringan yang mendukung proses enkripsi c. Model jaringan yang mendukung proses dekripsi d. Model jaringan yang sulit untuk dilakukan *hijacking* e. Model jaringan yang membuat algoritma kriptografi menjadi aman dari kriptanalis	
	Prinsip perancangan *cipher* blok berupa *weak key* berarti... a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci b. Kunci acak hasil *keystream generator* sama dengan *keystream* sebelumnya c. Kunci yang sama digunakan pada dua cipherteks d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu	
Mahasiswa dapat mengidentifikasikan algoritma RSA	1) *p* dan *q* bilangan prima 2) *PK* (kunci enkripsi) 3) *SK* (kunci dekripsi) 4) *X* (plainteks) 5) *Y* (cipherteks) Besaran di atas yang bersifat tidak rahasia pada algoritma RSA adalah... a. 1) dan 4) d. 3) dan 4) b. 2) dan 3) e. 1) dan 5) c. 2) dan 5)	
	Kunci RSA pada umumnya memiliki panjang... a. 64 – 128 bit d. 512 – 1024 bit b. 128 – 256 bit e. 1024 – 2048 bit c. 256 – 512 bit	

Indikator	Soal	Validasi Butir
Mahasiswa dapat mengidentifikasikan algoritma *rabin*	Keamanan algoritma *Rabin* terletak pada... a. Sulitnya memfaktorkan bilangan prima menjadi bilangan bulat b. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima c. Sulitnya mencari faktor bilangan prima pada proses enkripsi d. Sulitnya mencari faktor bilangan prima pada proses dekripsi e. Sulitnya mencari faktor bilangan bulat menjadi bilangan desimal	
	Proses enkripsi pada algoritma *Rabin* dapat dilakukan dalam waktu yang relatif singkat sehingga memiliki keuntungan menghadapi keterbatasan *resource* yang ada pada media kriptografi seperti... a. *Smart card* b. Tanda tangan digital c. *E-commerce* d. Otentikasi pin e. Kartu kredit	
Mahasiswa dapat menjelaskan pembangkit bilangan acak semu	Salah satu syarat sebagai pembangkit bilangan acak yang cocok untuk kriptografi adalah.. a. Memori yang dibutuhkan tidak terlalu besar b. Data algoritma memiliki kompleksitas yang tinggi c. Nilai bilangan harus non-prima d. Lolos uji keacakan statistik e. Logaritma diskrit yang tidak mudah ditembus	
	Dibawah ini yang termasuk dalam contoh pembangkit bilangan acak semu, **kecuali**... a. *InitializationVector* b. *LinearCongruentialGenerator* c. *Blum Blum Shut* d. *Pseudo-RandomNumber Generator* e. *CryptographicallySecurePseudorandomGenerator*	
	Keamanan pembangkit bilangan acak *Blum Blum Shub* (BBS) terletak pada... a. Logaritma diskrit yang sulit dipecahkan b. Integral bilangan yang rumit c. Sulitnya memfaktorkan hasil kali dua bilangan prima d. Diferensial bilangan yang tidak mudah diketahui nilainya e. Nilai perpangkatan yang tinggi	

Indikator	Soal	Validitas Butir
Mahasiswa dapat mengidentifikasikan fungsi *hash* satu arah	Salah satu keuntungan penggunaan fungsi *hash* satu arah adalah... a. Algoritma tidak mudah diserang b. Menjaga integritas data c. Kompleksitas data bersifat tetap d. Kompleksitas memori hanya sedikit e. Data tersimpan dalam *host*	
	Kondisi dua *string* sembarang memiliki nilai *hash* yang sama disebut... a. *Chaos* d. *Keystream* *b.* Destruksi e. Kolisi *c. Message digest*	
	Salah satu sifat dari fungsi *hash* satu arah adalah... a. Fungsi *H* dapat diterapkan pada blok data berukuran berapa saja b. Setiap variabel pada fungsi *Hash* didapat dari pemfaktoran bilangan c. $H(x)$ sulit dihitung untuk setiap nilai x yang diberikan tetap d. Untuk setiap h yang dihasilkan, sangat mungkin dikembalikan nilai x sedemikian sehingga $H(x) = h$ e. Setiap variabel pada fungsi H bersifat bilangan non-prima	
Mahasiswa dapat menyebutkan algoritma MD5	Algoritma MD5 membutuhkan 4 buah *buffer* dengan panjang masing-masingnya adalah... a. 512 bit d. 32 bit b. 128 bit e. 64 bit c. 256 bit	
	Penemu dari kolisi algoritma MD5 adalah... a. Ron rivest d. Lucifer b. Charles Babbage e. Leonard Adleman c. Vlastimil Klima	
	Algoritma MD5 menghasilkan *message digest* dengan panjang... a. 32 bit d. 256 bit b. 64 bit e. 512 bit c. 128 bit	
Mahasiswa dapat mengidentifikasikan konsep tanda tangan digital	Kelemahan dari teknologi tanda tangan digital adalah... a. Membutuhkan proses yang lama untuk otentikasi data b. Memerlukan biaya tambahan secara institusional c. Mudah dipalsukan d. Penggunaan memori yang terlalu besar e. Kompleksitas integritas data yang sangat tinggi	

Indikator	Soal	Validitas Butir
	Kelebihan yang paling utama dari adanya tanda tangan digital adalah... a. Lebih terjaminnya otentikasi dari sebuah dokumen b. Proses pembuatan tanda tangan digital dilakukan dengan cepat c. Biaya yang dibutuhkan pada penggunaan tanda tangan digital relatif murah d. Integritas data yang baik dalam pengunaannya e. Tidak mudah diserang oleh kriptanalis	
	Otentikasi dokumen merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti... a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya	
Mahasiswa dapat mengidentifikasikan protokol kriptografi	Contoh aplikasi protokol yang dirancang untuk dipakai oleh kelompok yang terdiri dari lebih dari dua orang pemakai adalah... a. *E-mail* b. Internet c. *Skype* d. Telepon e. *Teleconferencing*	
	Hybrid Cryptosystem adalah... a. Sebuah sistem kriptografi yag digunakan untuk pertukaran pesan b. Pertukaran kunci yang dilakukan pada protokol sistem kriptografi c. Sistem kriptografi yang berhasil disadap oleh kriptanalis d. Dua gabungan sistem kriptografi yang digunakan pada sebuah protokol e. Protokol kriptografi yang menggunakan sebuah sistem kriptografi	

Indikator	Soal	Validasi Butir
	Protokol menandatangani dokumen digital dengan sistem kriptografi simetri dan juru penengah tidak praktis karena... a. Kunci harus tetap rahasia sebelum, sepanjang, dan setelah protokol b. Biaya opersional yang digunakan menjadi besar c. Proses sertifikasi keabsahan dokumen yang memakan waktu lama d. Algoritma protokol yang digunakan terlalu rumit e. Penggunaan protokol komunikasi dengan sistem kriptografi yang tidak aman	
Mahasiswa dapat menjelaskan pembangkit bilangan prima	Teknik yang akan membagi sebuah bilangan yang akan diuji dengan semua bilangan bulat positif yang lebih kecil dari akar bilangan tersebut disebut... a. *Brute force* b. *Pseudorandom generator* c. *Keystream generator* d. *Keystream* e. *Digital signature*	
Mahasiswa dapat mengidentifikasikan algoritma MAC	Penggunaan algoritma MAC yang berbasiskan DES-CBC adalah... a. *Electronic Code Book* b. *Data Authentication Algorithm* c. *Digital Signature Standard* d. *Output Feedback* e. *Cipher Feedback*	
	Pembangkitan nilai hash pada algoritma MAC membutuhkan kunci yang bersifat... a. Privat b. Publik c. Sementara d. Tetap e. Simetri	
Mahasiswa dapat menganalisis penggunaan kriptografi dalam kehidupan sehari-hari	1) Kartu kredit 2) Pemancar radio 3) Pay TV 4) Kartu cerdas 5) Satelit TV Contoh penggunaan kriptografi dalam kehidupan sehari-hari ditunjukkan oleh nomor... a. 1), 2), dan 3) b. 2), 3), dan 4) c. 2), 4), dan 5) d. 1), 3), dan 4) e. 3), 4), dan 5)	
	Sistem kriptografi yang digunakan pada komunikasi melalui GSM *mobile phone* adalah... a. Kunci publik b. Simetri c. *Stream cipher* d. *Caesar cipher* e. Asimetri	

Indikator	Soal	Validasi Butir
	GSM *mobile phone* diperlukan dua kebutuhan keamanan, yaitu... a. Kerahasiaan dan otentikasi penerima pesan b. Otentikasi pengirim dan penerima pesan c. Efisiensi dan integritas data d. Integritas data dan verifikasi data e. Kerahasiaan dan otentikasi pengguna	
Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi	Cipherteks dari "CUACA HARI INI SANGAT TIDAK MENENTU" dengan menggunakan aturan Caesar Cipher adalah... a. FXDFD KDUL LQL VDQJDW WLGDN PHQHQWX b. FXDFD KDUL LQL VDQJDW WLGDT PHQHQWX c. FXDFD KDUL LQL VDQJDW WLGDH PHQHQWX d. FXDFD KDUL LQL VDQJDW WLGDT PHQHQWD e. FXDFD KDUL LQL VDQJDW WLGDN PHQHQWD	
	Cipherteks dari "ALGORITMA KIRPTOGRAFI MODERN LEBIH RUMIT DARI PADA KLASIK" dengan menggunakan aturan Caesar Cipher adalah... a. DOJRULWPD NULSWRJUDIL PRGNUQ OHELK UXPLW GDUL SDGD NODVLN b. DOJRULWPD NULSWRJUDIL PRGHUQ OHELK UXPLW GDUL SDGD NODVLN c. DOJRULWPD NULSWRJUDIL PRGHUQ OHELK UXRLW GDUL SDGD NODVLN d. DOJRULWPD NULSWRJUDIL PRGHUQ ONELK UXPLW GDUL SDGD NODVLN e. DOJRUTWPD NULSWRJUDIL PRGNUQ OHELK UXRLW GDUL SDGD NODVLN	
	Cipherteks dari "PROGRAM STUDI PTIK JURUSAN TEKNIK ELEKTRO" dengan menggunakan aturan Caesar Cipher adalah... a. SURJUDP VWXGL SWLN MXUXVDQ WHNQLN HONNWUR b. SURJUDP VWXGL SWLN MXUVDQ WHNQLN HOHNWUIR c. SURJUDP VWXGL SWLN MXUXVDQ WHNQLN HOHNWUR d. SURJUDP VWXGL SWLN MXUNVDQ WHNQLN HOHNWUS e. SURJUDP VWXGL SWLN MXUXVDQ WHNOLN HOHNWUS	

Indikator	Soal	Validasi Butir
Mahasiswa dapat mengaplikasikan algoritma *cipher* transposisi	Cipherteks dari "MATERI KRIPTOGRAFI YANG DIUJIKAN DIMULAI DARI DES" dengan menggunakan aturan *blocking* berupa 3 blok adalah... a. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TIRTRIA_UK_MADIE b. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TIRTRA_UK_MADIE_ c. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TRTRIA_UK_MADIE d. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TIRTRIA_UK_MADIE_ e. ME_IOA_NDJADUIA_SARKPGFYGINIL_RD_TIRTRIA_UK_MADIE	
	Cipherteks dari "ISILAH SEMUA SOAL DENGAN BENAR" dengan menggunakan aturan *blocking* berupa 3 blok adalah... a. IL_M_ADG_NSASUSLEABAIHEAO_NHER b. IL_M_ADG_NSASUSLEABAINEAO_NNER c. IL_M_ADG_NSASUSLEABAIHEAO_NNER d. IL_M_ADG_NSASUSLEABAINEAO_HNER e. IL_M_ADG_NSASUSLEABAIHEAO_HNER	
	Cipherteks dari "FAKULTAS TEKNIK UNIVERSITAS NEGERI JAKARTA" dengan menggunakan aturan *blocking* berupa 2 blok adalah... a. FKLA_ENKUIESTSNGR_AATAUTSTKI_NVRTA_EEIJKRA b. FKLA_ENKUIESTSNGR_AATAUTSTKI_NVRIA_EEIJKRAI c. FKLA_ENKUIESTSNGR_ATAUTSTKI_NVRIA_EEIJKRA_ d. FKLA_ENKUIESTSNGR_AATAUTSTK_NVRIA_EEIJKRA_ e. FKLA_ENKUIESTSNGR_AATAUTSTKI_NVRIA_EEIJKRA	
Mahasiswa dapat menjelaskan *cipher* aliran	*Keystream* yang didapat dari *pseudo-random number generation* menggunakan kunci enkripsi merupakan cara pembuatan keystream pada kriptografi... a. *Cipher* aliran b. *Cipher* blok c. *Caesar Cipher* d. *Cipher* substitusi e. *Cipher* ekspansi	

Dosen Pengampu

Prasetyo Wibowo Yunanto, M.Eng

Lampiran 38: Paket Soal 4

1. Algoritma *Lucifer* merupakan algoritma yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit. Algoritma ini telah dimodifikasi sehingga menghasilkan sebuah algortima baru bernama...
   a. AES
   b. RC4
   c. A5
   d. DES
   e. RSA
2. 1) 10 putaran
   2) 12 putaran
   3) 14 putaran
   4) 16 putaran
   Jumlah putaran yang digunakan setiap blok pada AES-256 adalah...
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. Semua jawaban benar
3. *Ciphertext-only attack* dapat terjadi apabila...
   a. *Keystream* yang sama digunakan dua kali terhadap potongan plainteks yang berbeda
   b. *Keystream generator* menghasilkan kunci yang sama
   c. Cipherteks menggunakan sebuah kunci yang dihasilkan oleh *keystream generator*
   d. Plainteks menggunakan sebuah kunci yang dihasilkan oleh *keystream generator*
   e. Cipherteks dihasilkan oleh rangkaian bit kunci yang sudah diubah oleh kriptanalis
4. Pada flip-bit attack, kriptanalis yang akan melakukan pengubahan pesan tidak perlu mengetahui...
   a. Cipherteks
   b. Plainteks
   c. Cipherteks dan plainteks
   d. Keystream generator
   e. Kunci
5. 1) Substitusi
   2) Transposisi
   3) Faktorisasi
   4) Diferensiasi
   Teknik di atas yang merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah...
   a. 1) dan 3)
   b. 1) dan 2)
   c. 2) dan 4)
   d. 1)
   e. 2)
6. 1) *Plaintext Block Chaining* (PBC)
   2) *Plaintext Feedback* (PFC)
   3) *Electronic Feedback* (EFB)
   4) *Cipher Block Chaining* (CBC)
   5) *Input Feedback* (IFB)

Pada mode di atas yang merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah...

a. 5)
b. 4)
c. 3)
d. 2)
e. 1)

7. Prinsip perancangan *cipher* blok berupa *feistel network* berarti...
   a. Model jaringan yang membuat algoritma kriptografi menjadi *reversible*
   b. Model jaringan yang mendukung proses enkripsi
   c. Model jaringan yang mendukung proses dekripsi
   d. Model jaringan yang sulit untuk dilakukan *hijacking*
   e. Model jaringan yang membuat algoritma kriptografi menjadi aman dari kriptanalis
8. Prinsip perancangan *cipher* blok berupa *weak key* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Kunci acak hasil *keystream generator* sama dengan *keystream* sebelumnya
   c. Kunci yang sama digunakan pada dua cipherteks
   d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
   e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain
9. 1) *p* dan *q* bilangan prima
   2) *PK* (kunci enkripsi)
   3) *SK* (kunci dekripsi)
   4) *X* (plainteks)
   5) *Y* (cipherteks)

   Besaran di atas yang bersifat tidak rahasia pada algoritma RSA adalah...

   a. 1) dan 4)
   b. 2) dan 3)
   c. 2) dan 5)
   d. 3) dan 4)
   e. 1) dan 5)
10. Kunci RSA pada umumnya memiliki panjang...
    a. 64 – 128 bit
    b. 128 – 256 bit
    c. 256 – 512 bit
    d. 512 – 1024 bit
    e. 1024 – 2048 bit
11. Keamanan algoritma *Rabin* terletak pada...
    a. Sulitnya memfaktorkan bilangan prima menjadi bilangan bulat
    b. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima
    c. Sulitnya mencari faktor bilangan prima pada proses enkripsi
    d. Sulitnya mencari faktor bilangan prima pada proses dekripsi
    e. Sulitnya mencari faktor bilangan bulat menjadi bilangan desimal
12. Proses enkripsi pada algoritma *Rabin* dapat dilakukan dalam waktu yang relatif singkat sehingga memiliki keuntungan menghadapi keterbatasan *resource* yang ada pada media kriptografi seperti...

    a. *Smart card*
    d. Otentikasi pin

b. Tanda tangan digital
c. *E-commerce*
e. Kartu kredit

13. Salah satu syarat sebagai pembangkit bilangan acak yang cocok untuk kriptografi adalah..
    a. Memori yang dibutuhkan tidak terlalu besar
    b. Data algoritma memiliki kompleksitas yang tinggi
    c. Nilai bilangan harus non-prima
    d. Lolos uji keacakan statistik
    e. Logaritma diskrit yang tidak mudah ditembus
14. Dibawah ini yang termasuk dalam contoh pembangkit bilangan acak semu, **kecuali**...
    a. *InitializationVector*
    b. *Linear Congruential Generator*
    c. *Blum Blum Shut*
    d. *Pseudo-Random Number Generator*
    e. *Cryptographically Secure Pseudorandom Generator*
15. Keamanan pembangkit bilangan acak *Blum Blum Shub* (BBS) terletak pada...
    a. Logaritma diskrit yang sulit dipecahkan
    b. Integral bilangan yang rumit
    c. Sulitnya memfaktorkan hasil kali dua bilangan prima
    d. Diferensial bilangan yang tidak mudah diketahui nilainya
    e. Nilai perpangkatan yang tinggi
16. Salah satu keuntungan penggunaan fungsi *hash* satu arah adalah...
    a. Algoritma tidak mudah diserang
    b. Menjaga integritas data
    c. Kompleksitas data bersifat tetap
    d. Kompleksitas memori hanya sedikit
    e. Data tersimpan dalam *host*
17. Kondisi dua *string* sembarang memiliki nilai *hash* yang sama disebut...
    a. *Chaos*
    b. Destruksi
    c. *Message digest*
    d. *Keystream*
    e. Kolisi
18. Salah satu sifat dari fungsi *hash* satu arah adalah...
    a. Fungsi *H* dapat diterapkan pada blok data berukuran berapa saja
    b. Setiap variabel pada fungsi *Hash* didapat dari pemfaktoran bilangan
    c. $H(x)$ sulit dihitung untuk setiap nilai x yang diberikan tetap
    d. Untuk setiap h yang dihasilkan, sangat mungkin dikembalikan nilai x sedemikian sehingga $H(x) = h$
    e. Setiap variabel pada fungsi H bersifat bilangan non-prima
19. Algoritma MD5 membutuhkan 4 buah *buffer* dengan panjang masing-masingnya adalah...
    a. 512 bit
    b. 128 bit
    c. 256 bit
    d. 32 bit
    e. 64 bit

20. Penemu dari kolisi algoritma MD5 adalah...
    a. Ron rivest
    b. Charles Babbage
    c. Vlastimil Klima
    d. Lucifer
    e. Leonard Adleman
21. Algoritma MD5 menghasilkan *message digest* dengan panjang...
    a. 32 bit
    b. 64 bit
    c. 128 bit
    d. 256 bit
    e. 512 bit
22. Kelemahan dari teknologi tanda tangan digital adalah...
    a. Membutuhkan proses yang lama untuk otentikasi data
    b. Memerlukan biaya tambahan secara institusional
    c. Mudah dipalsukan
    d. Penggunaan memori yang terlalu besar
    e. Kompleksitas integritas data yang sangat tinggi
23. Kelebihan yang paling utama dari adanya tanda tangan digital adalah...
    a. Lebih terjaminnya otentikasi dari sebuah dokumen
    b. Proses pembuatan tanda tangan digital dilakukan dengan cepat
    c. Biaya yang dibutuhkan pada penggunaan tanda tangan digital relatif murah
    d. Integritas data yang baik dalam pengunaannya
    e. Tidak mudah diserang oleh kriptanalis
24. Otentikasi dokumen merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti...
    a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
    b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
    c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
    d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
    e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya
25. Contoh aplikasi protokol yang dirancang untuk dipakai oleh kelompok yang terdiri dari lebih dari dua orang pemakai adalah...
    a. *E-mail*
    b. Internet
    c. Skype
    d. Telepon
    e. *Teleconferencing*
26. *Hybrid Cryptosystem* adalah...
    a. Sebuah sistem kriptografi yag digunakan untuk pertukaran pesan
    b. Pertukaran kunci yang dilakukan pada protokol sistem kriptografi
    c. Sistem kriptografi yang berhasil disadap oleh kriptanalis
    d. Dua gabungan sistem kriptografi yang digunakan pada sebuah protokol
    e. Protokol kriptografi yang menggunakan sebuah sistem kriptografi

27. Protokol menandatangani dokumen digital dengan sistem kriptografi simetri dan juru penengah tidak praktis karena...
    a. Kunci harus tetap rahasia sebelum, sepanjang, dan setelah protokol
    b. Biaya opersional yang digunakan menjadi besar
    c. Proses sertifikasi keabsahan dokumen yang memakan waktu lama
    d. Algoritma protokol yang digunakan terlalu rumit
    e. Penggunaan protokol komunikasi dengan sistem kriptografi yang tidak aman
28. Teknik yang akan membagi sebuah bilangan yang akan diuji dengan semua bilangan bulat positif yang lebih kecil dari akar bilangan tersebut disebut...
    a. *Brute force*
    b. *Pseudorandom generator*
    c. *Keystream generator*
    d. *Keystream*
    e. *Digital signature*
29. Penggunaan algoritma MAC yang berbasiskan DES-CBC adalah...
    a. *Electronic Code Book*
    b. *Data Authentication Algorithm*
    c. *Digital Signature Standard*
    d. *Output Feedback*
    e. *Cipher Feedback*
30. Pembangkitan nilai hash pada algoritma MAC membutuhkan kunci yang bersifat...
    a. Privat
    b. Publik
    c. Sementara
    d. Tetap
    e. Simetri
31. 1) Kartu kredit
    2) Pemancar radio
    3) Pay TV
    4) Kartu cerdas
    5) Satelit TV

    Contoh penggunaan kriptografi dalam kehidupan sehari-hari ditunjukkan oleh nomor...
    a. 1), 2), dan 3)
    b. 2), 3), dan 4)
    c. 2), 4), dan 5)
    d. 1), 3), dan 4)
    e. 3), 4), dan 5)
32. Sistem kriptografi yang digunakan pada komunikasi melalui GSM *mobile phone* adalah...
    a. Kunci publik
    b. Simetri
    c. *Stream cipher*
    d. *Caesar cipher*
    e. Asimetri
33. GSM *mobile phone* diperlukan dua kebutuhan keamanan, yaitu...
    a. Kerahasiaan dan otentikasi penerima pesan
    b. Otentikasi pengirim dan penerima pesan
    c. Efisiensi dan integritas data
    d. Integritas data dan verifikasi data
    e. Kerahasiaan dan otentikasi pengguna

34. Cipherteks dari “CUACA HARI INI SANGAT TIDAK MENENTU” dengan menggunakan aturan Caesar Cipher adalah...
    a. FXDFD KDUL LQL VDQJDW WLGDN PHQHQWX
    b. FXDFD KDUL LQL VDQJDW WLGDT PHQHQWX
    c. FXDFD KDUL LQL VDQJDW WLGDH PHQHQWX
    d. FXDFD KDUL LQL VDQJDW WLGDT PHQHQWD
    e. FXDFD KDUL LQL VDQJDW WLGDN PHQHQWD
35. Cipherteks dari “ALGORITMA KIRPTOGRAFI MODERN LEBIH RUMIT DARI PADA KLASIK” dengan menggunakan aturan Caesar Cipher adalah...
    a. DOJRULWPD NULSWRJUDIL PRGNUQ OHELK UXPLW GDUL SDGD NODVLN
    b. DOJRULWPD NULSWRJUDIL PRGHUQ OHELK UXPLW GDUL SDGD NODVLN
    c. DOJRULWPD NULSWRJUDIL PRGHUQ OHELK UXRLW GDUL SDGD NODVLN
    d. DOJRULWPD NULSWRJUDIL PRGHUQ ONELK UXPLW GDUL SDGD NODVLN
    e. DOJRUTWPD NULSWRJUDIL PRGNUQ OHELK UXRLW GDUL SDGD NODVLN
36. Cipherteks dari “PROGRAM STUDI PTIK JURUSAN TEKNIK ELEKTRO” dengan menggunakan aturan Caesar Cipher adalah...
    a. SURJUDP VWXGL SWLN MXUXVDQ WHNQLN HONNWUR
    b. SURJUDP VWXGL SWLN MXUVDQ WHNQLN HOHNWUIR
    c. SURJUDP VWXGL SWLN MXUXVDQ WHNQLN HOHNWUR
    d. SURJUDP VWXGL SWLN MXUNVDQ WHNQLN HOHNWUS
    e. SURJUDP VWXGL SWLN MXUXVDQ WHNOLN HOHNWUS
37. Cipherteks dari “MATERI KRIPTOGRAFI YANG DIUJIKAN DIMULAI DARI DES” dengan menggunakan aturan *blocking* berupa 3 blok adalah...
    a. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TIRTRIA_UK_MADIE
    b. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TIRTRA_UK_MADIE_
    c. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TRTRIA_UK_MADIE
    d. ME_IOA_NDJADUIA_SARKPGFYGIINIL_RD_TIRTRIA_UK_MADIE_
    e. ME_IOA_NDJADUIA_SARKPGFYGINIL_RD_TIRTRIA_UK_MADIE
38. Cipherteks dari “ISILAH SEMUA SOAL DENGAN BENAR” dengan menggunakan aturan *blocking* berupa 3 blok adalah...
    a. IL_M_ADG_NSASUSLEABAIHEAO_NHER
    b. IL_M_ADG_NSASUSLEABAINEAO_NNER
    c. IL_M_ADG_NSASUSLEABAIHEAO_NNER
    d. IL_M_ADG_NSASUSLEABAINEAO_HNER
    e. IL_M_ADG_NSASUSLEABAIHEAO_HNER
39. Cipherteks dari “FAKULTAS TEKNIK UNIVERSITAS NEGERI JAKARTA” dengan menggunakan aturan *blocking* berupa 2 blok adalah...
    a. FKLA_ENKUIESTSNGR_AATAUTSTKI_NVRTA_EEIJKRA
    b. FKLA_ENKUIESTSNGR_AATAUTSTKI_NVRIA_EEIJKRAI

c. FKLA_ENKUIESTSNGR_ATAUTSTKI_NVRIA_EEIJKRA_
d. FKLA_ENKUIESTSNGR_AATAUTSTK_NVRIA_EEIJKRA_
e. FKLA_ENKUIESTSNGR_AATAUTSTKI_NVRIA_EEIJKRA

40. *Keystream* yang didapat dari *pseudo-random number generation* menggunakan kunci enkripsi merupakan cara pembuatan keystream pada kriptografi...
    a. *Cipher* aliran
    b. *Cipher* blok
    c. *Caesar Cipher*
    d. *Cipher* substitusi
    e. *Cipher* ekspansi

VALIDITAS BUTIR SOAL PILIHAN GANDA dengan Korelasi Produk Moment
Taraf Signifikan = 5%

NO	Nama	Butir Soal																																					Skor Total (Y)	Y2	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40			
1	Nur Fadhilah Safitri	1	1	1	1	1	1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	0	1	1	0	30	900	
2	Dini Novianti	1	0	1	1	1	1	1	1	0	1	0	1	0	1	0	1	1	1	1	0	1	0	0	1	1	0	1	1	0	0	1	1	1	1	1	1	1	1	1	0	28	784	
3	Aditya Fathurohman	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	0	1	1	1	1	1	0	0	0	1	1	1	1	1	1	0	1	1	0	30	900	
4	Akbar Jaya	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	1	1	0	33	1089	
5	Vina Septiani	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1	1	1	1	18	324	
6	Muhammad Aldi Azmy	0	0	0	1	1	1	0	0	1	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	1	1	1	1	0	17	289	
7	Annisa Aprilianti	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	1	1	0	1	1	1	1	1	1	1	0	15	225	
8	Moctar Afendi	0	0	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	1	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	30	900	
9	Engki Budi Adiyanto	1	0	0	1	1	1	0	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	1	1	1	0	1	1	1	1	0	1	0	17	289	
10	Citra Lestari Sibarani	1	0	0	1	1	1	1	1	1	0	1	0	0	1	0	1	0	1	1	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	30	900	
11	Siti Roosniah	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	0	0	1	0	1	0	0	1	1	0	1	1	1	1	1	1	1	17	289	
12	Dios Athina Malonda	0	0	0	1	1	1	1	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	1	1	1	0	1	1	0	1	1	1	20	400	
13	Rona Cahyanto	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	0	1	0	1	1	1	1	1	1	0	0	0	0	1	0	1	1	1	1	1	0	0	0	1	27	729	
14	Rangga Bintang R.	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	1	1	0	15	225	
15	Muhamad Rizki	0	0	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	25	625	
16	Ivan Firman	0	0	1	0	1	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	1	0	16	256	
17	Lestiana K. H.	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	1	0	0	0	1	0	1	1	0	1	1	1	0	1	1	1	17	289	
18	Setiawan Bayu Puja Saputra	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	1	0	0	1	1	0	1	1	1	1	0	1	1	0	15	225	
19	Rendra Andika	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	1	0	17	289	
20	Ahmad Salahuddin Mauludi	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	17	289	
	Benar (∑X)	10	4	8	14	16	15	12	9	7	9	7	7	7	11	3	12	7	12	7	5	12	8	16	12	9	8	7	8	5	7	18	16	13	20	19	20	12	17	19	6	434	10216	188356
	Salah	10	16	12	6	4	5	8	11	13	11	13	13	13	9	17	8	13	8	13	15	8	12	4	8	11	12	13	12	15	13	2	4	7	0	1	0	8	3	1	14			
	∑XY	247	120	203	334	350	353	292	227	182	228	191	185	151	275	90	291	179	291	186	137	289	206	357	292	198	210	189	208	109	149	377	370	314	434	417	434	246	374	407	124			
	rxy	0,475	0,657	0,475	0,522	0,055	0,503	0,511	0,504	0,499	0,520	0,649	0,549	-0,015	0,577	0,552	0,494	0,450	0,494	0,566	0,521	0,462	0,523	0,194	0,511	0,043	0,588	0,616	0,556	0,009	-0,048	-0,359	0,451	0,529	#DIV/0!	0,171	#DIV/0!	-0,233	0,113	-0,192	-0,107			
	R Tabel	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444	0,444			
	Keterangan	Valid	Valid	Valid	Valid	Tidak Vali	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Tidak Vali	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Valid	Tidak Vali	Valid	Tidak Vali	Valid	Valid	Valid	Tidak Vali	Tidak Vali	Tidak Vali	Valid	Valid	#DIV/0!	Tidak Vali	#DIV/0!	Tidak Vali	Tidak Vali	Tidak Vali	Tidak Vali			

Tingkat Kesukaran	0,5	0,2	0,4	0,7	0,8	0,75	0,6	0,45	0,35	0,45	0,35	0,35	0,35	0,55	0,15	0,6	0,35	0,6	0,35	0,25	0,6	0,4	0,8	0,6	0,45	0,4	0,35	0,4	0,25	0,35	0,9	0,8	0,65	1	0,95	1	0,6	0,85	0,95	0,3
Indeks	Sedang	Sukar	Sedang	Mudah	Mudah	Mudah	Sedang	Sedang	Sedang	Sedang	Sedang	Sedang	Sedang	Sedang	Sukar	Sedang	Sedang	Sedang	Sedang	Sukar	Sedang	Sedang	Mudah	Sedang	Sedang	Sedang	Sedang	Sedang	Sukar	Sedang	Mudah	Mudah	Sedang	Mudah	Mudah	Mudah	Sedang	Mudah	Mudah	Mudah	Sedang

DATA KELOMPOK ATAS

NO	Nama	Butir Soal																																								Skor Total (Y)
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
1	Akbar Jaya	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	1	1	0	33
2	Aditya Fathurohman	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	0	1	1	1	1	0	0	0	1	1	1	1	1	1	1	0	1	1	0	30
3	Moctar Afendi	0	0	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	1	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1	0	30
4	Nur Fadhilah Safitri	1	1	1	1	1	1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	0	1	1	0	30
5	Citra Lestari Sibarani	1	0	0	1	1	1	1	1	1	0	1	0	0	1	0	1	0	1	1	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	30
6	Dini Novianti	1	0	1	1	1	1	1	1	0	1	0	1	0	1	0	1	1	1	1	0	1	0	0	1	1	0	1	1	0	0	1	1	1	1	1	1	1	1	1	0	28
7	Rona Cahyanto	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	0	1	0	1	1	1	1	1	1	0	0	0	0	1	0	1	1	1	1	1	0	0	0	1	27
8	Muhamad Rizki	0	0	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	25
9	Dios Athina Malonda	0	0	0	1	1	1	1	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1	0	1	1	1	20
10	Vina Septiani	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1	1	1	1	18
	Total Benar	7	4	6	9	8	10	8	6	5	6	6	6	4	8	3	8	5	8	6	4	8	6	9	9	4	6	7	6	2	4	8	9	9	10	10	10	5	9	9	4	271

DATA KELOMPOK BAWAH

NO	Nama	Butir Soal																																								Skor Total
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
1	Lestiana K. H.	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	1	0	1	0	0	0	1	0	1	1	0	1	1	1	0	1	1	1	17
2	Muhammad Aldi Azmy	0	0	0	1	1	1	0	0	1	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	1	1	1	1	0	17
3	Engki Budi Adiyanto	1	0	0	1	1	1	0	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	1	1	1	0	1	1	1	1	0	1	0	17
4	Siti Roosniah	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0	1	1	1	1	1	1	1	17
5	Rendra Andika	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	1	0	17
6	Ahmad Salahuddin Mauludi	1	0	0	0	0	0	1	1	0	0	0	1	0	0	0	1	0	1	0	0	0	0	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	0	17
7	Ivan Firman	0	0	1	0	1	1	0	0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	1	0	16
8	Annisa Aprilianti	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	1	1	0	1	1	1	1	1	1	0	15
9	Rangga Bintang R.	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	1	0	1	1	1	1	1	1	1	0	15
10	Setiawan Bayu Puja Saputra	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	1	1	0	15
	Total Benar	3	0	2	5	8	5	4	3	2	3	1	1	3	3	0	4	2	4	1	1	4	2	7	3	5	2	0	2	3	3	10	7	4	10	9	10	7	8	10	2	163

Daya Beda	0,4	0,4	0,4	0,4	0	0,5	0,4	0,3	0,3	0,3	0,5	0,5	0,1	0,5	0,3	0,4	0,3	0,4	0,5	0,3	0,4	0,4	0,2	0,6	-0,1	0,4	0,7	0,4	-0,1	0,1	-0,2	0,2	0,5	0	0,1	0	-0,2	0,1	-0,1	0,2

Butir Soal Nomor 1

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	0	0	7	2	0	10
Kelompok Bawah	6	0	1	3	0	0	10
Jumlah	7	0	1	10	2	0	20

Butir Soal Nomor 2

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	1	4	4	1	0	10
Kelompok Bawah	0	1	0	7	2	0	10
Jumlah	0	2	4	11	3	0	20

Butir Soal Nomor 3

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	0	1	0	1	2	10
Kelompok Bawah	2	1	4	1	1	1	10
Jumlah	8	1	5	1	2	3	20

Butir Soal Nomor 4

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	0	0	9	1	10
Kelompok Bawah	0	2	0	3	5	0	10
Jumlah	0	2	0	3	14	1	20

Butir Soal Nomor 5

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	8	0	2	0	0	10
Kelompok Bawah	1	8	0	0	1	0	10
Jumlah	1	16	0	2	1	0	20

Butir Soal Nomor 6

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	10	0	0	0	0	10
Kelompok Bawah	0	5	0	0	5	0	10
Jumlah	0	15	0	0	5	0	20

Butir Soal Nomor 7

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	1	0	1	0	0	10
Kelompok Bawah	4	1	2	0	3	0	10
Jumlah	12	2	2	1	3	0	20

Butir Soal Nomor 8

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	1	1	6	1	0	10
Kelompok Bawah	2	1	1	3	3	0	10
Jumlah	3	2	2	9	4	0	20

Butir Soal Nomor 9

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	2	1	5	0	2	0	10
Kelompok Bawah	4	1	2	1	2	0	10
Jumlah	6	2	7	1	4	0	20

Butir Soal Nomor 10

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	1	2	0	6	0	10
Kelompok Bawah	1	3	2	1	3	0	10
Jumlah	2	4	4	1	9	0	20

Butir Soal Nomor 11

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	6	3	1	0	0	10
Kelompok Bawah	0	1	3	6	0	0	10
Jumlah	0	7	6	7	0	0	20

Butir Soal Nomor 12

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	2	0	1	1	0	10
Kelompok Bawah	1	3	1	4	1	0	10
Jumlah	7	5	1	5	2	0	20

Butir Soal Nomor 13

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	2	1	4	3	0	10
Kelompok Bawah	1	4	0	3	2	0	10
Jumlah	1	6	1	7	5	0	20

Butir Soal Nomor 14

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	0	1	0	0	1	10
Kelompok Bawah	3	1	3	3	0	0	10
Jumlah	11	1	4	3	0	1	20

Butir Soal Nomor 15

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	3	2	3	1	1	0	10
Kelompok Bawah	3	3	0	3	1	0	10
Jumlah	6	5	3	4	2	0	20

Butir Soal Nomor 16

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	1	8	1	0	0	0	10
Kelompok Bawah	3	4	2	1	0	0	10
Jumlah	4	12	3	1	0	0	20

Butir Soal Nomor 17

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	2	0	3	0	5	0	10
Kelompok Bawah	4	1	1	2	2	0	10
Jumlah	6	1	4	2	7	0	20

Butir Soal Nomor 18

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	8	0	0	2	0	0	10
Kelompok Bawah	4	1	1	4	0	0	10
Jumlah	12	1	1	6	0	0	20

Butir Soal Nomor 19

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	2	1	6	0	0	10
Kelompok Bawah	2	4	0	1	3	0	10
Jumlah	3	6	1	7	3	0	20

Butir Soal Nomor 20

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	4	1	4	0	1	0	10
Kelompok Bawah	6	2	1	0	1	0	10
Jumlah	10	3	5	0	2	0	20

Butir Soal Nomor 21

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	8	0	2	0	10
Kelompok Bawah	0	0	4	3	3	0	10
Jumlah	0	0	12	3	5	0	20

Butir Soal Nomor 22

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	2	6	0	1	1	0	10
Kelompok Bawah	5	2	2	0	1	0	10
Jumlah	7	8	2	1	2	0	20

Butir Soal Nomor 23

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	9	1	0	0	0	0	10
Kelompok Bawah	7	2	0	1	0	0	10
Jumlah	16	3	0	1	0	0	20

Butir Soal Nomor 24

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	0	9	0	0	0	10
Kelompok Bawah	1	4	3	2	0	0	10
Jumlah	2	4	12	2	0	0	20

Butir Soal Nomor 25

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	4	1	0	4	0	10
Kelompok Bawah	2	2	0	1	5	0	10
Jumlah	3	6	1	1	9	0	20

Butir Soal Nomor 26

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	1	0	0	6	2	1	10
Kelompok Bawah	5	1	1	2	1	0	10
Jumlah	6	1	1	8	3	1	20

Butir Soal Nomor 27

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	2	0	7	0	1	0	10
Kelompok Bawah	3	2	0	4	1	0	10
Jumlah	5	2	7	4	2	0	20

Butir Soal Nomor 28

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	3	0	0	0	1	10
Kelompok Bawah	2	3	3	1	1	0	10
Jumlah	8	6	3	1	1	1	20

Butir Soal Nomor 29

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	3	2	2	0	3	0	10
Kelompok Bawah	3	3	4	0	0	0	10
Jumlah	6	5	6	0	3	0	20

Butir Soal Nomor 30

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	4	3	0	3	0	0	10
Kelompok Bawah	3	1	0	3	3	0	10
Jumlah	7	4	0	6	3	0	20

Butir Soal Nomor 31

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	0	1	0	8	1	0	10
Kelompok Bawah	0	0	0	10	0	0	10
Jumlah	0	1	0	18	1	0	20

Butir Soal Nomor 32

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	9	0	0	1	10
Kelompok Bawah	2	2	6	0	0	0	10
Jumlah	2	2	15	0	0	1	20

Butir Soal Nomor 33

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	0	0	1	0	9	0	10
Kelompok Bawah	1	3	2	0	4	0	10
Jumlah	1	3	3	0	13	0	20

Butir Soal Nomor 34

Pilihan Jawab	a*	b	c	d	e	O	Jumlah
Kelompok Atas	6	0	4	0	0	0	10
Kelompok Bawah	8	0	2	0	0	0	10
Jumlah	14	0	6	0	0	0	20

Butir Soal Nomor 35

Pilihan Jawab	a	b*	c	d	e	O	Jumlah
Kelompok Atas	0	10	0	0	0	0	10
Kelompok Bawah	1	9	0	0	0	0	10
Jumlah	1	19	0	0	0	0	20

Butir Soal Nomor 36

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	0	0	10	0	0	0	10
Kelompok Bawah	0	0	10	0	0	0	10
Jumlah	0	0	20	0	0	0	20

Butir Soal Nomor 37

Pilihan Jawab	a	b	c	d*	e	O	Jumlah
Kelompok Atas	3	0	1	5	1	0	10
Kelompok Bawah	2	1	0	7	0	0	10
Jumlah	5	1	1	12	1	0	20

Butir Soal Nomor 38

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	1	0	9	0	0	0	10
Kelompok Bawah	0	2	8	0	0	0	10
Jumlah	1	2	17	0	0	0	20

Butir Soal Nomor 39

Pilihan Jawab	a	b	c	d	e*	O	Jumlah
Kelompok Atas	1	0	2	0	7	0	10
Kelompok Bawah	0	0	0	0	10	0	10
Jumlah	1	0	2	0	17	0	20

Butir Soal Nomor 40

Pilihan Jawab	a	b	c*	d	e	O	Jumlah
Kelompok Atas	4	3	3	0	0	0	10
Kelompok Bawah	2	0	1	4	1	2	10
Jumlah	6	3	4	4	1	2	20

Lampiran 40: Kisi-kisi Instrumen Bank Soal Mata Kuliah Kriptografi

Universitas : Universitas Negeri Jakarta

Mata Kuliah : Kriptografi

Jumlah Soal : 284

Bentuk Soal : Pilihan Ganda

No.	Materi Pokok	Indikator	Jumlah Soal	Taksonomi Bloom
1	Pengantar kriptografi	Mahasiswa dapat mendeskripsikan terminologi kriptografi	6	C1
		Mahasiswa dapat mengidentifikasikan tujuan kriptografi	6	C1
		Mahasiswa dapat menyebutkan sejarah kriptografi	8	C1
		Mahasiswa dapat mendefinisikan pengertian dari kriptanalisis	6	C1
		Mahasiswa dapat mengidentifikasikan perbedaan antara kriptografi kunci simetris dengan kriptografi kunci asimetris	6	C1
2	Serangan terhadap kriptografi	Mahasiswa dapat menjelaskan fungsi keamanan algoritma kriptografi	5	C2
		Mahasiswa dapat menyebutkan jenis-jenis serangan terhadap kriptografi	5	C1
		Mahasiswa dapat mengidentifikasikan kompleksitas serangan terhadap kriptografi	6	C1
3	Landasan matematika pada kriptografi	Mahasiswa dapat menerapkan penggunaan fungsi matematika pada kriptografi	6	C3
		Mahasiswa dapat menghitung fungsi permutasi	8	C3

No.	Materi Pokok	Indikator	Jumlah Soal	Taksonomi Bloom
		Mahasiswa dapat menghitung fungsi kombinasi	7	C3
		Mahasiswa dapat menerapkan teori peluang	7	C3
		Mahasiswa dapat menerapkan teori bilangan	5	C3
4	Algoritma kriptografi klasik	Mahasiswa dapat mengplikasikan algoritma *cipher* subtitusi	6	C3
		Mahasiswa dapat mengplikasikan algoritma *cipher* transposisi	7	C3
		Mahasiswa dapat mengplikasikan algoritma *affine cipher*	9	C3
		Mahasiswa dapat mengplikasikan algoritma *vigenere*	5	C3
		Mahasiswa dapat mengplikasikan algoritma *playfair*	6	C3
		Mahasiswa dapat mengaplikasikan algoritma *one-time pad*	**6**	C3
5	Algoritma kriptografi modern	Mahasiswa dapat menerapkan rangkaian bit dan operasinya	5	C3
		Mahasiswa dapat menerapkan algoritma enkripsi dengan XOR sederhana	6	C3
		Mahasiswa dapat mengoperasikan pembangkitan kunci	7	C3
		Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES	9	C1
		Mahasiswa dapat mengidentifikasikan perbedaan antara RC4 dengan A5	5	C1
		Mahasiswa dapat menjelaskan *cipher* aliran	5	C2
		Mahasiswa dapat mengidentifikasikan serangan terhadap *cipher* aliran	10	C1

No.	Materi Pokok	Indikator	Jumlah Soal	Taksonomi Bloom
		Mahasiswa dapat mengidentifikasikan *cipher* blok	9	C1
		Mahasiswa dapat mendeskripsikan prinsip perancangan *cipher* blok	11	C1
6	Kriptografi kunci publik	Mahasiswa dapat menjelaskan konsep kriptografi kunci publik	5	C2
		Mahasiswa dapat mengidentifikasikan algoritma RSA	12	C1
		Mahasiswa dapat menjelaskan algoritma *ElGamal*	5	C2
		Mahasiswa dapat mengidentifikasikan algoritma *rabin*	11	C1
		Mahasiswa dapat menjelaskan pembangkit bilangan prima	5	C2
		Mahasiswa dapat menjelaskan pembangkit bilangan acak semu	10	C2
7	Fungsi *hash* dan tanda tangan digital	Mahasiswa dapat mengidentifikasikan fungsi *hash* satu arah	9	C1
		Mahasiswa dapat menyebutkan algoritma MD5	10	C1
		Mahasiswa dapat mengidentifikasikan algoritma MAC	8	C1
		Mahasiswa dapat mengidentifikasikan konsep tanda tangan digital	8	C1
		Mahasiswa dapat mengidentifikasikan protokol kriptografi	9	C1
8	Kriptografi dalam kehidupan sehari-hari	Mahasiswa dapat menganalisis penggunaan kriptografi dalam kehidupan sehari-hari	5	C4

Lampiran 41: Bank Soal Mata Kuliah Kriptografi

Indikator: Mahasiswa dapat mendeskripsikan terminologi kriptografi

Soal:

1. Pesan berupa teks, gambar, audio, video dalam kriptografi disebut...
   a. Cipherteks
   b. Plainteks
   c. Enkripsi
   d. Dekripsi
   e. Kunci algoritma

   Kunci Jawaban: b. Plainteks

2. Enkripsi adalah...
   a. Proses menyandikan plainteks menjadi cipherteks
   b. Pesan berupa teks, gambar, audio, video dalam kriptografi
   c. Pesan yang telah disandikan sehingga tidak memiliki makna
   d. Data yang dapat dibaca dan memiliki makna
   e. Proses menerjemahkan cipherteks menjadi plainteks

   Kunci Jawaban: a. Proses menyandikan plainteks menjadi cipherteks

3. Dekripsi adalah...
   a. Proses menyandikan plainteks menjadi cipherteks
   b. Pesan berupa teks, gambar, audio, video dalam kriptografi
   c. Pesan yang telah disandikan sehingga tidak memiliki makna
   d. Data yang dapat dibaca dan memiliki makna
   e. Proses menerjemahkan cipherteks menjadi plainteks

   Kunci Jawaban: e. Proses menerjemahkan cipherteks menjadi plainteks

4. Kriptografi merupakan serapan bahasa yunani yang berarti...
   a. *Secret*
   b. *Secret Reading*
   c. *Secret Writing*
   d. *Writing*
   e. *Hiding*

   Kunci Jawaban: c. *Secret Writing*

5. Pembuat sistem kriptografi disebut...
   a. Kriptografer
   b. Kriptografi
   c. Kriptologi
   d. Kriptanalisis
   e. Kriptanalis

   Kunci Jawaban: a. Kriptografer

6. Studi mengenai kriptografi dan kriptanalisis disebut...
   a. Kriptografi
   d. Kriptografer

b. Kriptanalisis
c. Kriptanalis
e. Kriptologi

Kunci Jawaban: e. Kriptologi

Indikator: Mahasiswa dapat mengidentifikasikan tujuan kriptografi

Soal:

1. Di bawah ini yang bukan merupakan tujuan dari kriptografi adalah...
   a. Kerahasiaan
   b. Integritas data
   c. Autentikasi
   d. Non-repudiasi
   e. Ketepatan waktu

   Kunci Jawaban: e. Ketepatan waktu

2. Pesan yang telah dikirim tidak akan dapat dibatalkan mendefinisikan tujuan kriptografi berupa...
   a. Kerahasiaan
   b. Integritas data
   c. Autentikasi
   d. Non-repudiasi
   e. Ketepatan waktu

   Kunci Jawaban: d. Non-repudiasi

3. Di bawah ini yang merupakan salah satu tujuan dari kriptografi adalah...
   a. Kerahasiaan
   b. Ketepatan Waktu
   c. Kecepatan
   d. Ketelitian
   e. Ketepatan kunci

   Kunci Jawaban: a. Kerahasiaan

4. Tujuan kriptografi yang bersifat integritas data berarti...
   a. Menjaga isi informasi dari siapapun kecuali yang memiliki otoritas
   b. Penjagaan dari perubahan data yang tidak sah
   c. Identifikasi baik secara kesatuan sistem maupun informasi itu sendiri
   d. Pesan yang telah dikirim tidak akan dapat dibatalkan
   e. Pembuatan kunci yang sulit diprediksi

   Kunci Jawaban: b. Penjagaan dari perubahan data yang tidak sah

5. Tujuan kriptografi yang bersifat autentikasi berarti...
   a. Menjaga isi informasi dari siapapun kecuali yang memiliki otoritas
   b. Penjagaan dari perubahan data yang tidak sah
   c. Identifikasi baik secara kesatuan sistem maupun informasi itu sendiri
   d. Pesan yang telah dikirim tidak akan dapat dibatalkan
   e. Pembuatan kunci yang sulit diprediksi

Kunci Jawaban: c. Identifikasi baik secara kesatuan sistem maupun informasi itu sendiri

6. Tujuan kriptografi yang bersifat non-repudiasi berarti...
   a. Menjaga isi informasi dari siapapun kecuali yang memiliki otoritas
   b. Penjagaan dari perubahan data yang tidak sah
   c. Identifikasi baik secara kesatuan sistem maupun informasi itu sendiri
   d. Pesan yang telah dikirim tidak akan dapat dibatalkan
   e. Pembuatan kunci yang sulit diprediksi

   Kunci Jawaban: d. Pesan yang telah dikirim tidak akan dapat dibatalkan

Indikator: Mahasiswa dapat menyebutkan sejarah kriptografi

Soal:

1. Ukiran rahasia yang digunakan bangsa mesir untuk menyampaikan pesan kepada orang-orang yang berhak disebut...
   a. *Scytale*
   b. *Hieroglyphics*
   c. *Risalah fi Istikhraj al-Mu'amma*
   d. *Al-Kindi*
   e. *Steganografi*

   Kunci Jawaban: b. *Hieroglyphics*

2. Pita panjang berbahan daun papyrus yang dibaca dengan cara digulungkan ke sebatang silinder merupakan kriptografi bangsa yunani yang disebut..
   a. *Scytale*
   b. *Hieroglyphics*
   c. *Risalah fi Istikhraj al-Mu'amma*
   d. *Al-Kindi*
   e. *Steganografi*

   Kunci Jawaban: a. *Scytale*

3. Buku yang berisikan tentang penjelasan teknik analisis frekuensi kriptanalisis yang pertama kalinya pada abad 9 M berjudul...
   a. *Scytale*
   b. *Hieroglyphics*
   c. *Risalah fi Istikhraj al-Mu'amma*
   d. *Al-Kindi*
   e. *Steganografi*

   Kunci Jawaban: c. *Risalah fi Istikhraj al-Mu'amma*

4. Menyembunyikan kehadiran pesan sehingga pesan tersebut menjadi rahasia disebut...
   a. *Scytale*
   b. *Hieroglyphics*
   c. *Risalah fi Istikhraj al-Mu'amma*
   d. *Al-Kindi*
   e. *Steganografi*

Kunci Jawaban: e. *Steganografi*

5. Sebuah mesin yang digunakan sebagai alat untuk mengenkripsi pesan rahasia oleh Jerman pada perang dunia II adalah...
   a. Enigma
   b. Bombe
   c. Christoper
   d. Turing machine
   e. Maide Vale

   Kunci Jawaban: a. Enigma

6. Pada dasarnya semua sandi tetap rentan kepada kriptanalisis menggunakan teknik analisis frekuensi hingga pengembangan dari sandi polyalphabetic merupakan penjelasan oleh...
   a. Julis Caesar
   b. Charles Babbage
   c. Leon Battista Alberti
   d. Friedrich Kasiski
   e. Auguste Kerckhoffs

   Kunci Jawaban: c. Leon Battista Alberti

7. Pada pertengahan abad ke-19 orang yang menunjukkan bahwa sandi Vigenère sangat rentan terhadap *pemeriksaan Kasiski* adalah...
   a. Charles Babbage
   b. Julius Caesar
   c. Auguste Kerckhoffs
   d. Leon Alberti
   e. Claude Shannon

   Kunci Jawaban: a. Charles Babbage

8. Alat sandi pertama kali berupa tangkai yang digunakan oleh bangsa Spartan sebagai alat bantuk untuk memindahkan sandi adalah...
   a. *Kasiski*
   b. *Scytale*
   c. *Alberti*
   d. *Vigenere*
   e. *Shannon*

   Kunci Jawaban: b. *Scytale*

Indikator: Mahasiswa dapat mendefinisikan pengertian dari kriptanalisis

Soal:

1. Menemukan plainteks, kunci atau algoritma merupakan tujuan...
   a. Kriptografi
   b. Kriptografer
   c. Kriptanalisis
   d. Kriptanalis
   e. Kriptologi

   Kunci Jawaban: c. Kriptanalisis

2. Istilah yang digunakan untuk mempelajari metode untuk memperoleh arti dari informasi enkripsi tanpa mengakses sandi secara normal yang dibutuhkan untuk melakukannya adalah..
   a. Kriptografi
   b. Kriptografer
   c. Kriptanalisis
   d. Kriptanalis
   e. Kriptologi

   Kunci Jawaban: c. Kriptanalisis

3. Ilmu yang mempelajari cara untuk memecahkan algoritma enkripsi atau implementasinya disebut..
   a. Kriptografi
   b. Kriptografer
   c. Kriptanalisis
   d. Kriptanalis
   e. Kriptologi

   Kunci Jawaban: c. Kriptanalisis

4. Kriptanalis adalah...
   a. Orang yang membuat plainteks dengan sebuah kunci yang berbeda
   b. Orang yang membuat plainteks dengan kunci yang sama sebelumnya
   c. Orang yang memecahkan cipherteks tanpa mengetahui kunci yang digunakan
   d. Orang yang memecahkan cipherteks dengan kunci yang digunakan
   e. Orang yang memecahkan kunci dan algoritma yang digunakan pada cipherteks

   Kunci Jawaban: c. Orang yang memecahkan cipherteks tanpa mengetahui kunci yang digunakan

5. Ilmu yang mempelajari tentang pemecahan sebuah cipherteks tanpa mengetahui kunci dan algoritma yang digunakan oleh pengirim adalah...
   a. Kriptanalisis
   b. Kriptanalis
   c. Kriptografer
   d. Kriptologi
   e. Kriptolog

   Kunci Jawaban: a. Kriptanalisis

6. Kriptanalisis adalah...
   a. Ilmu dan seni untuk memecahkan cipherteks dan plainteks dengan sebuah kunci yang sama
   b. Ilmu dan seni untuk memecahkan cipherteks dan plainteks dengan dua kunci yang berbeda
   c. Ilmu dan seni untuk membuat sebuah cipherteks yang sulit terpecahkan algoritmnya
   d. Ilmu dan seni untuk memecahkan cipherteks tanpa mengetahui kunci dan algoritma yang digunakan
   e. Ilmu dan seni untuk untuk membuat plainteks tersembunyi

Kunci Jawaban: d. Ilmu dan seni untuk memecahkan cipherteks tanpa mengetahui kunci dan algoritma yang digunakan

Indikator: Mahasiswa dapat mengidentifikasikan perbedaan antara kriptografi kunci simetris dengan kriptografi kunci asimetris

Soal:

1. Termasuk jenis kunci manakah apabila kunci yang digunakan pada proses enkripsi dan dekripsi berbeda...
   a. Kunci simetris
   b. Kunci substitusi
   c. Kunci transposisi
   d. Kunci asimetris
   e. Kunci kombinasi

   Kunci Jawaban: d. Kunci asimetris

2. Di bawah ini yang termasuk contoh kunci asimetris adalah...
   a. 3DES
   b. RSA
   c. DES
   d. AES
   e. Blowfish

   Kunci Jawaban: b. RSA

3. Algoritma kriptografi simetris terbagi menjadi dua kategori yaitu...
   a. *Blok ciphers* dan transposisi *caesar*
   b. *Caesar ciphers* dan ekspansi blok
   c. *Stream ciphers* dan *blok ciphers*
   d. Ekspansi dan transposisi
   e. Subtitusi dan *blocking*

   Kunci Jawaban: c. *Stream ciphers* dan *blok ciphers*

4. Pada algoritma kriptografi asimetris, kunci yang digunakan pada proses enkripsi bersifat...
   a. Publik
   b. Unik
   c. Rahasia
   d. Sama
   e. Privat

   Kunci Jawaban: a. Publik

5. Pada algoritma kriptografi simetris, kunci yang digunakan pada proses dekripsi bersifat...
   a. Publik
   b. Unik
   c. Rahasia
   d. Sama
   e. Privat

   Kunci Jawaban: e. Privat

6. Perbedaan utama yang mendasar pada algoritma kriptografi asimetris adalah...
   a. Algoritma yang digunakan pada proses enkripsi
   b. Algoritma yang digunakan pada proses dekripsi
   c. Waktu pemecahan yang berbeda pada proses enkripsi dan dekripsi
   d. Kunci yang berbeda pada proses enkripsi dan dekripsi
   e. Jumlah algoritma yang berbeda pada proses enkripsi dan dekripsi

   Kunci Jawaban: d. Kunci yang berbeda pada proses enkripsi dan dekripsi

Indikator: Mahasiswa dapat menjelaskan fungsi keamanan algoritma kriptografi

Soal:

1. Menurut Lars Knudsen, kriptanalis menemukan algoritma alternatif A yang ekivalen dengan $D_K(C)$ tapi tidak mengetahui kunci K termasuk ke dalam hasil kriptanalis kategori...
   a. Induksi parsial
   b. Deduksi informasi
   c. Deduksi global
   d. Deduksi total
   e. Pemecahan total

   Kunci Jawaban: c. Deduksi global

2. Menurut Lars Knudsen, kriptanalis menemukan beberapa informasi perihal kunci atau plainteks termasuk ke dalam hasil kriptanalisis kategori...
   a. Induksi parsial
   b. Deduksi informasi
   c. Deduksi global
   d. Deduksi total
   e. Pemecahan total

   Kunci Jawaban: b. Deduksi informasi

3. Hasil kriptanalisis dengan kategori “Deduksi Global” menurut Lars Knudsen berarti...
   a. Kriptanalis menemukan kunci K
   b. Kriptanalis menemukan algoritma alternatif A tetapi tidak mengetahui kunci K
   c. Kriptanalis menemukan plainteks dari cipherteks yang disadap
   d. Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks
   e. Kriptanalis menemukan plainteks yang tersembunyi dalam kunci K

   Kunci Jawaban: b. Kriptanalis menemukan algoritma aternatif A tetapi tidak mengetahui kunci K

4. Hasil kriptanalisis dengan kategori “Deduksi Total” menurut Lars Knudsen berarti...
   a. Kriptanalis menemukan kunci K

b. Kriptanalis menemukan algoritma alternatif A tetapi tidak mengetahui kunci K
c. Kriptanalis menemukan plainteks dari cipherteks yang disadap
d. Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks
e. Kriptanalis menemukan plainteks yang tersembunyi dalam kunci K

Kunci Jawaban: c. Kriptanalis menemukan plainteks dari cipherteks yang disadap

5. Hasil kriptanalisis dengan kategori "Deduksi Informasi" menurut Lars Knudsen berarti...
   a. Kriptanalis menemukan kunci K
   b. Kriptanalis menemukan algoritma alternatif A tetapi tidak mengetahui kunci K
   c. Kriptanalis menemukan plainteks dari cipherteks yang disadap
   d. Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks
   e. Kriptanalis menemukan plainteks yang tersembunyi dalam kunci K

   Kunci Jawaban: e. Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks

Indikator: Mahasiswa dapat menyebutkan jenis-jenis serangan terhadap kriptografi

Soal:

1. 1) *Release of Message Content*
   2) *Traffic Analysis*
   3) *Masquerade*
   4) *Replay*
   5) *Modification of Message*
   Dari jenis serangan di atas, Serangan yang termasuk *passive attack* menurut William Stallings adalah...
   a. 1) dan 3)
   b. 3), 4), dan 5)
   c. 2), 3), dan 4)
   d. 2) dan 5)
   e. 1) dan 2)

   Kunci Jawaban: e. 1) dan 2)

2. 1) *Release of Message Content*
   2) *Traffic Analysis*
   3) *Masquerade*
   4) *Replay*
   5) *Modification of Message*
   Dari jenis serangan di atas, Serangan yang termasuk *active attack* menurut William Stallings adalah...
   a. 1) dan 3)
   d. 2) dan 5)

b. 3), 4), dan 5)
c. 2), 3), dan 4)
e. 1) dan 2)

Kunci Jawaban: b. 3), 4), dan 5)

3. Di bawah ini yang termasuk *active attack* menurut William Stallings, **kecuali**...
   a. *Masquerade*
   b. *Replay*
   c. *Modification of Message*
   d. *Traffic Analysis*
   e. *Denial of Service*

   Kunci Jawaban: d. *Traffic Analysis*

4. Di bawah ini yang termasuk *passive attack* menurut William Stallings adalah...
   a. *Masquerade*
   b. *Replay*
   c. *Release of Message Content*
   d. *Modification of Message*
   e. *Denial of Service*

   Kunci Jawaban: c. *Release of Message Content*

5. Di bawah ini yang termasuk *active attack* menurut William Stallings adalah...
   a. *Masquerade*
   b. *Traffic Analysis*
   c. *Release of Message Content*
   d. *Sniffing*
   e. *Wardriving*

   Kunci Jawaban: a. *Masquerade*

Indikator: Mahasiswa dapat mengidentifikasikan kompleksitas serangan terhadap kriptografi

Soal:

1. Semakin lama waktu yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut merupakan kompleksitas serangan yang diukur berdasarkan...
   a. Kompleksitas memori
   b. Kompleksitas kunci
   c. Kompleksitas data
   d. Kompleksitas waktu
   e. Kompleksitas cipherteks

   Kunci Jawaban: d. Kompleksitas waktu

2. Semakin banyak memori yang dibutuhkan untuk melakukan serangan berarti semakin bagus sistem kriptografi tersebut merupakan kompleksitas serangan yang diukur berdasarkan...
   a. Kompleksitas memori
   b. Kompleksitas kunci
   c. Kompleksitas data
   d. Kompleksitas waktu
   e. Kompleksitas cipherteks

Kunci Jawaban: a. Kompleksitas memori

3. 1) Kompleksitas waktu
   2) Kompleksitas memori
   3) Kompleksitas data
   4) Kompleksitas algoritma
   Kategori di atas yang merupakan tolak ukur kompleksitas serangan, **kecuali**...
   a. 1) dan 2)
   b. 2)
   c. 3) dan 4)
   d. 4)
   e. 1) dan 3)

   Kunci Jawaban: d. 4)

4. Dibawah ini yang termasuk ke dalam kategori tolak ukur kompleksitas serangan adalah...
   a. Kompleksitas algoritma
   b. Kompleksitas data
   c. Kompleksitas kunci
   d. Kompleksitas cipherteks
   e. Kompleksitas plainteks

   Kunci Jawaban: b. Kompleksitas data

5. Jumlah data (plainteks dan cipherteks) yang dibutuhkan sebagai masukkan untuk serangan merupakan kategori tolak ukur...
   a. Kompleksitas data
   b. Kompleksitas algoritma
   c. Kompleksitas kunci
   d. Kompleksitas waktu
   e. Kompleksitas memori

   Kunci Jawaban: a. Kompleksitas data

6. Waktu yang dibutuhkan untuk melakukan serangan merupakan kategori tolak ukur...
   a. Kompleksitas data
   b. Kompleksitas algoritma
   c. Kompleksitas kunci
   d. Kompleksitas waktu
   e. Kompleksitas memori

   Kunci Jawaban: d. Kompleksitas waktu

Indikator: Mahasiswa dapat menerapkan penggunaan fungsi matematika pada kriptografi

Soal:

1. Fungsi matematika untuk cipherteks Caesar Cipher yang digeser 3 ke kanan adalah...
   a. E(P+3)
   b. D(C+3)
   c. E(P-3)
   d. E(C-3)
   e. D(E)

Kunci Jawaban: a. E(P+3)

2. D(C-3) merupakan fungsi matematika dari...
   a. Substitusi yang digeser 3 ke atas
   b. Transposisi yang digeser 3 ke bawah
   c. Plainteks yang digeser 3 ke kiri
   d. Cipherteks yang digeser 3 ke kanan
   e. Ekspansi yang digeser 3 ke kanan

   Kunci Jawaban: c. Plainteks yang digeser 3 ke kiri

3. E(P) merupakan fungsi matematika dari...
   a. Substitusi
   b. Transposisi
   c. Plainteks
   d. Cipherteks
   e. Ekspansi

   Kunci Jawaban: d. Cipherteks

4. E(P+13) merupakan fungsi matematika dari...
   a. Substitusi ROT_{13}
   b. Transposisi ROT_{13}
   c. Plainteks ROT_{13}
   d. Cipherteks ROT_{13}
   e. Ekspansi ROT_{13}

   Kunci Jawaban: d. Cipherteks ROT_{13}

5. D(C-13) merupakan fungsi matematika dari...
   a. Substitusi ROT_{13}
   b. Transposisi ROT_{13}
   c. Plainteks ROT_{13}
   d. Cipherteks ROT_{13}
   e. Ekspansi ROT_{13}

   Kunci Jawaban: c. Plainteks ROT_{13}

6. Fungsi matematika dari plainteks pada ROT_{13} adalah...
   a. E(P-13)
   b. D(C-13)
   c. E(C-13)
   d. D(P-13)
   e. D(C.P)

   Kunci Jawaban: b. D(C-13)

Indikator: Mahasiswa dapat menghitung fungsi permutasi

Soal:

1. Hasil dari P_3^5 adalah...
   a. 210
   b. 30
   c. 12
   d. 60
   e. 120

   Kunci Jawaban: d. 60

2. Hasil dari P_2^6 adalah...
   a. 210
   b. 30
   c. 12
   d. 60
   e. 120

   Kunci Jawaban: b. 30

3. Hasil dari P_2^4 adalah...
   a. 210
   b. 30
   c. 12
   d. 60
   e. 120

   Kunci Jawaban: c. 12

4. Hasil dari P_3^7 adalah...
   a. 210
   b. 30
   c. 12
   d. 60
   e. 120

   Kunci Jawaban: a. 210

5. Hasil dari P_4^6 adalah...
   a. 360
   b. 840
   c. 24
   d. 56
   e. 20

   Kunci Jawaban: a. 360

6. Hasil dari P_2^8 adalah...
   a. 360
   b. 840
   c. 24
   d. 56
   e. 20

   Kunci Jawaban: d. 56

7. Hasil dari P_2^5 adalah...
   a. 24
   d. 84

b. 56 e. 72
c. 20

Kunci Jawaban: c. 20

8. Hasil dari P_2^9 adalah...
   a. 24 d. 84
   b. 56 e. 72
   c. 20

   Kunci Jawaban: e. 72

Indikator: Mahasiswa dapat menghitung fungsi kombinasi

Soal:

1. Hasil dari C_7^{10} adalah...
   a. 84 d. 28
   b. 210 e. 70
   c. 120

   Kunci Jawaban: c. 120

2. Hasil dari C_6^{10} adalah...
   a. 84 d. 28
   b. 210 e. 70
   c. 120

   Kunci Jawaban: b. 210

3. Hasil dari C_3^8 adalah...
   a. 56 d. 165
   b. 126 e. 55
   c. 252

   Kunci Jawaban: a. 56

4. Hasil dari C_9^{11} adalah...
   a. 56 d. 165
   b. 126 e. 55
   c. 252

   Kunci Jawaban: e. 55

5. Hasil dari C_8^{12} adalah...
   a. 56 d. 220

b. 126
c. 495
e. 330

Kunci Jawaban: c. 495

6. Hasil dari C_9^{12} adalah...
   a. 56
   b. 126
   c. 495
   d. 220
   e. 330

   Kunci Jawaban: d. 220

7. Hasil dari C_7^{11} adalah...
   a. 56
   b. 126
   c. 495
   d. 220
   e. 330

   Kunci Jawaban: e. 330

Indikator: Mahasiswa dapat menerapkan teori peluang

Soal:

1. Apabila terdapat sebuah kunci yang berisikan 2 huruf (huruf boleh sama dan tidak) dari jumlah alfabet, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,01331
   b. 0,01775
   c. 0,01479
   d. 0,001479
   e. 0,004438

   Kunci Jawaban: d. 0,001479

2. Apabila terdapat 3 kunci yang berisikan 2 huruf (huruf boleh sama dan tidak) dari jumlah alfabet, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,01331
   b. 0,01775
   c. 0,01479
   d. 0,001479
   e. 0,004438

   Kunci Jawaban: e. 0,004438

3. Apabila terdapat 9 kunci yang berisikan 2 huruf (huruf boleh sama dan tidak) dari jumlah alfabet, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,01331
   b. 0,01775
   c. 0,01479
   d. 0,001479
   e. 0,004438

   Kunci Jawaban: a. 0,01331

4. Apabila terdapat 2 kunci yang berisikan 2 huruf (boleh sama dan tidak) dari huruf T, U, R, P, dan M, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,08
   b. 0,12
   c. 0,16
   d. 0,2
   e. 0,24

   Kunci Jawaban: a. 0,08

5. Apabila terdapat 3 kunci yang berisikan 2 huruf (boleh sama dan tidak) dari huruf T, U, R, P, dan M, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,08
   b. 0,12
   c. 0,16
   d. 0,2
   e. 0,24

   Kunci Jawaban: b. 0,12

6. Apabila terdapat 4 kunci yang berisikan 2 huruf (boleh sama dan tidak) dari huruf T, U, R, P, dan M, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,08
   b. 0,12
   c. 0,16
   d. 0,2
   e. 0,24

   Kunci Jawaban: c. 0,16

7. Apabila terdapat 1 kunci yang berisikan 2 huruf (boleh sama dan tidak) dari huruf S, A, T, dan N, peluang untuk mendapatkan kunci yang benar adalah...
   a. 0,08
   b. 0,12
   c. 0,0625
   d. 0,125
   e. 0,1875

   Kunci Jawaban: c. 0,0625

Indikator: Mahasiswa dapat menerapkan teori bilangan

Soal:

1. Hasil pembulatan dari bilangan 12,74535 dengan 4 angka penting adalah...
   a. 12,74
   b. 12,7453
   c. 12,75
   d. 12,7454
   e. 13

   Kunci Jawaban: c. 12,75

2. Hasil pembulatan dari bilangan 79,6427 dengan 3 angka penting adalah...
   a. 79,7
   b. 79,64
   d. 79,6
   e. 79,65

c. 79,5

Kunci Jawaban: d. 79,6

3. Hasil pembulatan dari bilangan 358,6801 dengan 4 angka penting adalah...
   a. 358
   b. 358,7
   c. 358,69
   d. 358,68
   e. 358,681

   Kunci Jawaban: b. 358,7

4. Hasil pembulatan dari bilangan 807,650 dengan 3 angka penting adalah...
   a. 807,6
   b. 807
   c. 808
   d. 807,5
   e. 807,7

   Kunci Jawaban: c. 808

5. Hasil pembulatan dari bilangan 901,1994 dengan 3 angka penting adalah...
   a. 901
   b. 902
   c. 901,2
   d. 901,19
   e. 901,199

   Kunci Jawaban: a. 901

Indikator: Mahasiswa dapat mengaplikasikan algoritma *cipher* substitusi

Soal:

1. Cipherteks dari "CUACA BESOK AKAN CERAH" dengan menggunakan aturan Caesar Cipher adalah...
   a. FXDFS EHVRN DNDS FHUDS
   b. FXDFT EHVRN DNDT FHUDK
   c. FXDFD EHVRT DNDQ FHUDT
   d. FXDFD EHVRN DNDQ FHUDK
   e. FXDFR EHVRN DNDR FHUDR

   Kunci Jawaban: d. FXDFD EHVRN DNDQ FHUDK

2. Cipherteks dari "HARI INI AKAN DIADAKAN UAS KRIPTOGRAFI" dengan menggunakan aturan Caesar Cipher adalah...
   a. KDUL LQL DNDQ GLDGONDQ XDV NULSWRJUDIL
   b. KDUL LQL DNDQ GLOGDNDQ XDV NULSWRJUDIL
   c. KDUL LQL DNDQ GLDGDNDQ XDV NULSWRJUDIL
   d. KDUL LQL DNOQ GLDGDNDQ XDT NULSWRJUDIL
   e. KDUL LQL DNOQ GLOGDNDQ XDV NULSWRJUDIL

Kunci Jawaban: c. KDUL LQL DNDQ GLDGDNDQ XDV NULSWRJUDIL

3. Cipherteks dari "UJIAN AKHIR SEMESTER MATA KULIAH KRIPTOGRAFI" dengan menggunakan aturan Caesar Cipher adalah...
   a. XMLDQ DKLU VHPHVWHU PDND NXOLDK NULSWRJUDIL
   b. XMLDQ DKLU VHPNVWHU PDWD NXOLDK NULSWRJUDIL
   c. XMLDQ DKLU VHPHVWHU POND NXOLDK NULSWRJUDIL
   d. XMLDQ DKLU VHPNVWHU POWD NXOLDK NULSWRJUDIL
   e. XMLDQ DKLU VHPHVWHU PDWD NXOLDK NULSWRJUDIL

   Kunci Jawaban: e. XMLDQ DKLU VHPHVWHU PDWD NXOLDK NULSWRJUDIL

4. Cipherteks dari "HARI INI HARI RABU TANGGAL SEPULUH JUNI" dengan menggunakan aturan Caesar Cipher adalah...
   a. KDUL LQL KDUL UDEX WDQJJDO VHSXOXK MXQL
   b. KDUL LQL KDUL UDEX WDQTJDO VHSXOXK MXQL
   c. KDUL LQL KDUL UDEX WDQJJDO VHSXOXN MXQL
   d. KDUL LQL KDUL UDEX WDQJTDO VHSXOXK MXQL
   e. KDUL LQL KDUL UDEX WDQJJDO VHSXXOXK MXQL

   Kunci Jawaban: a. KDUL LQL KDUL UDEX WDQJJDO VHSXOXK MXQL

5. Cipherteks dari "UAS KRIPTOGRAFI AKAN DISELENGGARAKAN HARI INI" dengan menggunakan aturan Caesar Cipher adalah...
   a. XDV NULSWRJUDIL DNDQ GLVHOHQJDUDNDQ KDUL LQL
   b. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDNDQ KDUL LQL
   c. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUONDQ KDUL LQL
   d. XDV NULSWRJUDIL DNDQ GLVNOHQJJDUDNDQ KDUL LQL
   e. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDHDQ KDUL LQL

   Kunci Jawaban: b. XDV NULSWRJUDIL DNDQ GLVHOHQJJDUDNDQ KDUL LQL

6. Cipherteks dari "PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER" dengan menggunakan aturan Caesar Cipher adalah...
   a. SHQGLGLNDQ WHNQLN LOIRUPDWLND GDQ NRPSXWHU
   b. SHQGLGLNDQ WHNQLN LQIRUPDWLMD GDQ NRPSXWHU
   c. SHQGLGLNDQ WHNQLN LQIRURDWLND GDQ NRPSXWHU
   d. SHQGLGLNDQ WHNQLN LQIRUPDWLND GDQ NRPSXWHU
   e. SHQGLGLNDQ WHNQLN LQIRUPDWLND GDQ NRPSXWNU

   Kunci Jawaban: d. SHQGLGLNDQ WHNQLN LQIRUPDWLND GDQ NRPSXWHU

Indikator: Mahasiswa dapat mengaplikasikan algoritma *cipher* transposisi

Soal:

1. Cipherteks dari "HARI INI TANGGAL DUA PULUH MEI" dengan menggunakan aturan *blocking* berupa 3 blok adalah...
   a. HINTGLUPUMA_IAG_AUHERI_NAD_L_I
   b. HINTGLUPUMA_UAG_AUHERI_NAD_L_M
   c. HINTGLUPUMA_UAG_AUHERI_NAD_L_E
   d. HINTGLUPUMA_IAG_AUHERI_NAD_L_M
   e. HINTGLUPUMA_UAG_AUHERI_NAD_L_I

   Kunci Jawaban: a. HINTGLUPUMA_IAG_AUHERI_NAD_L_I

2. Cipherteks dari "HARI INI AKAN DIADAKAN KUIS MATA KULIAH KRIPTOGRAFI" dengan menggunakan aturan *blocking* berupa 4 blok adalah...
   a. H__NAAUM_IKTAAIA_DNIAKAROFRNKDA_STUHIGIIIAIKK_AL_P R
   b. H__NAAUM_IKTAAIA_DNIAKAROFRNKDA_STUHIGIIIAIKK_AL_P R_
   c. H_NAAUM_IKTAAIA_DNIAKAROFRNKDA_STUHIGIIIAIKK_AL_PR _
   d. H_NAAUM_IKTAAIA_DNIAKAROFRNKDA_STUHIGIIIAIKK_AL_PR
   e. H__NAAUM_IKTAAIA_DNIAKAROFRNKDA_STUHIGIIIAIKK_AL_P R_I

   Kunci Jawaban: b. H__NAAUM_IKTAAIA_DNIAKAROFRNKDA_STUHIGI

   IIAIKK_AL_PR_

3. Cipherteks dari "PERKULIAHAN KRIPTOGRAFI AKAN SEGERA DIMULAI" dengan menggunakan aturan *blocking* berupa 3 blok adalah...
   a. PKIAKPGFANERDUIEUANRTRIK_GAILRLH_IOA_ASE_MA
   b. PKIAKPGFANERDUIEUANRTRIK_GAILRLH_NOA_ASE_MA_T
   c. PKIAKPGFANERDUIEUANRTRIK_GAILRLH_IOA_ASE_MA_
   d. PKIAKPGFANERDUIEUANRTRIK_GAILRLH_NOA_ASE_MA
   e. PKIAKPGFANERDUIEUANRTRIK_GAILRLN_IOA_ASE_MA

   Kunci Jawaban: c. PKIAKPGFANERDUIEUANRTRIK_GAILRLH_IOA_ASE_MA_

4. Cipherteks dari "HARI INI AKAN DIADAKAN UAS KRIPTOGRAFI" dengan menggunakan aturan *blocking* berupa 4 blok adalah...
   a. H__NAAAROFAIA_DNSIGIRNKDA__PR_IIAIKUNTA_
   b. H__NAAAROFAIA_DNSIGIRNKDA__PR__IAIKUKTA_
   c. H__NAAAROFAIA_DNSIGIRNKDA__PR_IIAIKUKTA_
   d. H__NAAAROFAIA_DNSIGIRNKDA__PR_IIAIKUKTA

e. H__NAAAROFAIA_DNSIGIRNKDA_PR_IIAIKUKTA_

Kunci Jawaban: c. H__NAAAROFAIA_DNSIGIRNKDA__PR_IIAIKUKTA_

5. Cipherteks dari “HARI INI HARI RABU TANGGAL SEPULUH JUNI” dengan menggunakan aturan *blocking* berupa 2 blok adalah...
   a. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN_
   b. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN
   c. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPNHJN_
   d. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTHGLSPLHJN
   e. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTGLSPLHJN_

   Kunci Jawaban: a. HR_N_AIRB_AGA_EUU_UIAIIIHR_AUTNGLSPLHJN_

6. Cipherteks dari “PROGRAM STUDI PTIK JURUSAN TEKNIK ELEKTRO” dengan menggunakan aturan *blocking* berupa 3 blok adalah...
   a. PGMTIT_RATN_ERRR_U_IJUNEIEKOOASDPKUS_KKLT
   b. PGMTIT_RATN_ERRR_U_IJUNEIEKOOASDPKUSKKLT_
   c. PGMTIT_RATN_ERRR_U_IJUNEIEKOOASDPNUS_KKLT
   d. PGMTIT_RATN_ERRR_U_IJUNEIEKOOASDPKUS_KLT
   e. PGMTIT_RATN_ERRR_U_IJUNEIEKOOASDPKUS_KKLT_

   Kunci Jawaban: e. PGMTIT_RATN_ERRR_U_IJUNEIEKOOASDPKUS_

   KKLT_

7. Cipherteks dari “MATA KULIAH KRIPTOGRAFI ADALAH MATA KULIAH PILIHAN” dengan menggunakan aturan *blocking* berupa 3 blok adalah...
   a. MAUAKPGFAL_TKI_LAA_LHRTRIDAMAUAPINTKI_IOA_AHA_LHIH
   b. MAUAKPGFAL_TKI_LAA_LHRTRIDAMAUAPINTKI_IOA_AHA_LHIH_
   c. MAUAKPGFAL_TKI_LAA_LHRTRIDAMAUAPINTKI_IOA_ANA_LHIH
   d. MAUAKPGFAL_TKI_LAA_LHRTRIDAMAUAPNTKI_IOA_AHA_LHIH_
   e. MAUAKPGFAL_TKI_LAA_LHTRIDAMAUAPINTKI_IOA_AHA_LHIH

   Kunci Jawaban: b. MAUAKPGFAL_TKI_LAA_LHRTRIDAMAUAPINTKI_IOA_AHA_LHIH_

Indikator: Mahasiswa dapat mengaplikasikan algoritma *affine cipher*

Soal:

1. Cipherteks dari “ENKRIPSI” yang menggunakan algoritma *affine cipher* dengan kunci a = 5 dan b = 6 adalah...
   a. DTNHYKLO
   b. SDVBYJKP
   c. ATENUDSU
   d. RGUXOPOP
   e. HJIRKLDE

   Kunci Jawaban: c. ATENUDSU

2. Cipherteks dari “DEKRIPSI” yang menggunakan algoritma *affine cipher* dengan kunci a = 5 dan b = 6 adalah...
   a. SFGTRVNM
   b. DRTYNMJK
   c. VBNMUHTR
   d. VBHYUJKL
   e. VAENUDSU

   Kunci Jawaban: e. VAENUDSU

3. Cipherteks dari “PLAINTEKS” yang menggunakan algoritma *affine cipher* dengan kunci a = 5 dan b = 6 adalah...
   a. TGBHNJMKL
   b. DJGUTXAES
   c. RTYUIJHGB
   d. ASEVGTHUJ
   e. BGTNJUMVF

   Kunci Jawaban: b. DJGUTXAES

4. Cipherteks dari “PASSWORD” yang menggunakan algoritma *affine cipher* dengan kunci a = 5 dan b = 6 adalah...
   a. DGSSMYNV
   b. KLOHYRCX
   c. WTGNJUKL
   d. XCTGHNJI
   e. ZXYUNJFR

   Kunci Jawaban: a. DGSSMYNV

5. Cipherteks dari “KRIPTOGRAFI” yang menggunakan algoritma *affine cipher* dengan kunci a = 4 dan b = 6 adalah...
   a. UWMOEKEWGAM
   b. DTHUYIOPLNM
   c. FRTGYHJUIKM
   d. UWMOGTBVFSK
   e. YTGBVCDERKI

   Kunci Jawaban: a. UWMOEKEWGAM

6. Cipherteks dari “TRANSPOSISI” yang menggunakan algoritma *affine cipher* dengan kunci a = 4 dan b = 6 adalah...
   a. EWGGTRFSVBH
   b. WJUYHMKLOPU
   d. SDBHYEDJMJM
   e. SNJHUTRBGBG

c. EWGGAOKAMAM

Kunci Jawaban: c. EWGGAOKAMAM

7. Cipherteks dari "SUBSTITUSI" yang menggunakan algoritma *affine cipher* dengan kunci a = 4 dan b = 6 adalah...
   a. ABGTHUJKIL
   b. AIKANHTRFV
   c. AJKIMNBMNU
   d. AIKAEMEIAM
   e. DSBGTHNMJU

   Kunci Jawaban: d. AIKAEMEIAM

8. Cipherteks dari "KEAMANAN" yang menggunakan algoritma *affine cipher* dengan kunci a = 4 dan b = 6 adalah...
   a. UWGCGGGG
   b. ZXGYHNMK
   c. THNFRWDW
   d. BNHTFVBN
   e. VGBHYRGT

   Kunci Jawaban: a. UWGCGGGG

9. Cipherteks dari "AFFINECIPHER" yang menggunakan algoritma *affine cipher* dengan kunci a = 4 dan b = 6 adalah...
   a. APPYHBGTRSJ
   b. GAAMGWOMOIWW
   c. AMMWLJYJLWWW
   d. BWWMJHYGTBCD
   e. VBBWSMKLLPUY

   Kunci Jawaban: b. GAAMGWOMOIWW

Indikator: Mahasiswa dapat mengaplikasikan algoritma *vigenere*

Soal:

1. Cipherteks dari "KOMPUTER" yang menggunakan algoritma *vigenere* dengan kunci "ILMU" adalah...
   a. FWRTYBUL
   b. SZYJCEQL
   c. RTKLGUYH
   d. GHPTYMNE
   e. STNJITUM

   Kunci Jawaban: b. SZYJCEQL

2. Cipherteks dari "VIGENERE" yang menggunakan algoritma *vigenere* dengan kunci "ILMU" adalah...
   a. BRWTYUGH
   b. DOPWXYMI
   c. DTSYVPDY
   d. LPRTGUWA
   e. DRTLNAWC

Kunci Jawaban: c. DTSYVPDY

3. Cipherteks dari “PERMUTASI” yang menggunakan algoritma *vigenere* dengan kunci “ILMU” adalah...
   a. DWQBJKTVE
   b. HKWXUIAPT
   c. SMNQPOFJU
   d. ETZUNMWBI
   e. XPDGCEMMQ

   Kunci Jawaban: e. XPDGCEMMQ

4. Cipherteks dari “ALGORITMA” yang menggunakan algoritma *vigenere* dengan kunci “ILMU” adalah...
   a. IWSIZTFGI
   b. KTPWRTBGI
   c. UHDWPLOTZ
   d. GTMVSWRFT
   e. QPTCXIINL

   Kunci Jawaban: a. IWSIZTFGI

5. Cipherteks dari “ENKRIPSI” yang menggunakan algoritma *vigenere* dengan kunci “ILMU” adalah...
   a. WNMTUCIP
   b. ELTCIIGS
   c. WRTXYIQP
   d. MYWLQAEC
   e. SPWUXZYN

   Kunci Jawaban: d. MYWLQAEC

Indikator: Mahasiswa dapat mengaplikasikan algoritma *playfair*

Soal:

1. Cipherteks dari “PENDIDIKAN TIK UNJ” yang menggunakan algoritma *playfair* dengan kunci “KOMPUTER” adalah...
   a. GANLPTILMTQKEKFARGSV
   b. EQDPTNRKGAQEXGTQBX
   c. MTQKEKFARGVTQEILUV
   d. DALFLCVTRQCVOKQL
   e. ERMIVTLQDMFRBEVTBY

   Kunci Jawaban: d. DALFLCVTRQCVOKQL

2. Cipherteks dari “KRIPTOGRAFI KLASIK” yang menggunakan algoritma *playfair* dengan kunci “KOMPUTER” adalah...
   a. GANLPTILMTQKEKFARGSV
   b. EQDPTNRKGAQEXGTQBX
   c. MTQKEKFARGVTQEILUV
   d. DALFLCVTRQCVOKQL

e. ERMIVTLQDMFRBEVTBY

Kunci Jawaban: c. MTQKEKFARGVTQEILUV

3. Cipherteks dari “KRIPTOGRAFI MODERN” yang menggunakan algoritma *playfair* dengan kunci “ILMU” adalah...
   a. RXBVZTKPFOLUKFDSOY
   b. VGBHNJMKUJYHTGRFD
   c. VGTWSDFGYJIMBVGHRE
   d. TGRRMKHAAOPPRWSCF
   e. UMMBVCHYFDSZXCVKKU

   Kunci Jawaban: a. RXBVZTKPFOLUKFDSOY

4. Cipherteks dari “CIPHER SUBSTITUSI” yang menggunakan algoritma *playfair* dengan kunci “ILMU” adalah...
   a. BGUJGRDSWGHPLZAE
   b. BUJMCDESXZFGTLKG
   c. BLQGDSYEEPPASAPU
   d. ZWDVTGBMKIHTRDW
   e. MEDPOCXZHJLTRSCF

   Kunci Jawaban: c. BLQGDSYEEPPASAPU

5. Cipherteks dari “FUNGSI MATEMATIKA” yang menggunakan algoritma *playfair* dengan kunci “ILMU” adalah...
   a. BGTDFJKLOPWSXCVF
   b. VFRTJKLMNXZERGHJ
   c. BVXGHJUILPEQWASB
   d. EAOHPUUISFUIPAOM
   e. MOPLMCDERFSZXVGT

   Kunci Jawaban: d. EAOHPUUISFUIPAOM

6. Cipherteks dari “TERMINOLOGI KRIPTOGRAFI” yang menggunakan algoritma *playfair* dengan kunci “ILMU” adalah...
   a. SFXDUGHAGHMGPMQPGHTMBA
   b. NMHYTGVFREDCXSWQAZXCVB
   c. MHGFRTGBNHYUJMBGFDCXGH
   d. NMUHJKLVFRCXBGHJMNBVFR
   e. MKLOPJHGFRTYUBVCDEFRTG

   Kunci Jawaban: a. SFXDUGHAGHMGPMQPGHTMBA

Indikator: Mahasiswa dapat mengaplikasikan algoritma *one-time pad*

Soal:

1. Cipherteks dari “UNIVERSITAS” yang menggunakan algoritma *one-time pad* dengan kunci “ASDFGHJKLPO” adalah...
   a. GHYSWERVBMI
   b. VGMBLZCTFQH
   c. LPOUYTRDCGT
   d. TYHNVCDEWPO
   e. HGTYUIHGFRE

   Kunci Jawaban: b. VGMBLZCTFQH

2. Cipherteks dari “KOMUNIKASI” yang menggunakan algoritma *one-time pad* dengan kunci “ASDFGHJKLP” adalah...
   a. FTBWIPMFRT
   b. DKOTRVFCHU
   c. TRBNJGFWQK
   d. IOMNFRDCAZ
   e. LHQAUQULEG

   Kunci Jawaban: e. LHQAUQULEG

3. Cipherteks dari “HORIZONTAL” yang menggunakan algoritma *one-time pad* dengan kunci “ASDFGHJKLP” adalah...
   a. IHVOGWXEMB
   b. OYTBGSEOPL
   c. VGTNJIGTHJ
   d. IKWPLXUYET
   e. ZMKLEWTVCA

   Kunci Jawaban: a. IHVOGWXEMB

4. Cipherteks dari “DISTRIBUSI” yang menggunakan algoritma *one-time pad* dengan kunci “ASDFGHJKLP” adalah...
   a. RTYUNMCDGT
   b. TGBNJUIOPL
   c. DRFVUNHTRE
   d. EBWZYQLFEY
   e. VGTKLOWERB

   Kunci Jawaban: d. EBWZYQLFEY

5. Cipherteks dari “ONETIMEPAD” yang menggunakan algoritma *one-time pad* dengan kunci “ACDZIBOCQR” adalah...
   a. PQITROTSRV
   b. AMKLOPKNBG
   c. GPOIUYVBGF
   d. BNHVCDRTGH
   e. NBGTFCDESX

   Kunci Jawaban: a. PQITROTSRV

6. Cipherteks dari “ALGORITMA” yang menggunakan algoritma *one-time pad* dengan kunci “ACDZIBOCQ” adalah...
   a. MJHFCVRTG
   b. BOKOAKIPR
   d. NMHBFREDX
   e. BGTRFXSWE

c. NJHFCVTYO

Kunci Jawaban: b. BOKOAKIPR

Indikator: Mahasiswa dapat menerapkan rangkaian bit dan operasinya

Soal:

1. Plainteks “011100111000” yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu...
   a. A 6 5
   b. E 5 C
   c. 7 3 8
   d. 8 6 D
   e. 1 7 9

   Kunci Jawaban: c. 7 3 8

2. Plainteks “101101101101” yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu...
   a. A 6 5
   b. E 5 C
   c. 7 3 8
   d. 8 6 D
   e. 1 7 9

   Kunci Jawaban: d. 8 6 D

3. Plainteks “110110000111” yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu...
   a. 6 D 8
   b. D 8 7
   c. C D 9
   d. 3 9 8
   e. C F C

   Kunci Jawaban: b. D 8 7

4. Plainteks “110011011001” yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu...
   a. 6 D 8
   b. D 8 7
   c. C D 9
   d. 3 9 8
   e. C F C

   Kunci Jawaban: c. C D 9

5. Plainteks “001110011000” yang dibagi menjadi blok bit dengan panjang 4 dapat dinyatakan dalam notasi HEX, yaitu...
   a. 6 D 8
   b. D 8 7
   c. C D 9
   d. 3 9 8
   e. C F C

Kunci Jawaban: d. 3 9 8

Indikator: Mahasiswa dapat menerapkan algoritma enkripsi dengan XOR sederhana

Soal:

1. Cipherteks dari 10010 dengan kunci 01001 adalah...
   a. 11011
   b. 00001
   c. 00110
   d. 01011
   e. 01101

   Kunci Jawaban: a. 11011

2. Cipherteks dari 10111 dengan kunci 11010 adalah...
   a. 11011
   b. 01101
   c. 00110
   d. 01011
   e. 00001

   Kunci Jawaban: b. 01101

3. Cipherteks dari 10101 dengan kunci 01110 adalah...
   a. 11011
   b. 00001
   c. 00110
   d. 01011
   e. 11010

   Kunci Jawaban: a. 11011

4. Cipherteks dari 10010 dengan kunci 01100 adalah...
   a. 11110
   b. 01111
   c. 11011
   d. 10000
   e. 11101

   Kunci Jawaban: a. 11110

5. Cipherteks dari 00010 dengan kunci 10010 adalah...
   a. 11110
   b. 01111
   c. 11011
   d. 10000
   e. 11101

   Kunci Jawaban: d. 10000

6. Cipherteks dari 10001 dengan kunci 01100 adalah...
   a. 11110
   b. 01111
   c. 11011
   d. 10000
   e. 11101

   Kunci Jawaban: e. 11101

Indikator: Mahasiswa dapat mengoperasikan pembangkitan kunci

Soal:

1. Salah satu cara untuk membangkitkan kunci pada algoritma kunci publik adalah...
   a. Memfaktorkan bilangan
   b. Diferensial bilangan
   c. Integral data plainteks
   d. Menggunakan program khusus
   e. Menambah memori eksternal

   Kunci Jawaban: d. Menggunakan program khusus

2. Metode yang dapat digunakan pada pembangkitan kunci adalah...
   a. Pembangkit bilangan faktor
   b. Pembangkit bilangan acak
   c. Pembangkit kunci simetri
   d. Pembangkit kunci asimetri
   e. Pembangkit kunci publik

   Kunci Jawaban: b. Pembangkit bilangan acak

3. Pembangkitan kunci pada algoritma simetri pada umumnya menggunakan kunci simetri rangkaian...
   a. Algoritma
   b. Karakter
   c. Byte
   d. Notasi
   e. Biner

   Kunci Jawaban: b. Karakter

4. Pada manajemen kunci, pembangkitan sebuah kunci dilakukan setelah proses...
   a. *Distribution*
   b. *Usage*
   c. *Storage*
   d. *Change*
   e. *Destruction*

   Kunci Jawaban: e. *Destruction*

5. Membuat kunci yang tidak dapat diprediksi merupakan masalah utama yang muncul pada...
   a. Pembangkitan kunci
   b. Penggunaan kunci
   c. Penghancuran kunci
   d. Penyimpanan kunci
   e. Pengubahan kunci

   Kunci Jawaban: a. Pembangkitan Kunci

6. Untuk membentuk kunci pada algoritma kunci publik, salah satu proses rumit yang harus dilakukan adalah...
   a. Perhitugan jumlah setiap putaran kunci

b. Pembuatan kunci yang bersifat publik
c. Pembangkitan bilangan prima yang besar
d. Pembuatan kunci yang sulit diprediksi
e. Perhitungan integral bilangan biner

Kunci Jawaban: c. Pembangkitan bilangan prima yang besar

7. *User* dapat membangkitkan kuncinya sendiri dapat dilakukan pada pembangkitan kunci algoritma...
   a. Asimetris
   b. Publik
   c. Klasik
   d. Simetris
   e. Caesar Cipher

   Kunci Jawaban: d. Simetris

Indikator: Mahasiswa dapat mengidentifikasikan perbedaan antara DES dengan AES

Soal:

1. 1) 56 bit
   2) 128 bit
   3) 192 bit
   4) 256 bit
   Dari jumlah bit di atas, jumlah bit yang dapat digunakan oleh kunci DES adalah...
   a. 3)
   b. 1) dan 2)
   c. 1)
   d. 3) dan 4)
   e. 2), 3), dan 4)

   Kunci Jawaban: c. 1)

2. 1) 56 bit
   2) 128 bit
   3) 192 bit
   4) 256 bit
   Dari jumlah bit di atas, jumlah bit yang dapat digunakan oleh kunci AES adalah...
   a. 3)
   b. 1) dan 2)
   c. 1)
   d. 3) dan 4)
   e. 2), 3), dan 4)

   Kunci Jawaban: e. 2), 3), dan 4)

3. 1) Rijndael
   2) Ruth M. Davis
   3) Lucifer
   Dari daftar nama di atas, nama yang merupakan penemu dari AES adalah...

a. 1)
b. 1) dan 2)
c. 3)
d. 2)
e. 2) dan 3)

Kunci Jawaban: a. 1)

4. AES merupakan salah satu algoritma kriptografi *cipher block* dengan ukuran blok yaitu...
   a. 56 bit
   b. 128 bit
   c. 192 bit
   d. 255 bit
   e. 256 bit

   Kunci Jawaban: b. 128 bit

5. Dalam proses *enchiper* pada algoritma DES, blok plainteks terbagi menjadi dua bagian yaitu bagian kiri (L) dan bagian kanan (R), yang masing-masing memilki panjang yaitu...
   a. 8 bit
   b. 16 bit
   c. 32 bit
   d. 64 bit
   e. 128 bit

   Kunci Jawaban: c. 32

6. Algoritma *Lucifer* merupakan algoritma yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit. Algoritma ini telah dimodifikasi sehingga menghasilkan sebuah algortima baru bernama...
   a. AES
   b. RC4
   c. A5
   d. DES
   e. RSA

   Kunci Jawaban: d. DES

7. Algoritma *Lucifer* telah diperbaharui menjadi algoritma DES yang kemudian digantikan kembali karena faktor keamanan yang kurang baik oleh algoritma...
   a. 3DES
   b. RC4
   c. A5
   d. RSA
   e. AES

   Kunci Jawaban: e. AES

8. 1) 10 putaran
   2) 12 putaran
   3) 14 putaran
   4) 16 putaran
   Jumlah putaran yang digunakan setiap blok pada AES-128 adalah...
   a. 1)
   b. 2)
   d. 4)
   e. Semua jawaban benar

c. 3)

Kunci Jawaban: a. 1)

9. 1) 10 putaran
   2) 12 putaran
   3) 14 putaran
   4) 16 putaran
   Jumlah putaran yang digunakan setiap blok pada AES-256 adalah...
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. Semua jawaban benar

   Kunci Jawaban: c. 3)

Indikator: Mahasiswa dapat mengidentifikasikan perbedaan antara RC4 dengan A5

Soal:

1. 1) Bit
   2) Byte
   3) Huruf
   4) Blok
   Algoritma RC4 melakukan proses data dalam ukuran...
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. Semua jawaban benar

   Kunci Jawaban: b. 2)

2. 1) Bit
   2) Byte
   3) Huruf
   4) Blok
   Algoritma A5 melakukan proses data dalam ukuran...
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. Semua jawaban benar

   Kunci Jawaban: a. 1)

3. Algoritma yang digunakan untuk menghasilkan aliran kunci 228 bit yang kemudian di XOR-kan dengan frame adalah...
   a. MD5
   b. MAC
   d. RC4
   e. A5

c. 3DES

Kunci Jawaban: e. A5

4. Algoritma yang digunakan untuk membangkitkan aliran kunci yang kemudian di XOR-kan dengan plainteks adalah...
   a. MD5
   b. MAC
   c. 3DES
   d. RC4
   e. A5

   Kunci Jawaban: d. RC4

5. Panjang kunci eksternal dari A5 adalah...
   a. 128 bit
   b. 256 bit
   c. 64 bit
   d. 8 byte
   e. 12 byte

   Kunci Jawaban: c. 64 bit

Indikator: Mahasiswa dapat menjelaskankan *cipher* aliran

Soal:

1. *Cipher* aliran atau *stream cipher* termasuk ke dalam salah satu algoritma kriptografi...
   a. Asimetri
   b. Simetri
   c. Transisi
   d. Transposisi
   e. Permutasi

   Kunci Jawaban: b. Simetri

2. *Cipher* aliran beroperasi pada...
   a. Bit tunggal
   b. Blok
   c. Kata
   d. Byte
   e. Huruf

   Kunci Jawaban: a. Bit tunggal

3. Proses enkripsi dan dekripsi pada cipher aliran dilakukan dengan cara mentransformasikan...
   a. Blok per blok
   b. Kata per kata
   c. Huruf per huruf
   d. Bit per bit
   e. Byte per byte

   Kunci Jawaban: d. Bit per bit

4. Bit-bit kunci untuk proses enkripsi maupun dekripsi pada cipher aliran disebut...

a. *Standard key*
b. *Keybits*
c. *Cipherkey*
d. *Verman key*
e. *Keystream*

Kunci Jawaban: e. *Keystream*

5. Mengenkripiskan suara digital pada jaringan telepon *mobile* GSM merupakan contoh penggunaan kriptografi...
   a. Cipher blok
   b. Caesar cipher
   c. Cipher aliran
   d. Cipher asimetri
   e. Cipher byte

   Kunci Jawaban: c. Cipher aliran

Indikator: Mahasiswa dapat mengidentifikasikan serangan terhadap *cipher* aliran

Soal:

1. Kriptanalis mengetahui potongan P dan C yang berkoresponden merupakan jenis serangan terhadap cipher aliran yang disebut...
   a. *Known-plaintext attack*
   b. *Known-ciphertext attack*
   c. *Ciphertext-only attack*
   d. *Plaintext-only attack*
   e. *Flip-bit attack*

   Kunci Jawaban: a. *Known-plaintext attack*

2. Pengubahan bit cipherteks tertentu sehingga hasil dekripsinya berubah merupakan jenis serangan terhadap cipher aliran yang disebut...
   a. *Known-plaintext attack*
   b. *Known-ciphertext attack*
   c. *Ciphertext-only attack*
   d. *Plaintext-only attack*
   e. *Flip-bit attack*

   Kunci Jawaban: e. *Flip-bit attack*

3. *Flip-bit attack* adalah...
   a. Pengubahan bit plainteks tertentu sehingga hasil enkripsinya berubah
   b. Pengubahan bit cipherteks tertentu sehingga hasil dekripsinya berubah
   c. Kriptanalis mengetahui potongan P dan C yang berkoresponden
   d. Kriptanalis memiliki dua potongan cipherteks berbeda (C_1 dan C_2)
   e. Kriptanalis memiliki dua potongan kunci yang berbeda

   Kunci Jawaban: b. Pengubahan bit cipherteks tertentu sehingga hasil dekripsinya berubah

4. *Known-plaintext attack* adalah...
   a. Pengubahan bit plainteks tertentu sehingga hasil enkripsinya berubah

b. Pengubahan bit cipherteks tertentu sehingga hasil dekripsinya berubah
c. Kriptanalis mengetahui potongan P dan C yang berkoresponden
d. Kriptanalis memiliki dua potongan cipherteks berbeda (C_1 dan C_2)
e. Kriptanalis memiliki dua potongan kunci yang berbeda

Kunci Jawaban: c. Kriptanalis mengetahui potongan P dan C yang berkoresponden

5. *Ciphertext-only attack* dapat terjadi apabila...
   a. *Keystream* yang sama digunakan dua kali terhadap potongan plainteks yang berbeda
   b. *Keystream generator* menghasilkan kunci yang sama
   c. Cipherteks menggunakan sebuah kunci yang dihasilkan oleh *keystream generator*
   d. Plainteks menggunakan sebuah kunci yang dihasilkan oleh *keystream generator*
   e. Cipherteks dihasilkan oleh rangkaian bit kunci yang sudah diubah oleh kriptanalis

   Kunci Jawaban: a. *keystream* yang sama digunakan dua kali terhadap potongan plainteks yang berbeda

6. *Keystream* yang sama digunakan dua kali terhadap potongan plainteks yang berbeda dapat mengakibatkan terjadinya serangan...
   a. *Known-plaintext attack*
   b. *Known-ciphertext attack*
   c. *Ciphertext-only attack*
   d. *Plaintext-only attack*
   e. *Flip-bit attack*

   Kunci Jawaban: c. *Ciphertext-only attack*

7. Contoh dari *ciphertext-only attack* adalah...
   a. Pengubahan bit plainteks tertentu sehingga hasil enkripsinya berubah
   b. Pengubahan bit cipherteks tertentu sehingga hasil dekripsinya berubah
   c. Kriptanalis mengetahui potongan P dan C yang berkoresponden
   d. Kriptanalis memiliki dua potongan cipherteks berbeda (C_1 dan C_2) yang dienkripsi dengan bit-bit kunci yang sama
   e. Kriptanalis memiliki dua potongan kunci yang berbeda yang dibangkitkan dengan kunci acak semu

   Kunci Jawaban: d. Kriptanalis memiliki dua potongan cipherteks berbeda (C_1 dan C_2) yang dienkripsi dengan bit-bit kunci yang sama

8. Pada flip-bit attack, kriptanalis yang akan melakukan pengubahan pesan tidak perlu mengetahui...
   a. Cipherteks
   b. Plainteks
   d. Keystream generator
   e. Kunci

c. Cipherteks dan plainteks

Kunci Jawaban: e. Kunci

9. Agar dapat terhindar dari serangan seorang kriptanalis, penggunaan cipher aliran harus mempunyai...
   a. *Keystream generator* yang tidak menghasilkan kunci yang sama
   b. Beberapa cipherteks yang sulit dipecahkan
   c. Kunci yang rumit agar mendapatkan cipherteks yang sulit didekripsi
   d. Bit-aliran-kunci yang tidak dapat diprediksi
   e. Kunci yang mengandung bilangan prima acak semu

   Kunci Jawaban: d. Bit-aliran-kunci yang tidak dapat diprediksi

10. Penggunaan bit-aliran-kunci yang tidak dapat diprediksi pada cipher aliran dimaksudkan untuk...
    a. Menghasilkan cipherteks yang sulit didekripsi
    b. Menghindarkan kemungkinan kriptanalis mendeduksi bit-aliran-kunci
    c. Membuat beberapa cipherteks yang sulit dipecahkan
    d. Menghasilkan kunci-kunci dengan bilangan prima acak semu
    e. Menghindarkan kemungkinan kriptanalis mendapatkan plainteks

    Kunci Jawaban: b. Menghindarkan kemungkinan kriptanalis mendeduksi bit-aliran-kunci

Indikator: Mahasiswa dapat mengidentifikasikan *cipher* blok

Soal:

1. 1) Bit per bit
   2) Kata per kata
   3) Huruf per huruf
   4) Blok per blok
   5) Byte per byte
   Proses enkripsi dan dekripsi pada cipher blok dapat dilakukan dengan cara mentransformasikan nomor...
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. 5)

   Kunci Jawaban: d. 4)

2. Cipher blok termasuk ke dalam salah satu algoritma kriptografi...
   a. Asimetri
   b. Simetri
   d. Transposisi
   e. Permutasi

c. Transisi

Kunci Jawaban: b. Simetri

3. Cipher blok beroperasi pada...
   a. Bit tunggal
   b. Huruf
   c. Karakter
   d. Byte
   e. Blok

   Kunci Jawaban: e. Blok

4. Cara di bawah ini yang tidak dapat dilakukan untuk proses enkripsi dan dekripsi pada cipher blok, **kecuali**...
   a. Mentransformasikan huruf per huruf
   b. Mentransformasikan byte per byte
   c. Mentransformasikan blok per blok
   d. Mentransformasikan kata per kata
   e. Mentransformasikan bit per bit

   Kunci Jawaban: c. Mentransformasikan blok per blok

5. 1) Substitusi
   2) Transposisi
   3) Faktorisasi
   4) Diferensiasi
   Teknik di atas yang **bukan** merupakan teknik kriptografi klasik yang digabungkan dalam proses enkripsi pada algoritma cipher blok adalah...
   a. 1) dan 3)
   b. 1) dan 2)
   c. 2) dan 4)
   d. 3) dan 4)
   e. 4)

   Kunci Jawaban: d. 3) dan 4)

6. Di bawah ini merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher*, **kecuali**...
   a. *Electronic Code Book* (*ECB*)
   b. *Cipher Block Chaining* (*CBC*)
   c. *Cipher Feedback* (*CFC*)
   d. *Output Feedback* (*OFB*)
   e. *Input Feedback* (IFB)

   Kunci Jawaban: e. *Input Feedback* (IFB)

7. 1) *Electronic Code Book* (*ECB*)
   2) *Cipher Block Chaining* (*CBC*)
   3) *Cipher Feedback* (*CFC*)
   4) *Output Feedback* (*OFB*)
   5) *Input Feedback* (IFB)

Pada mode di atas yang **bukan** merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah...

a. 5)
b. 4)
c. 3)
d. 2)
e. 1)

Kunci Jawaban: a. 5)

8. Di bawah ini yang merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah...
   a. *Plaintext Block Chaining* (PBC)
   b. *Cipher Block Chaining* (CBC)
   c. *Plaintext Feedback* (PFC)
   d. *Electronic Feedback* (EFB)
   e. *Input Feedback* (IFB)

   Kunci Jawaban: b. *Cipher Block Chaining* (CBC)

9. 1) *Plaintext Block Chaining* (PBC)
   2) *Plaintext Feedback* (PFC)
   3) *Electronic Feedback* (EFB)
   4) *Cipher Block Chaining* (CBC)
   5) *Input Feedback* (IFB)

   Pada mode di atas yang merupakan mode operasi yang lazim diterapkan pada sistem blok *cipher* adalah...

   a. 5)
   b. 4)
   c. 3)
   d. 2)
   e. 1)

   Kunci Jawaban: b. 4)

Indikator: Mahasiswa dapat mendeskripsikan prinsip perancangan *cipher* blok

Soal:

1. Prinsip perancangan cipher blok yang menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks adalah...
   a. *Feistel Network*
   b. *Iterated Cipher*
   c. *S-Box*
   d. *Confussion*
   e. *Diffusion*

   Kunci Jawaban: e. *Diffusion*

2. Fungsi transformasi sederhana yang mengubah plainteks menjadi cipherteks diulang beberapa kali pada prinsip perancangan cipher blok disebut...
   a. *Feistel Network*
   d. *Confussion*

b. *Iterated Cipher*
c. *S-Box*
e. *Diffusion*

Kunci Jawaban: b. *Iterated Cipher*

3. Model jaringan yang membuat algoritma kriptografi menjadi reversible merupakan prinsip perancangan cipher blok yaitu...
   a. *Feistel Network*
   b. *Iterated Cipher*
   c. *S-Box*
   d. *Confussion*
   e. *Diffusion*

   Kunci Jawaban: a. *Feistel Network*

4. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain pada prinsip perancangan cipher blok disebut...
   a. *Feistel Network*
   b. *Iterated Cipher*
   c. *S-Box*
   d. *Confussion*
   e. *Diffusion*

   Kunci Jawaban: c. *S-Box*

5. Prinsip perancangan *cipher* blok berupa *confussion* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks
   c. Mengubah plainteks menjadi cipherteks diulang beberapa kali
   d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
   e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

   Kunci Jawaban: a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci

6. Prinsip perancangan *cipher* blok berupa *diffusion* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks
   c. Mengubah plainteks menjadi cipherteks diulang beberapa kali
   d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
   e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

Kunci Jawaban: b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks

7. Prinsip perancangan *cipher* blok berupa *iterated cipher* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks
   c. Mengubah plainteks menjadi cipherteks diulang beberapa kali
   d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
   e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

   Kunci Jawaban: c. Mengubah plainteks menjadi cipherteks diulang beberapa kali

8. Prinsip perancangan *cipher* blok berupa *feistel network* berarti...
   a. Model jaringan yang membuat algoritma kriptografi menjadi *reversible*
   b. Model jaringan yang mendukung proses enkripsi
   c. Model jaringan yang mendukung proses dekripsi
   d. Model jaringan yang sulit untuk dilakukan *hijacking*
   e. Model jaringan yang membuat algoritma kriptografi menjadi aman dari kriptanalis

   Kunci Jawaban: a. Model jaringan yang membuat algoritma kriptografi menjadi *reversible*

9. Prinsip perancangan *cipher* blok berupa *weak key* berarti...
   a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
   b. Kunci acak hasil *keystream generator* sama dengan *keystream* sebelumnya
   c. Kunci yang sama digunakan pada dua cipherteks
   d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
   e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

   Kunci Jawaban: d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi

10. Prinsip perancangan *cipher* blok berupa *s-box* berarti...
    a. Menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci
    b. Menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks
    c. Mengubah plainteks menjadi cipherteks diulang beberapa kali

d. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi
e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

Kunci Jawaban: e. Matriks yang berisi subtitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit yang lain

11. Kunci yang menyebabkan tidak adanya perbedaan antara enkripsi dan dekripsi merupakan prinsip perancangan *cipher* blok yaitu...
    a. *Strong key*
    b. *Weak key*
    c. *Long key*
    d. *Short key*
    e. *Low key*

    Kunci Jawaban: b. *Weak key*

Indikator: Mahasiswa dapat menjelaskan konsep kriptografi kunci publik

Soal:

1. Konsep sistem kriptografi kunci publik ditemukan oleh...
    a. Ron Rivest
    b. Adi Shamir
    c. Diffie dan Hellman
    d. Leonard dan Adleman
    e. Baron Lyon

    Kunci Jawaban: c. Diffie dan Hellman

2. Kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi, merupakan ide dasar dari sistem kriptografi...
    a. *Keystream*
    b. Caesar Cipher
    c. Modern
    d. Kunci privat
    e. Kunci publik

    Kunci Jawaban: e. Kunci Publik

3. Keamanan sistem kriptografi kunci publik terletak pada...
    a. Sulitnya menurunkan kunci rahasia dari kunci publik
    b. Sulitnya menurunkan cipherteks dari plainteks
    c. Sulitnya mengubah susunan bit rangkaian pada proses enkripsi
    d. Sulitnya mengubah susunan byte rangkaian pada proses dekripsi
    e. Sulitnya membuat logaritma setiap bit

    Kunci Jawaban: a. Sulitnya menurunkan kunci rahasia dari kunci publik

4. Kelemahan sistem kriptografi kunci publik adalah...
    a. Memerlukan memori yang banyak

b. Data yang digunakan bersifat tidak rahasia karena memiliki kunci publik
c. Waktu yang dibutuhkan dalam proses enkripsi cepat sehingga mudah mendapat serangan
d. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri
e. Sulitnya menurunkan plainteks dari cipherteks

Kunci Jawaban: d. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri

5. Kunci yang digunakan pada proses dekripsi bersifat...
   a. Publik
   b. Privat
   c. Simetri
   d. Sementara
   e. Tetap

   Kunci Jawaban: b. Privat

Indikator: Mahasiswa dapat mengidentifikasikan algoritma RSA

Soal:

1. Keamanan algoritma RSA terletak pada...
   a. Sulitnya memfaktorkan bilangan prima menjadi bilangan bulat
   b. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima
   c. Sulitnya mencari faktor bilangan prima pada proses enkripsi
   d. Sulitnya mencari faktor bilangan prima pada proses dekripsi
   e. Sulitnya mencari faktor bilangan bulat menjadi bilangan desimal

   Kunci Jawaban: b. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima

2. Pemfaktoran yang dilakukan pada algoritma RSA bertujuan untuk...
   a. Memperoleh kunci publik
   b. Memperoleh hasil enkripsi
   c. Memperoleh hasil dekripsi
   d. Memperoleh kunci pribadi
   e. Memperoleh data plainteks

   Kunci Jawaban: d. Memperoleh kunci pribadi

3. Alasan yang menjadikan algoritma RSA masih digunakan hingga kini adalah...
   a. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima
   b. Sulitnya mencari faktor bilangan bulat menjadi bilangan desimal
   c. Sulitnya memfaktorkan bilangan prima menjadi bilangan bulat
   d. Sulitnya mencari faktor bilangan prima pada proses enkripsi
   e. Sulitnya mencari faktor bilangan prima pada proses dekripsi

Kunci Jawaban: a. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima

4. 1) Bangkitkan kunci rahasia dengan menggunakan persamaan $SK \cdot PK \equiv 1 \pmod{\phi(r)}$.
   2) Hitung $\phi(r) = (p - 1)(q - 1)$.
   3) Pilih dua buah bilangan prima sembarang, p dan q.
   4) Hitung $r = p \cdot q$. Sebaiknya $p \neq q$, sebab jika $p = q$ maka $r = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari r.
   5) Pilih kunci publik, PK, yang relatif prima terhadap $\phi(r)$.
   Urutan prosedur yang benar untuk membuat pasangan kunci pada algoritma RSA adalah...
   a. 1) – 2) – 4) – 3) – 5)
   b. 4) – 1) – 3) – 2) – 5)
   c. 5) – 3) – 2) – 4) – 1)
   d. 2) – 4) – 1) – 3) – 5)
   e. 3) – 4) – 2) – 5) – 1)

   Kunci Jawaban: e. 3) – 4) – 2) – 5) – 1)

5. 1) Adi Shamir
   2) Leonard Adleman
   3) Ruth Davis
   4) Ron Rivest
   Nama di atas yang termasuk dalam pembuat algoritma RSA adalah...
   a. 1), 2), dan 3)
   b. 1), 2), dan 4)
   c. 2), 3), dan 4)
   d. 1), 3), dan 4)
   e. Semua benar

   Kunci Jawaban: b. 1), 2), dan 4)

6. 1) p dan q bilangan prima
   2) PK (kunci enkripsi)
   3) SK (kunci dekripsi)
   4) X (plainteks)
   5) Y (cipherteks)
   Besaran di atas yang bersifat rahasia pada algoritma RSA adalah...
   a. 1), 3), dan 4)
   b. 1), 2), dan 5)
   c. 2), 3), dan 5)
   d. 2), 3), dan 4)
   e. 1), 3), dan 5)

   Kunci Jawaban: a. 1), 3), dan 4)

7. 1) p dan q bilangan prima
   2) PK (kunci enkripsi)
   3) SK (kunci dekripsi)
   4) X (plainteks)
   5) Y (cipherteks)

Besaran di atas yang bersifat tidak rahasia pada algoritma RSA adalah...

a. 1) dan 4)
b. 2) dan 3)
c. 2) dan 5)
d. 3) dan 4)
e. 1) dan 5)

Kunci Jawaban: c. 2) dan 5)

8. Kunci RSA pada umumnya memiliki panjang...

a. 64 – 128 bit
b. 128 – 256 bit
c. 256 – 512 bit
d. 512 – 1024 bit
e. 1024 – 2048 bit

Kunci Jawaban: e. 1024 – 2048 bit

9. $C = M^e \bmod n$ merupakan fungsi pada algoritma RSA untuk melakukan proses...

a. Dekripsi
b. Pembangkitan kunci
c. Faktorisasi bilangan prima
d. Enkripsi
e. Pencarian bilangan prima

Kunci Jawaban: d. Enkripsi

10. $M = C^d \bmod n$ merupakan fungsi pada algoritma RSA untuk melakukan proses...

a. Dekripsi
b. Pembangkitan kunci
c. Faktorisasi bilangan prima
d. Enkripsi
e. Pencarian bilangan prima

Kunci Jawaban: a. Dekripsi

11. Cipherteks pada algoritma RSA bersifat...

a. Simetris
b. Privat
c. Publik
d. Sementara
e. Tetap

Kunci Jawaban: c. Publik

12. Kunci dekripsi pada algoritma RSA bersifat...

a. Simetris
b. Privat
c. Publik
d. Sementara
e. Tetap

Kunci Jawaban: b. Privat

Indikator: Mahasiswa dapat menjelaskan algoritma *ElGamal*

Soal:

1. Awal mula penggunaan algoritma *ElGamal* adalah untuk...
   a. Layanan Wifi
   b. GSM
   c. Satelit radio
   d. Tanda tangan digital
   e. Jaringan WAN

   Kunci Jawaban: d. Tanda tangan digital

2. Kekuatan algoritma *ElGamal* terleta pada...
   a. Sulitnya menghitung logaritma diskrit
   b. Sulitnya menghitung integral bilangan
   c. Sulitnya menghitung faktor bilangan
   d. Sulitnya menghitung diferensial diskrit
   e. Sulitnya menghitung pengakaran prima

   Kunci Jawaban: a. Sulitnya menghitung logaritma diskrit

3. 1) Pilih dua buah bilangan acak, g dan x, dengan syarat $g < p$ dan $x < p$.
   2) Pilih sembarang bilangan prima p.
   3) Kunci publik adalah y, kunci rahasia adalah x. Nilai g dan p tidak dirahasiakan dan dapat diumumkan kepada anggota kelompok.
   4) Hitung $y = g^x \bmod p$.

   Urutan prosedur yang benar untuk membuat pasangan kunci pada algoritma *ElGamal* adalah...
   a. 3) – 2) – 4) – 1)
   b. 1) – 2) – 4) – 3)
   c. 2) – 1) – 4) – 3)
   d. 3) – 1) – 4) – 2)
   e. 4) – 2) – 3) – 1)

   Kunci Jawaban: c. 2), 1), 4), dan 3)

4. 1) Bilangan prima, p
   2) Bilangan acak, g ($g < p$)
   3) Bilangan acak, x ($x < p$)
   4) M (plainteks)
   5) a dan b (cipherteks)

   Besaran di atas yang bersifat rahasia pada algoritma *ElGamal* adalah...
   a. 1) dan 2)
   b. 3) dan 4)
   c. 4) dan 5)
   d. 2) dan 3)
   e. 1) dan 5)

   Kunci Jawaban: b. 3) dan 4)

5. 1) Bilangan prima, p
   2) Bilangan acak, g ($g < p$)
   3) Bilangan acak, x ($x < p$)
   4) M (plainteks)
   5) a dan b (cipherteks)

   Besaran di atas yang bersifat tidak rahasia pada algoritma *ElGamal* adalah...

   a. 1), 2), dan 3)
   b. 3), 4), dan 5)
   c. 2), 4), dan 5)
   d. 2), 3), dan 4)
   e. 1), 2), dan 5)

   Kunci Jawaban: e. 1), 2), dan 5)

Indikator: Mahasiswa dapat mengidentifikasikan algoritma *rabin*

Soal:

1. 1) Menghitung nilai $n = p$ x q
   2) Memilih dua buah bilangan prima p dan q
   3) Mendapatkan nilai kunci publik dan kunci privat, dimana kunci publik adalah n dan kunci privat adalah q dan n

   Urutan prosedur yang benar untuk membangkitkan kunci pada algoritma Rabin adalah...

   a. 3) – 1) – 2)
   b. 2) – 1) – 3)
   c. 1) – 2) – 3)
   d. 1) – 3) – 2)
   e. 3) – 2) – 1)

   Kunci Jawaban: b. 2) – 1) – 3)

2. "P^2 mod n" pada algoritma Rabin merupakan rumus...

   a. Pembangkitan kunci
   b. Faktor bilangan
   c. Logaritma diskrit
   d. Proses dekripsi
   e. Proses enkripsi

   Kunci Jawaban: e. Proses enkripsi

3.
```
Enkripsi(n,P)
{
      C ← P^2 mod n
      return C
}
```

   Potongan program di atas merupakan proses enkripsi pada algoritma...

   a. RSA
   b. RC4
   d. MD5
   e. A5

c. Rabin

Kunci Jawaban: c. Rabin

4.
```
{
    Pilih 2 bilangan prima p dan q
    dalam persamaan 4k+3

    n ← p x q

    kunci_publik ← n
    kunci_privat ← (q, n)

    return kunci_publik dan kunci_privat
}
```

Potongan program di atas merupakan proses pembangkitan kunci pada algoritma...

a. Rabin
b. RSA
c. RC4
d. A5
e. MD5

Kunci Jawaban: a. Rabin

5.
```
Dekripsi(p,q,C)
{
    a1 ← +(C^((p+1)/4)) mod p
    a2 ← -(C^((p+1)/4)) mod p
    b1 ← +(C^((q+1)/4)) mod q
    b2 ← -(C^((q+1)/4)) mod q

    // Chinese_Rem adalah fungsi yang
    // memanggil fungsi untuk Chinese
    // Remainder

    P1 ← Chinese_Rem(a1,b1,p,q)
    P2 ← Chinese_Rem(a1,b2,p,q)
    P3 ← Chinese_Rem(a2,b1,p,q)
    P4 ← Chinese_Rem(a2,b2,p,q)

    return P1,P2,P3,P4
}
```

Potongan program di atas merupakan proses dekripsi pada algoritma...

a. MD5
b. A5
c. RC4
d. Rabin
e. RSA

Kunci Jawaban: d. Rabin

6. Algoritma *Rabin* merupakan algoritma dengan kriptografi...
   a. Simetris
   b. Kunci rahasia
   c. Kunci publik
   d. Cipher substitusi
   e. Cipher transposisi

   Kunci Jawaban: c. Kunci publik

7. Keamanan algoritma *Rabin* terletak pada...
   a. Sulitnya memfaktorkan bilangan prima menjadi bilangan bulat
   b. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima
   c. Sulitnya mencari faktor bilangan prima pada proses enkripsi
   d. Sulitnya mencari faktor bilangan prima pada proses dekripsi
   e. Sulitnya mencari faktor bilangan bulat menjadi bilangan desimal

   Kunci Jawaban: b. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima

8. Kunci dekripsi pada algoritma *Rabin* bersifat...
   a. Simetris
   b. Sementara
   c. Tetap
   d. Privat
   e. Publik

   Kunci Jawaban: d. Privat

9. Kunci enkripsi pada algoritma *Rabin* bersifat...
   a. Simetris
   b. Sementara
   c. Tetap
   d. Privat
   e. Publik

   Kunci Jawaban: e. Publik

10. Proses enkripsi pada algoritma *Rabin* dapat dilakukan dalam waktu yang relatif singkat sehingga memiliki keuntungan menghadapi keterbatasan *resource* yang ada pada media kriptografi seperti...
    a. *Smart card*
    b. Tanda tangan digital
    c. *E-commerce*
    d. Otentikasi pin
    e. Kartu kredit

    Kunci Jawaban: a. *Smart card*

11. Proses enkripsi pada algoritma *Rabin* dapat dilakukan dalam waktu yang relatif singkat sehingga memiliki keuntungan yaitu...
    a. Memudahkan pengirim pesan untuk mengenkripsi plainteks dengan cepat
    b. Dapat mengefisienkan waktu yang digunakan dalam proses enkripsi
    c. Menghadapi keterbatasan *resource* yang ada pada media kriptografi
    d. Tidak mudah untuk dilakukan *hijacking* oleh kriptanalis
    e. Tidak membutuhkan kunci yang rumit pada proses enkripsi

    Kunci Jawaban: c. Menghadapi keterbatasan *resource* yang ada pada media kriptografi

Indikator: Mahasiswa dapat menjelaskan pembangkit bilangan prima

Soal:

1. Membangkitkan bilangan acak dan menguji kemungkinan bilangan tersebut prima merupakan salah satu metode untuk...
    a. Pembangkit bilangan acak
    b. Pembangkit bilangan acak semu
    c. Memfaktorkan bilangan prima
    d. Pembangkit bilangan prima
    e. Mencari logaritma diskrit

    Kunci Jawaban: d. Pembangkit bilangan prima

2. Teknik yang akan membagi sebuah bilangan yang akan diuji dengan semua bilangan bulat positif yang lebih kecil dari akar bilangan tersebut disebut...
    a. *Brute force*
    b. *Pseudorandom generator*
    c. *Keystream generator*
    d. *Keystream*
    e. *Digital signature*

    Kunci Jawaban: a. *Brute force*

3. Kelemahan dari teknik *brute force* adalah...
    a. Semakin banyak bilangan bulat yang akan digunakan sebagai pembagi maka semakin besar pula media penyimanan yang digunakan untuk menguji
    b. Semakin banyak bilangan bulat yang akan digunakan sebagai pembagi maka semakin besar pula waktu yang dibutuhkan untuk menguji
    c. Semakin banyak bilangan bulat yang akan digunakan sebagai pembagi maka semakin besar pula data algoritma yang akan dihasilkan
    d. Menggunakan sedikit bilangan bulat yang digunakan sebagai pembagi bilangan prima
    e. Menggunakan akar logaritma diskrit yang membutuhkan perangkat khusus untuk menghitungnya

Kunci Jawaban: b. Semakin banyak bilangan bulat yang akan digunakan sebagai pembagi maka semakin besar pula waktu yang dibutuhkan untuk menguji

4. Salah satu metode dalam pembangkit bilangan prima yaitu menggunakan teknik yang mirip dengan *brute force* yang memiliki perbedan pada...
   a. Pemfaktoran bilangan prima dengan bilangan besar
   b. Logaritma diskrit yang digunakan lebih sedikit
   c. Menggunakan setiap kemungkinan diferensial bilangan
   d. Menggunakan pembagi bilangan yang bernilai besar
   e. Menggunakan pembagi yang jauh lebih sedikit

   Kunci Jawaban: e. Menggunakan pembagi yang jauh lebih sedikit

5. Dalam pembangkit bilangan prima, menggunakan pembagi yang jauh lebih sedikit memiliki kelemahan yaitu...
   a. Memakan waktu yang lama pada saat pengujian
   b. Data algoritma yang dihasilkan memiliki banyak bilangan prima
   c. Bergantung pada media penyimpanan bilangan prima yang pernah dihasilkan
   d. Membutuhkan biaya tambahan untuk penggunaan perangkat khusus
   e. Data pengujian tidak akurat untuk menemukan nilai bilangan prima

   Kunci Jawaban: c. Bergantung pada media penyimpanan bilangan prima yang pernah dihasilkan

Indikator: Mahasiswa dapat menjelaskan pembangkit bilangan acak semu

Soal:

1. Keunggulan *Linear Congruential Generator* (LCG) terletak pada...
   a. Algoritmanya sulit ditembus oleh kriptanalis
   b. Kecepatannya dan hanya membutuhkan sedikit operasi bit
   c. Menggunakan algoritma operasi byte
   d. Tidak membutuhkan memori yang besar
   e. Data algoritma pada proses enkripsi tidak rumit

   Kunci Jawaban: b. Kecepatannya dan hanya membutuhkan sedikit operasi bit

2. *Linear Congruential Generator* (LCG) tidak dapat digunakan untuk kriptografi karena...
   a. Bilangan acaknya dapat diprediksi urutan kemunculannya
   b. Faktor bilangan terlalu rumit
   c. Logaritma diskritnya dapat diprediksi nilainya
   d. Membutuhkan memori yang besar
   e. Tidak lulus uji keacakan statistik

Kunci Jawaban: a. Bilangan acaknya dapat diprediksi urutan kemunculannya

3. Keamanan pembangkit bilangan acak *Blum Blum Shub* (BBS) terletak pada...
   a. Logaritma diskrit yang sulit dipecahkan
   b. Integral bilangan yang rumit
   c. Sulitnya memfaktorkan hasil kali dua bilangan prima
   d. Diferensial bilangan yang tidak mudah diketahui nilainya
   e. Nilai perpangkatan yang tinggi

   Kunci Jawaban: c. Sulitnya memfaktorkan hasil kali dua bilangan prima

4. Pembangkit bilangan acak *Blum Blum Shub* (BBS) berbasis pada...
   a. Biner
   b. Teori peluang
   c. Bit
   d. Byte
   e. Teori bilangan

   Kunci Jawaban: e. Teori bilangan

5. Salah satu contoh penggunaan pembangkit bilangan acak semu yaitu untuk pembangkitan parameter kunci pada...
   a. Algoritma kunci publik
   b. Algoritma kunci privat
   c. Algoritma *cipher* transposisi
   d. Algoritma *cipher* substitusi
   e. Algoritma kunci asimetris

   Kunci Jawaban: a. Algoritma kunci publik

6. *LCG* (*Linear Congruential Generator*) berguna untuk aplikasi non-kriptografi seperti...
   a. Kartu kredit
   b. ATM
   c. Simulasi
   d. Otentikasi PIN
   e. E-commerce

   Kunci Jawaban: d. Simulasi

7. 1) Memori yang dibutuhkan tidak terlalu besar
   2) Data algoritma memiliki kompleksitas yang tinggi
   3) Lolos uji keacakan statistik
   4) Logaritma diskrit yang tidak mudah ditembus

   Salah satu syarat sebagai pembangkit bilangan acak yang cocok untuk kriptografi ditunjukkan oleh nomor..
   a. 1)
   b. 2)
   c. 3)
   d. 4)
   e. Semua Benar

   Kunci Jawaban: c. 3)

8. Dibawah ini yang termasuk dalam contoh pembangkit bilangan acak semu, **kecuali**...
   a. *InitializationVector*
   b. *Linear Congruential Generator*
   c. *Blum Blum Shut*
   d. *Pseudo-Random Number Generator*
   e. *Cryptographically Secure Pseudorandom Generator*

   Kunci Jawaban: a. *Initialization Vector*

9. 1) *Blum Blum Shut*
   2) *Chaos*
   3) *InitializationVector*
   4) *Linear Congruential Generator*
   5) *Keystream Generator*
   Contoh di atas yang bukan termasuk dalam contoh pembangkit bilangan acak semu adalah...
   a. 1) dan 3)
   b. 2) dan 4)
   c. 3) dan 4)
   d. 4) dan 5)
   e. 3) dan 5)

   Kunci Jawaban: e. 3) dan 5)

10. 1) Nilai bilangan harus non-prima
    2) Data algoritma memiliki kompleksitas yang tinggi
    3) Memori yang dibutuhkan tidak terlalu besar
    4) Tahan terhadap serangan yang serius
    Salah satu syarat sebagai pembangkit bilangan acak yang cocok untuk kriptografi ditunjukkan oleh nomor..
    a. 1)
    b. 2)
    c. 3)
    d. 4)
    e. Semua Benar

    Kunci Jawaban: d. 4)

Indikator: Mahasiswa dapat mengidentifikasikan fungsi *hash* satu arah

Soal:

1. Salah satu sifat dari fungsi *hash* satu arah, **kecuali**...
   a. Fungsi *H* dapat diterapkan pada blok data berukuran berapa saja
   b. *H* menghasilkan nilai (*h*) dengan panjang tetap
   c. *H*(*x*) mudah dihitung untuk setiap nilai *x* yang diberikan tetap

d. Untuk setiap *h* yang dihasilkan, tidak mungkin dikembalikan nilai *x* sedemikian sehingga *H*(*x*) = *h*
e. Setiap variabel pada fungsi H bersifat bilangan non-prima

Kunci Jawaban: e. Setiap variabel pada fungsi H bersifat bilangan non-prima

2. Salah satu contoh dari fungsi *hash* satu arah, **kecuali**...
   a. MD2
   b. RSA
   c. MD4
   d. MD5
   e. SHA

   Kunci Jawaban: b. RSA

3. 1) SHA
   2) RSA
   3) MD5
   4) A5
   Algoritma di atas yang termasuk dalam contoh fungsi *hash* satu arah adalah...
   a. 1) dan 2)
   b. 2) dan 3)
   c. 1) dan 4)
   d. 1) dan 3)
   e. 2) dan 4)

   Kunci Jawaban: d. 1) dan 3)

4. Salah satu sifat dari fungsi *hash* satu arah adalah...
   a. Fungsi *H* dapat diterapkan pada blok data berukuran berapa saja
   b. Setiap variabel pada fungsi *Hash* didapat dari pemfaktoran bilangan
   c. *H*(*x*) sulit dihitung untuk setiap nilai *x* yang diberikan tetap
   d. Untuk setiap *h* yang dihasilkan, sangat mungkin dikembalikan nilai *x* sedemikian sehingga *H*(*x*) = *h*
   e. Setiap variabel pada fungsi H bersifat bilangan non-prima

   Kunci Jawaban: a. Fungsi H dapat diterapkan pada blok data berukuran berapa saja

5. Salah satu keuntungan penggunaan fungsi *hash* satu arah adalah...
   a. Algoritma tidak mudah diserang
   b. Menjaga integritas data
   c. Kompleksitas data bersifat tetap
   d. Kompleksitas memori hanya sedikit
   e. Data tersimpan dalam *host*

   Kunci Jawaban: b. Menjaga integritas data

6. Di bawah ini yang bukan merupakan keuntungan penggunaan fungsi *hash* satu arah adalah...
   a. Peka terhadap perubahan 1 bit pada pesan

b. Menormalkan panjang data yang beraneka ragam
c. Algoritma tidak mudah diserang
d. Menghemat waktu pengiriman
e. Menjaga integritas data

Kunci Jawaban: c. Algoritma tidak mudah diserang

7. Kolisi adalah...
   a. Nilai variabel pada *hash* bersifat bilangan prima
   b. Keadaan dimana nilai *hash* dapat didekripsi kembali
   c. Keadaan dimana nilai *hash* dapat dienkripsi kembali
   d. Kondisi dua *string* sembarang memiliki nilai *hash* yang sama
   e. Nilai variabel pada *hash* bersifat bilangan non-prima

   Kunci Jawaban: d. Kondisi dua *string* sembarang memiliki nilai *hash* yang sama

8. Kondisi dua *string* sembarang memiliki nilai *hash* yang sama disebut...
   a. *Chaos*
   b. Destruksi
   c. *Message digest*
   d. *Keystream*
   e. Kolisi

   Kunci Jawaban: e. Kolisi

9. Fungsi *hash* berarti...
   a. Mentransformasikan pesan menjadi *string* dengan ukuran tetap
   b. Melakukan uji coba statistik pada sebuah *string*
   c. Nilai-nilai variabel pada proses enkripsi bersifat tetap
   d. Nilai-nilai variabel pada proses dekripsi bersifat sementara
   e. Algoritma yang ditransformasikan dengan kunci privat

   Kunci Jawaban: a. Mentransformasikan pesan menjadi *string* dengan ukuran tetap

Indikator: Mahasiswa dapat menyebutkan algoritma MD5

Soal:

1. Algoritma MD5 menghasilkan *message digest* dengan panjang...
   a. 32 bit
   b. 64 bit
   c. 128 bit
   d. 256 bit
   e. 512 bit

   Kunci Jawaban: c. 128 bit

2. Pada algoritma MD5, pengolahan pesan dilakukan dalam blok berukuran...
   a. 512 bit
   d. 64 bit

b. 256 bit
c. 128 bit
e. 32 bit

Kunci Jawaban: a. 512 bit

3. 1) Penambahan nilai panjang pesan semula
   2) Pengolahan pesan dalam blok berukuran 512 bit
   3) Inisialisasi *buffer* MD
   4) Penambahan *padding bits*
   Urutan prosedur yang benar untuk pembuatan *message digest* pada algoritma MD5 adalah...
   a. 1) – 3) – 4) – 2)
   b. 4) – 1) – 3) – 2)
   c. 3) – 1) – 4) – 2)
   d. 2) – 4) – 1) – 3)
   e. 2) – 1) – 3) – 4)

   Kunci Jawaban: b. 4) – 1) – 3) – 2)

4. Algoritma MD5 membutuhkan 4 buah *buffer* dengan panjang masing-masingnya adalah...
   a. 512 bit
   b. 128 bit
   c. 256 bit
   d. 32 bit
   e. 64 bit

   Kunci Jawaban: d. 32 bit

5. Pada pengolahan pesan dalam algoritma MD5, proses H_{MD5} memiliki putaran sebanyak...
   a. 5 putaran
   b. 3 putaran
   c. 2 putaran
   d. 8 putaran
   e. 4 putaran

   Kunci Jawaban: e. 4 putaran

6. Algoritma MD5 adalah fungsi hash satu arah yang dibuat oleh...
   a. Ron Rivest
   b. Lucifer
   c. Adi Shamir
   d. Charles Babbage
   e. Baron Lyon

   Kunci Jawaban: a. Ron Rivest

7. Total panjang penyangga pada inisialisasi penyangga MD dalam algoritma MD5 adalah...
   a. 512 bit
   b. 128 bit
   c. 256 bit
   d. 32 bit
   e. 64 bit

   Kunci Jawaban: b. 128 bit

8. Panjang proses H_{MD5} pada algoritma MD5 adalah...
   a. 512 bit
   b. 128 bit
   c. 256 bit
   d. 32 bit
   e. 64 bit

   Kunci Jawaban: b. 128 bit

9. Kriptanalisis yang dapat dilakukan pada algoritma MD5 adalah...
   a. Destruksi
   b. *Padding bits*
   c. *Message digest*
   d. Kolisi
   e. *Chaos*

   Kunci Jawaban: d. Kolisi

10. Penemu dari kolisi algoritma MD5 adalah...
    a. Ron rivest
    b. Charles Babbage
    c. Vlastimil Klima
    d. Lucifer
    e. Leonard Adleman

    Kunci Jawaban: c. Vlastimil Klima

Indikator: Mahasiswa dapat mengidentifikasikan algoritma MAC

Soal:

1. Fungsi satu arah yang menggunakan kunci rahasia dalam pembangkitan nilai *hash* disebut...
   a. RSA
   b. RC4
   c. A5
   d. MAC
   e. MD5

   Kunci Jawaban: d. MAC

2. Kegunaan algoritma MAC adalah...
   a. Untuk melakukan pembangkitan kunci bilangan acak semu
   b. Untuk melakukan pembangkitan kunci bilangan prima
   c. Untuk otentikasi tanpa perlu merahasiakan pesan
   d. Untuk menentukan jumlah cipher blok yang digunakan
   e. Untuk memudahkan pemfaktoran bilangan prima

   Kunci Jawaban: c. Untuk otentikasi tanpa perlu merahasiakan pesan

3. Algoritma MAC berbasiskan pada...
   a. Cipher blok
   b. Cipher substitusi
   c. Caesar cipher
   d. Cipher aliran
   e. Ekspansi cipher

Kunci Jawaban: a. Cipher blok

4. MAC dibangkitkan dengan menggunakan algoritma cipher blok dengan mode...
   a. *Electronic Code Book*
   b. *Output Feedback*
   c. *Cipher Code Book*
   d. *Plain Code Book*
   e. *Cipher Feedback*

   Kunci Jawaban: e. *Cipher Feed Back*

5. Algoritma MAC tidak memiliki fungsi tanda tangan digital, tetapi menyediakan...
   a. Kerahasiaan data pengirim pesan
   b. Otentikasi pengirim dan otentikasi pesan
   c. Dokumentasi proses pengiriman dan penerimaan pesan
   d. Efisiensi waktu pada proses pemgiriman pesan
   e. Kerahasiaan data penerima pesan

   Kunci Jawaban: b. Otentikasi pengirim dan otentikasi pesan

6. Salah satu contoh penggunaan algoritma MAC adalah...
   a. Pembuatan dan verifikasi tanda tangan digital
   b. Otentikasi PIN pada kartu ATM
   c. Otentikasi arsip yang digunakan lebih dari satu orang pengguna
   d. Penerimaan pesan pada GSM *mobile phone*
   e. Melakukan enkripsi pada pengirian sinyal *handphone* ke BTS

   Kunci Jawaban: c. Otentikasi arsip yang digunakan lebih dari satu orang pengguna

7. Algoritma MAC mempunyai 2 basis yaitu...
   a. Berbasis *cipher* aliran dan *cipher* blok
   b. Berbasis *cipher* aliran dan fungsi *hash*
   c. Berbasis kriptografi simetri dan asimetri
   d. Berbasis kriptografi asimetri dan *cipher* blok
   e. Berbasis *cipher* blok dan fungsi *hash* satu arah

   Kunci Jawaban: e. Berbasis *cipher* blok dan fungsi *hash* satu arah

8. Pada algoritma MAC berbasiskan fungsi *hash* satu arah, MAC dari sebuah pesan merupakan...
   a. Pembangkitan kunci rahasia dengan faktor bilangan
   b. Hasil enkripsi dari fungsi *hash* satu arah
   c. Hasil dekripsi dari fungsi *hash* satu arah
   d. Nilai *hash* dari penyambungan pesan dengan kunci
   e. Pembangkitan kunci rahasia dengan logaritma diskrit

   Kunci Jawaban: d. Nilai hash dari penyambungan pesan dengan kunci

Indikator: Mahasiswa dapat mengidentifikasikan konsep tanda tangan digital

Soal:

1. Penggunaan tanda tangan digital membutuhkan proses...
   a. Pembentukan tanda tangan digital
   b. Otentikasi tanda tangan digital
   c. Enkripsi dan dekripsi pada pembentukan tanda tangan digital
   d. Dekripsi pada otentikasi tanda tangan digital
   e. Pembentukan tanda tangan digital dan verifikasi tanda tangan digital

   Kunci Jawaban: e. Pembentukan tanda tangan digital dan verifikasi tanda tangan digital

2. Semua proses yang dilakukan pada tanda tangan digital menerapkan fungsi...
   a. MD5
   b. DAA
   c. SHA
   d. *Hash*
   e. RSA

   Kunci Jawaban: d. *Hash*

3. Di bawah ini merupakan unsur-unsur yang paling penting pada proses pembentukan dan verifikasi tanda tangan digital, **kecuali**...
   a. Integritas data
   b. Otentikasi penandatangan
   c. Otentikasi Dokumen
   d. Penegasan
   e. Efisiensi

   Kunci Jawaban: a. Integritas data

4. Kelemahan dari teknologi tanda tangan digital adalah...
   a. Membutuhkan proses yang lama untuk otentikasi data
   b. Memerlukan biaya tambahan secara institusional
   c. Mudah dipalsukan
   d. Penggunaan memori yang terlalu besar
   e. Kompleksitas integritas data yang sangat tinggi

   Kunci Jawaban: b. Memerlukan biaya tambahan secara institusional

5. Otentikasi penandatangan merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti...
   a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
   b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
   c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi

d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya

Kunci Jawaban: b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan

6. Otentikasi dokumen merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti...
   a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
   b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
   c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
   d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
   e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya

   Kunci Jawaban: c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi

7. Penegasan merupakan salah satu unsur penting pada pembentukan dan verifikasi tanda tangan digital yang berarti...
   a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
   b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan
   c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
   d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
   e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya

   Kunci Jawaban: d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan

8. Proses pembentukan tanda tangan digital pada penggunaan tanda tangan digital berarti...
   a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan
   b. Pasangan kunci publik dan kunci privat berasosiasi dengan pemilik sah penandatangan

c. Tanda tangan digital juga mengidentikkan dokumen yang ditandatangani dengan ketepatan yang tinggi
d. Membuat tanda tangan digital memerlukan penggunaan kunci privat dari penandatangan
e. Tidak perlu ada verifikasi antara tanda tangan yang terdapat di dokumen dengan contoh tanda tangan aslinya

Kunci Jawaban: a. Menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat penandatangan

Indikator: Mahasiswa dapat mengidentifikasikan protokol kriptografi

Soal:

1. Protokol kriptografi digunakan untuk...
   a. Proses enkripsi pada algoritma kriptografi
   b. Proses dekripsi pada algoritma kriptografi
   c. Mencari sebuah kunci pada setiap proses enkripsi
   d. Berbagi komponen rahasia untuk menghitung sebuah nilai
   e. Pengiriman hasil cipherteks kepada penerima pesan

   Kunci Jawaban: d. Berbagi komponen rahasia untuk menghitung sebuah nilai

2. Di bawah ini yang bukan kegunaan protokol kriptografi adalah...
   a. Pengiriman hasil cipherteks kepada penerima pesan
   b. Berbagi komponen rahasia untuk menghitung sebuah nilai
   c. Membangkitkan rangkaian bilangan acak
   d. Proses otentikasi identitas
   e. Membangkitkan rangkaian bilangan prima

   Jawaban: a. Pengiriman hasil cipherteks kepada penerima pesan

3. Algoritma terdistribusi yang didefinisikan sebagai barisan langkah-langkah secara tepat menspesifikasikan tindakan-tindakan dari dua entitas atau lebih yang diperlukan untuk mencapai tujuan keamanan tertentu disebut...
   a. Algortima kriptografi
   b. Pembangkitan kunci
   c. Protokol kriptografi
   d. *Keystream*
   d. *Keystream generator*

   Kunci Jawaban: c. Protokol kriptografi

4. Dalam mendesain protokol kriptografi dua langkah penting yang harus diperhatikan adalah...
   a. Proses otentikasi pada pengirim dan penerima pesan

b. Identifikasi semua asumsi yang digunakan dan tentukan pengaruhnya terhadap tujuan keamanan jika asumsi itu dilanggar
c. Penggunaan setiap kunci yang akan digunakan pada setiap proses enkripsi dan dekripsi
d. Proses enkripsi dan dekripsi yang terjamin keamanan algoritmanya
e. Setiap pembangkitan kunci bilangan prima dan acak semu harus bersifat *private* atau rahasia

Kunci Jawaban: b. Identifikasi semua asumsi yang digunakan dan tentukan pengaruhnya terhadap tujuan keamanan jika asumsi itu dilanggar

5. Sebuah kunci yang dipertukarkan antara pengirim dan penerima pesan pada protokol kriptografi disebut...
   a. *Switching key*
   b. *Keystream*
   c. *Generator key*
   d. *Session key*
   e. *Weak key*

   Kunci Jawaban: d. *Session key*

6. Protokol komunikasi dengan sistem kriptografi simetri tidak bagus karena...
   a. Kunci harus tetap rahasia sebelum, sepanjang, dan setelah protokol
   b. Biaya opersional yang digunakan menjadi besar
   c. Proses sertifikasi keabsahan dokumen yag memakan waktu lama
   d. Algoritma protokol yang digunakan terlalu rumit
   e. Penggunaan protokol komunikasi dengan sistem kriptografi yang tidak aman

   Kunci Jawaban: a. Kunci harus tetap rahasia sebelum, sepanjang, dan setelah protokol

7. Protokol menandatangani dokumen digital dengan sistem kriptografi simetri dan juru penengah tidak praktis karena...
   a. Kunci harus tetap rahasia sebelum, sepanjang, dan setelah protokol
   b. Biaya opersional yang digunakan menjadi besar
   c. Proses sertifikasi keabsahan dokumen yang memakan waktu lama
   d. Algoritma protokol yang digunakan terlalu rumit
   e. Penggunaan protokol komunikasi dengan sistem kriptografi yang tidak aman

   Kunci Jawaban: c. Proses sertifikasi keabsahan dokumen yang memakan waktu lama

8. *Hybrid Cryptosystem* adalah...
   a. Sebuah sistem kriptografi yag digunakan untuk pertukaran pesan
   b. Pertukaran kunci yang dilakukan pada protokol sistem kriptografi
   c. Sistem kriptografi yang berhasil disadap oleh kriptanalis
   d. Dua gabungan sistem kriptografi yang digunakan pada sebuah protokol
   e. Protokol kriptografi yang menggunakan sebuah sistem kriptografi

Kunci Jawaban: d. Dua gabungan sistem kriptografi yang digunakan pada sebuah protokol

9. *Session key* adalah...
   a. Kunci yang digunakan pada protokol komunikasi sebuah sistem kriptografi
   b. Kunci pada sebuah protokol yang menerapkan sistem kriptografi simetri
   c. Kunci pada sebuah protokol yang menerapkan sistem kriptografi kunci publik
   d. Kriptanalis berhasil mengetahui kunci yang digunakan pada protokol sebuah sistem kriptografi
   e. Sebuah kunci yang dipertukarkan antara pengirim dan penerima pesan pada protokol kriptografi

   Kunci Jawaban: e. Sebuah kunci yang dipertukarkan antara pengirim dan penerima pesan pada protokol kriptografi

Indikator: Mahasiswa dapat menganalisis penggunaan kriptografi dalam kehidupan sehari-hari

Soal:

1. Di bawah ini yang termasuk contoh penggunaan kriptografi dalam kehidupan sehari-hari adalah...
   a. Pemancar radio
   b. Kartu cerdas
   c. Satelit TV
   d. Pemancar televisi
   e. Penguat sinyal

   Kunci Jawaban: b. Kartu cerdas

2. Penggunaan kriptografi dalam *Pay* TV berupa...
   a. *Smart card* yang beisikan kunci privat pelanggan
   b. Sinyal radio yang dienkripsi menggunakan sistem kriptografi simetri
   c. Dekripsi penerimaan sinyal melalui antena
   d. *Smart card* yang berfungsi untuk mengenkripsi pesan
   e. Pengiriman gelombang mikro menggunakan sistem kriptografi kunci publik

   Kunci Jawaban: a. Smart card yang berisikan kunci privat pelanggan

3. Sistem kriptografi yang digunakan pada komunikasi melalui GSM *mobile phone* adalah...
   a. Kunci publik
   b. Simetri
   c. *Stream cipher*
   d. *Caesar cipher*
   e. Asimetri

   Kunci Jawaban: c. *Stream cipher*

4. GSM *mobile phone* diperlukan dua kebutuhan keamanan, yaitu...
   a. Kerahasiaan dan otentikasi penerima pesan
   b. Otentikasi pengirim dan penerima pesan
   c. Efisiensi dan integritas data
   d. Integritas data dan verifikasi data
   e. Kerahasiaan dan otentikasi pengguna

   Kunci Jawaban: e. Kerahasiaan dan otentikasi pengguna

5. Dua kebutuhan keamanan pada GSM *mobile phone* dipenuhi dengan penggunaan...
   a. SIM *card*
   b. *Base station*
   c. Sinyal radio
   d. Gelombang mikro
   e. Antena

   Kunci Jawaban: a. SIM *card*