

**PERBANDINGAN KOMBINASI ALGORITMA AES DAN RSA
DENGAN AES DAN HMAC DALAM MENJAMIN KEASLIAN
DAN INTEGRITAS DATA PADA TRANSAKSI *MOBILE*
*BANKING***

Skripsi

Disusun untuk Memenuhi salah satu syarat
memperoleh gelar Sarjana Matematika



Intelligentia - Dignitas

Leni Marni
1305622001

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

2026

LEMBAR PERSETUJUAN HASIL SIDANG SKRIPSI
PERBANDINGAN KOMBINASI ALGORITMA AES DAN RSA DENGAN
AES DAN HMAC DALAM MENJAMIN KEASLIAN DAN INTEGRITAS
DATA PADA TRANSAKSI *MOBILE BANKING*

Nama : Leni Marni

NIM : 1305622001

Penanggung Jawab

Dekan : Dr. Hadi Nasbey, S.Pd., M.Si.
NIP. 197909162005011004

Nama



Tanda Tangan Tanggal

3/7-2026

Wakil Penanggung Jawab

Wakil Dekan I : Dr. Meiliasari, S.Pd., M.Sc.
NIP. 197905042009122002

3/7-2026

Ketua : Drs. Sudarwanto, M.Si., DEA.
NIP. 196503251993031003

30/6-2026

Penguji Ahli : Med Irzal, M.Kom.
NIP. 197706152003121001

30/6-2026

Sekretaris : Dr. Eti Dwi Wiraningsih, S.Pd., M.Si.
NIP. 198102032006042001

30/6-2026

Pembimbing I : Dr. Lukita Ambarwati, S.Pd., M.Si.
NIP. 197210262001122001

30/6-2026

Pembimbing II : Dr. Yudi Mahatma, M.Si.
NIP. 197610202008121001

1/7-2026

Dinyatakan lulus ujian skripsi pada tanggal : 10 Juni 2026

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 : Leni Marni
No Registrasi : 1305622001
Program Studi : Matematika

Dengan ini menyatakan bahwa skripsi yang saya buat dengan judul "*Perbandingan Kombinasi Algoritma AES dan RSA dengan AES dan HMAC Dalam Menjamin Keaslian dan Integritas Data pada Transaksi Mobile Banking*" 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, 18 Mei 2026



Leni Marni



KEMENTERIAN PENDIDIKAN TINGGI, SAINS DAN TEKNOLOGI
UNIVERSITAS NEGERI JAKARTA
PERPUSTAKAAN DAN KEARSIPAN

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 : Leni Marni
NIM : 1305622001
Fakultas/Prodi : Matematika & Ilmu Pengetahuan Alam / Matematika
Alamat email : lenimarni189@gmail.com

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

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

yang berjudul :

Perbandingan Kombinasi Algoritma AES dan RSA Dengan AES dan HMAC
Dalam menjamin Keaslian dan Integritas Data Pada Transaksi
Mobile Banking.

Dengan Hak Bebas Royalti Non-Eksklusif ini Perpustakaan dan Kearsipan 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 izin 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, 13 Juli 2026

Penulis


(Leni Marni)
nama dan tanda tangan

ABSTRAK

LENI MARNI. Perbandingan Kombinasi Algoritma AES dan RSA dengan AES dan HMAC dalam Menjamin Keaslian dan Integritas Data pada Transaksi Mobile Banking. Skripsi, Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta. Mei 2026.

Keamanan transaksi pada layanan *mobile banking* menjadi perhatian serius seiring meningkatnya kasus kejahatan siber, seperti serangan *Man-in-the-Middle* (MitM). Penelitian ini bertujuan untuk mengamankan data transaksi dari manipulasi serta serangan MitM, sekaligus membandingkan performa antara dua skema kriptografi hibrida, yaitu kombinasi AES dengan RSA dan AES dengan HMAC. Metode penelitian dilakukan dengan mengimplementasikan enkripsi data transaksi menggunakan AES-256. Pada kombinasi pertama, kunci enkripsi AES dilindungi kembali menggunakan RSA-2048 (*key wrapping*), sedangkan pada kombinasi kedua, *ciphertext* divalidasi menggunakan kode autentikasi pesan dari HMAC-SHA256.

Hasil pengujian menunjukkan bahwa kombinasi AES dan RSA memberikan perlindungan yang kuat terhadap aspek keaslian (*authenticity*) dan kerahasiaan (*confidentiality*) kunci karena proses pertukaran kunci. Di sisi lain, kombinasi AES dan HMAC menunjukkan keunggulan signifikan dalam menjaga integritas data transaksi melalui verifikasi nilai *tag* secara eksplisit. Berdasarkan uji performa terhadap 100 data transaksi keuangan, skema AES dan HMAC memiliki waktu komputasi yang lebih efisien dibandingkan AES dan RSA karena didominasi oleh operasi *bitwise* yang lebih ringan daripada eksponensial modular. Penelitian ini menyimpulkan bahwa skema AES dan HMAC lebih optimal untuk pemrosesan transaksi harian *mobile banking* yang membutuhkan responsivitas tinggi, sementara AES dan RSA tetap memegang peranan vital pada fase awal komunikasi (*handshake*) untuk menjamin keaslian distribusi kunci.

Kata Kunci: AES, HMAC, Integritas Data, Man-in-the-Middle (MitM), RSA.

Intelligentia - Dignitas

ABSTRACT

LENI MARNI. Comparison of AES-RSA and AES-HMAC Algorithm Combinations in Ensuring Authenticity and Data Integrity in Mobile Banking Transactions. Undergraduate Thesis, Mathematics Study Program, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. May 2026.

Transaction security in mobile banking services has become a critical concern due to the rising cases of cybercrimes, such as Man-in-the-Middle (MitM) attacks. This study aims to secure transaction data against manipulation and MitM attacks, while comparing the performance of two hybrid cryptographic schemes: the combination of AES with RSA and AES with HMAC. The research method was conducted by implementing transaction data encryption using AES-256. In the first combination, the AES encryption key is further protected using RSA-2048 (key wrapping), whereas in the second combination, the integrity of the ciphertext is validated using a message authentication code from HMAC-SHA256.

The experimental results indicate that the AES and RSA combination provides robust protection for the authenticity and confidentiality of the key because the key exchange process is performed asymmetrically. On the other hand, the AES-HMAC combination demonstrates a significant advantage in maintaining transaction data integrity through explicit tag value verification. Based on performance testing over 100 financial transaction data, the AES and HMAC scheme achieves a more efficient computation time compared to AES and RSA, as it is dominated by lightweight bitwise operations rather than heavy modular exponentiation. This study concludes that the AES and HMAC scheme is more optimal for daily mobile banking transaction processing that requires high responsiveness, while AES and RSA maintains a vital role in the initial communication phase (handshake) to ensure the authenticity of key distribution.

Keywords: *AES, Data Integrity, HMAC, Man-in-the-Middle (MitM), RSA.*

Intelligentia - Dignitas

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT (Tuhan Yang Maha Esa), atas segala rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi yang berjudul “Perbandingan Kombinasi Algoritma AES dan RSA dengan AES dan HMAC Dalam Menjamin Keaslian dan Integritas Data pada Transaksi *Mobile Banking*” ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Matematika pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta.

Penulis menyadari bahwa penyusunan skripsi ini tidak terlepas dari bimbingan, dukungan, serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih yang tulus kepada :

1. Ibu Dr. Lukita Ambarwati, S.Pd., M.Si. selaku Dosen Pembimbing I yang telah meluangkan waktu untuk memberikan bimbingan, arahan, motivasi, serta kesabaran dalam mengoreksi setiap detail penulisan hingga skripsi ini dapat diselesaikan.
2. Bapak Dr. Yudi Mahatma, M.Si. selaku Dosen Pembimbing II yang telah memberikan saran, kritik yang membangun, serta berbagai masukan berharga yang membantu penulis dalam menyempurnakan penelitian ini.
3. Bapak dan Ibu Dosen Program Studi Matematika FMIPA UNJ yang telah membekali penulis dengan berbagai ilmu pengetahuan selama masa perkuliahan, yang menjadi dasar kuat bagi penulis dalam menyelesaikan tugas akhir ini.
4. Kedua orang tua tercinta yang selalu menjadi sumber kekuatan utama bagi penulis. Terima kasih atas kasih sayang yang tak terhingga, doa yang tiada henti yang menjadi penyemangat penulis dalam setiap langkah perjuangan.
5. Abang dan kakak tercinta yang tidak pernah berhenti memberikan doa, kasih sayang, dukungan moral maupun material, motivasi, serta semangat kepada penulis dalam setiap proses perkuliahan hingga terselesaikannya skripsi ini.

6. Andi Tabina, Deby Febrianty, dan Grace Maria yang telah menjadi sahabat terbaik, tempat berbagi cerita, serta selalu memberikan semangat, motivasi, dan bantuan kepada penulis selama menjalani perkuliahan hingga penyusunan skripsi ini.

7. Lucyana Fariska dan Rahmat Teguh Nazar yang senantiasa memberikan dukungan, semangat, serta bantuan kepada penulis selama proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari pembaca demi kesempurnaan di masa yang akan datang. Akhir kata, semoga skripsi ini dapat memberikan manfaat bagi perkembangan ilmu pengetahuan, khususnya di bidang kriptografi dan keamanan informasi.

Jakarta, 18 Mei 2026

Leni Marni

Intelligentia - Dignitas

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
BAB 2 KAJIAN PUSTAKA	7
2.1 Kriptografi	7
2.1.1 Kriptografi Klasik	8
2.1.2 Kriptografi Modern	9
2.1.2.1 Kriptografi Simetris	9

2.1.2.2	Kriptografi Asimetris	10
2.1.2.3	Kriptografi Hibrida	11
2.1.2.4	Hashing	12
2.2	Keamanan Informasi dan Penerapannya dalam Mobile Banking	14
2.2.1	Integritas Data	17
2.2.2	Keaslian Data	19
2.3	Ancaman pada Transaksi Mobile Banking	22
2.4	Operasi Matematis	23
2.4.1	Aritmatika Modulo	23
2.4.1.1	Eksponen Modular	24
2.4.1.2	Eksponsiasi Modular Cepat	25
2.4.2	Matriks	27
2.4.2.1	Matriks 4×4 dalam AES	27
2.4.2.2	Langkah AES dan Hubungannya dengan Matriks 4×4	28
2.4.3	Faktorisasi	28
2.4.3.1	Fungsi Totient Euler ($\varphi(n)$)	29
2.4.3.2	Invers Modular dan Algoritma <i>Euclidean Extended</i>	29
2.4.3.3	Dampak Faktorisasi pada Keamanan RSA	30
2.4.4	Bilangan Biner	32
2.4.5	Aritmatika Polinom di Medan Galois	33
2.4.5.1	Perkalian dalam $GF(2^8)$ di AES	36
2.4.6	Operasi Bitwise XOR	38
2.4.7	Bilangan Prima	40
2.5	AES (<i>Advanced Encryption Standard</i>)	42
2.5.1	Mode Operasi <i>Cipher Block Chaining</i> (CBC) dan Mekanisme Blok	43
2.5.2	Derivasi kunci (<i>Key Derivation</i>)	44
2.5.3	Enkripsi AES	45
2.5.4	Dekripsi AES-256	54
2.6	RSA (Rivest-Shamir-Adleman)	60

2.6.1	Pembangkitan Kunci RSA	61
2.6.2	Enkripsi RSA	62
2.6.3	Dekripsi (<i>Unwrapping</i>) Kunci AES	64
2.7	HMAC (<i>Hash-based Message Authentication Code</i>)	66
2.7.1	Derivasi Kunci HMAC	66
2.7.2	Perhitungan Algoritma HMAC	67
2.7.3	Algoritma Fungsi Hash SHA-256	68
2.8	Kombinasi Algoritma Keamanan Data Transaksi Perbankan . .	77
2.8.1	Alur Kombinasi AES-RSA pada Transaksi Mobile Banking	77
2.8.1.1	Alur Kombinasi AES-HMAC pada Transaksi Mobile Banking	78
2.9	Teori Kompleksitas Algoritma (Notasi Big-O)	79
2.10	Serangan <i>Man in the Middle</i> (MITM)	84
2.10.1	Contoh Serangan <i>Man-in-the-Middle</i> (MITM) pada Mobile Banking	85
2.10.2	Perhitungan Keberhasilan Serangan MitM	87
BAB 3	METODOLOGI PENELITIAN	92
3.1	Jenis Data	92
3.2	Sumber Data	92
3.3	Teknik Pengumpulan Data	93
3.4	Teknik Analisis Data	94
3.4.1	Lingkungan Pengujian	98
3.4.2	Analisis Kinerja	98
3.4.3	Keamanan	98
3.5	Diagram Alir Penelitian	99
BAB 4	HASIL DAN PEMBAHASAN	100
4.1	Prapemrosesan Data	100
4.1.1	Konversi ke Format ASCII	100
4.1.2	Konversi ke Format Heksadesimal	101
4.1.3	Implementasi <i>Padding</i>	101

4.1.4	Pembentukan Matriks <i>State</i> (4×4)	102
4.2	Implementasi AES-256	102
4.2.1	Ekspansi Kunci AES-256	103
4.2.2	Proses Enkripsi	105
4.2.3	Proses Dekripsi	108
4.2.4	Implementasi Menggunakan Python	112
4.3	Implementasi Kombinasi Algoritma AES-RSA (<i>Key Wrapping</i>)	113
4.3.1	Pembangkitan Kunci RSA (<i>Key Generation</i>)	114
4.3.2	Dekripsi RSA (<i>Key Unwrapping</i>)	115
4.3.3	Implementasi Menggunakan Python	118
4.4	Implementasi Kombinasi Algoritma AES-HMAC	120
4.4.1	Pembentukan Kunci Internal dengan <i>Inner Padding</i> (ipad)	120
4.4.2	<i>Inner Hashing</i> (Lapisan Dalam)	122
4.4.3	Pembentukan Kunci Eksternal dengan <i>Outer Padding</i> (opad)	126
4.4.4	Finalisasi Melalui <i>Outer Hashing</i> (Lapisan Luar)	127
4.4.5	Implementasi Menggunakan Python	131
4.5	Hasil Uji Kompleksitas Algoritma	135
4.6	Hasil Uji MITM	136
4.6.1	Hasil Uji Waktu	136
4.6.2	Hasil Uji MITM untuk Integritas dan keaslian	140
4.7	Waktu Komputasi	142
4.7.1	Kombinasi Algoritma AES dan RSA	142
4.7.2	Kombinasi Algoritma AES dan HMAC	143
4.8	Perbandingan Optimalitas	144
4.8.1	Analisis Keunggulan Metode AES-RSA	144
4.8.2	Analisis Keunggulan Metode AES-HMAC	145
4.8.3	Kesimpulan Optimalitas	145
BAB 5	PENUTUP	147
5.1	Kesimpulan	147
5.2	Saran	148

DAFTAR PUSTAKA

149

LAMPIRAN

154

RIWAYAT HIDUP

156



Intelligentia - Dignitas

DAFTAR TABEL

Tabel 2.1	Nilai Konstanta <i>Round Constant</i> (Rcon) pada AES	47
Tabel 2.2	Langkah Enkripsi RSA	64
Tabel 2.3	Langkah Dekripsi RSA $3037^{2753} \bmod 3233$	65
Tabel 3.1	Data Transaksi	95
Tabel 4.1	Hasil Konversi Karakter ke Nilai Desimal ASCII	100
Tabel 4.2	Hasil Konversi Nilai Desimal ke Format Heksadesimal . .	101
Tabel 4.3	Hasil Penerapan <i>Padding</i> PKCS#7 pada Kolom Amount .	102
Tabel 4.4	Ringkasan Output Tiap Ronde Enkripsi	107
Tabel 4.5	Output Tiap Ronde Dekripsi (AES-256)	110
Tabel 4.6	Perhitungan RSA <i>Wrapping</i> Kunci AES-256	115
Tabel 4.7	Perhitungan RSA <i>Unwrapping</i> Kunci AES-256	118
Tabel 4.8	Hasil Pengujian Enkripsi AES-256 dan RSA <i>Wrapping</i> . .	119
Tabel 4.9	Detail Perhitungan Bitwise XOR Inner Pad (S_{in})	121
Tabel 4.10	Nilai Variabel Kerja Setelah Round 16	125
Tabel 4.11	Detail Perhitungan <i>Bitwise XOR Outer Pad</i> (S_{out})	126
Tabel 4.12	Nilai Variabel Kerja Tahap Outer Setelah Round 16	130
Tabel 4.13	Tahap Inner Hashing	131
Tabel 4.14	Tahap Outer Hashing	133
Tabel 4.15	HMAC Tag	135
Tabel 4.16	Perbandingan Kinerja Algoritma (N=300)	135
Tabel 4.17	Waktu Komputasi AES dan RSA (ms)	142
Tabel 4.18	Waktu Komputasi AES dan RSA (ms)	143
Tabel 4.19	Perbandingan Kinerja Kombinasi Algoritma	144

DAFTAR GAMBAR

Gambar 2.1	Enkripsi Simetris	10
Gambar 2.2	Enkripsi Asimetris	11
Gambar 2.3	Enkripsi Hibrida	12
Gambar 2.4	Enkripsi Hashing	14
Gambar 2.5	Alur Simulasi Serangan MITM	84
Gambar 3.1	Hasil Perbandingan Uji Keaslian dan Integritas	99
Gambar 4.1	Hasil Ekspansi Kunci	112
Gambar 4.2	Hasil Enkripsi AES	112
Gambar 4.3	Hasil Dekripsi AES	113
Gambar 4.4	Hasil <i>Inner Hashing</i>	132
Gambar 4.5	Hasil Outer Hashing	134
Gambar 4.6	Uji Waktu	138
Gambar 4.7	Uji Waktu	140
Gambar 4.8	Uji MITM untuk kombinasi AES dan RSA	140
Gambar 4.9	Uji MITM Pada Kombinasi Algoritma AES dan HMAC	141

Intelligentia - Dignitas