KOMBINASI VIGÈNERE CIPHER, ALGORITMA RSA, DAN ELGAMAL DALAM KRIPTOGRAFI CITRA DIGITAL BESERTA ANALISIS KEAMANANNYA

Skripsi

Disusun untuk memenuhi salah satu syarat
memperoleh gelar Sarjana Matematika

Rafiqa Oktaviani

1305621034

PROGRAM STUDI MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS NEGERI JAKARTA

2025

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI

KOMBINASI *VIGÈNERE CIPHER*, ALGORITMA RSA, DAN ELGAMAL DALAM KRIPTOGRAFI CITRA DIGITAL BESERTA ANALISIS KEAMANANNYA

Nama : Rafiqa Oktaviani

No. Registrasi : 1305621034

	Nama	Tanda Tangan	Tanggal
Penanggung Jawab Dekan	: Dr. Hadi Nasbey, S.Pd., M.Si. NIP. 197909162005011004		5 Agustus 2025
Wakil Penanggung Jawab Wakil Dekan I	: Dr. Meiliasari, S.Pd., M.Sc. NIP. 197905042009122002		5 Agustus 2025
Ketua	: Drs. Sudarwanto, M.Si., DEA. NIP. 196503251993031003		28 Juli 2025
Sekretaris	: Dr. Yudi Mahatma, M.Si. NIP. 197610202008121001		28 Juli 2025
Penguji Ahli	: Devi Eka Wardani M, S.Pd., M.Si. NIP. 199005162019032014		29 Juli 2025
Pembimbing I	: Dr. Lukita Ambarwati, S.Pd., M.Si. NIP. 197210262001122001		29 Juli 2025
Pembimbing II	: Ibnu Hadi, M.Si. NIP. 198107182008011017		29 Juli 2025

Dinyatakan lulus ujian skripsi tanggal 21 Juli 2025

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini, mahasiswa Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta:

Nama	:	Rafiqa Oktaviani
No Registrasi	:	1305621034
Program Studi	:	Matematika

Dengan ini menyatakan bahwa skripsi yang saya buat dengan judul *"Kombinasi Vigènere Cipher, Algoritma RSA, dan ElGamal dalam Kriptografi Citra Digital beserta Analisis Keamanannya"* adalah:

1. Dibuat sendiri, mengadopsi hasil kuliah, buku-buku, dan referensi acuan yang tertera di dalam referensi pada skripsi saya.
2. Bukan merupakan hasil duplikasi skripsi yang telah dipublikasikan atau pernah dipakai untuk mendapatkan gelar sarjana di Universitas lain kecuali pada bagian-bagian sumber informasi dicantumkan berdasarkan tata cara referensi yang semestinya.

Pernyataan ini dibuat dengan sesungguhnya dan saya bersedia menanggung segala akibat yang timbul jika pernyataan saya tidak benar.

Jakarta, 10 Juli 2025

Rafiqa Oktaviani

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI JAKARTA
UPT PERPUSTAKAAN

Jalan Rawamangun Muka Jakarta 13220
Telepon/Faksimili: 021-4894221
Laman: lib.unj.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika Universitas Negeri Jakarta, yang bertanda tangan di bawah ini, saya:

Nama : Rafiqa Oktaviani
NIM : 1305621034
Fakultas/Prodi : FMIPA / Matematika
Alamat email : rafiqa.oktaviani5@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPT Perpustakaan Universitas Negeri Jakarta, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah:

☑ Skripsi ☐ Tesis ☐ Disertasi ☐ Lain-lain (.....)

yang berjudul :

Kombinasi Vigènere Cipher, Algoritma RSA, dan ElGamal dalam Kriptografi Citra Digital beserta Analisis Keamanannya

Dengan Hak Bebas Royalti Non-Ekslusif ini UPT Perpustakaan Universitas Negeri Jakarta berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan Universitas Negeri Jakarta, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 8 Agustus 2025

Penulis

(Rafiqa Oktaviani)
nama dan tanda tangan

KATA PENGANTAR

Alhamdulillahi rabbil 'alamin. Puji syukur kehadirat Allah SWT yang telah memberikan rahmat serta nikmat-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul: **Kombinasi *Vigènere Cipher*, Algoritma RSA, dan ElGamal dalam Kriptografi Citra Digital beserta Analisis Keamanannya**. Skripsi ini disusun sebagai salah satu syarat dan tugas akhir memperoleh gelar Sarjana Matematika selama studi di Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta.

Penulis menyadari bahwa penulisan skripsi ini tidak akan selesai tanpa adanya dukungan, bantuan, dan bimbingan dari berbagai pihak. Pada kesempatan kali ini penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Dr. Yudi Mahatma, M.Si. selaku Koordinator Prodi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta.
2. Ibu Dr. Lukita Ambarwati, S.Pd., M.Si. selaku dosen pembimbing I dan Bapak Ibnu Hadi, M.Si. selaku dosen pembimbing II yang telah memberikan bimbingan, menjawab pertanyaan-pertanyaan, memberi masukan serta saran kepada penulis dalam penyusunan skripsi ini.
3. Bapak Ibu dosen yang telah memberikan ilmu yang sangat bermanfaat bagi penulis dalam menyelesaikan skripsi ini dan bekal untuk masa depan penulis.
4. Kedua orang tua serta keluarga penulis yang senantiasa memberikan doa, nasehat, serta semangat dalam menyelesaikan skripsi ini. Berkat doa dan ridhonya, Allah memberi berbagai kemudahan kepada penulis.

5. Seluruh teman-teman matematika 2021 dan semua pihak yang tidak mungkin untuk dicantumkan namanya satu-persatu, terima kasih banyak atas segala bentuk bantuan, semangat, dan dukungan bagi penulis.

Penulis menyadari bahwa masih terdapat kekurangan dan kesalahan dalam penulisan skripsi ini disebabkan kurangnya ilmu dan komunikasi. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun sehingga dapat menjadi lebih baik lagi.

Semoga skripsi ini dapat memberikan manfaat bagi lingkungan akademik khususnya Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta, maupun pihak lain yang membutuhkan serta bagi penulis secara pribadi.

Jakarta, 10 Juli 2025

Rafiqa Oktaviani

ABSTRAK

RAFIQA OKTAVIANI. Kombinasi *Vigènere Cipher*, Algoritma RSA, dan ElGamal dalam Kriptografi Citra Digital beserta Analisis Keamanannya. Skripsi, Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta. Juli 2025.

Kriptografi dapat digunakan sebagai upaya untuk mengamankan data, salah satunya data berupa citra digital. Sebagian besar sistem keamanan mengombinasikan algoritma kriptografi simetri dan nirsimetri dalam satu sistem, yaitu *hybrid cryptosystem* untuk meningkatkan keamanan. Algoritma kriptografi simetri memiliki kelebihan dalam kecepatan proses, namun lemah dalam keamanan kunci. Sebaliknya, algoritma kriptografi nirsimetri memiliki kelebihan dalam keamanan kunci, namun membutuhkan waktu pemrosesan yang lebih lama. Penelitian ini mengombinasikan tiga algoritma, yaitu *Vigènere Cipher* (simetri), *RSA* (nirsimetri), dan ElGamal (nirsimetri) pada citra digital. Keamanan kombinasi ini dianalisis berdasarkan nilai NPCR (*Number of Pixel Change Rate*) dan UACI (*Unified Average Changing Intensity*). Dari tiga algoritma tersebut, terdapat enam kombinasi yang dilakukan pada proses enkripsi dan dekripsi. Kombinasi algoritma tersebut akan diterapkan pada delapan citra dengan variasi warna serta kompleksitas gambar yang berbeda. Hasil penelitian menunjukkan bahwa rata-rata nilai NPCR dan UACI yang diperoleh dari delapan citra untuk masing-masing kombinasi algoritma kriptografi tersebut telah melewati batas minimal. Hal tersebut menunjukkan bahwa kombinasi kriptografi dapat dikatakan baik atau aman. Lebih lanjut, urutan penerapan antara algoritma simetri dan nirsimetri dalam kombinasi algoritma berpengaruh terhadap nilai UACI yang dihasilkan.

Kata kunci. *Kriptografi, Citra Digital, Algoritma Simetri, Algoritma Nirsimetri, NPCR, UACI*

ABSTRACT

RAFIQA OKTAVIANI. Combination of Vigènere Cipher, RSA Algorithm, and ElGamal in Digital Image Cryptography and Its Security Analysis. Mini Thesis, Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. July 2025.

Cryptography can be used as a means of securing data, one of which is data in the form of digital images. Most security systems combine symmetric and asymmetric cryptographic algorithms into one system, known as a hybrid cryptosystem, to enhance security. Symmetric cryptographic algorithms have the advantage of fast processing speed but are weaker in key security. Conversely, asymmetric cryptographic algorithms offer stronger key security but require more processing time. This paper discusses the combination of three algorithms i.e the Vigenère Cipher (symmetric), RSA (asymmetric), and ElGamal (asymmetric) using digital images. The security of these combinations is analyzed based on NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) values. From these three algorithms, six combinations are applied in the encryption and decryption processes. These algorithm combinations are implemented on eight images with varying colors and image complexity. The results show that the average NPCR and UACI values obtained from the eight images for each of the six algorithm combinations exceed the minimum threshold. This indicates that the cryptographic combinations can be considered secure. Furthermore, the order of applying symmetric and asymmetric algorithms in the combination affects the resulting UACI value.

Keyword. *Cryptography, Digital Image, Symmetric Algorithm, Asymmetric Algorithm, NPCR, UACI*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN