# 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

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**

| | | Nama | Tanda Tangan | Tanggal |
|---|---|---|---|---|
| **Penanggung Jawab** | | | | |
| Dekan | : | Dr. Hadi Nasbey, S.Pd., M.Si.<br>NIP. 197909162005011004 | | 3/7-2026 |
| **Wakil Penanggung Jawab** | | | | |
| Wakil Dekan I | : | Dr. Meiliasari, S.Pd., M.Sc.<br>NIP. 197905042009122002 | | 3/7-2026 |
| Ketua | : | Drs. Sudarwanto, M.Si., DEA.<br>NIP. 196503251993031003 | | 30/6-2026 |
| Penguji Ahli | : | Med Irzal, M.Kom.<br>NIP. 197706152003121001 | | 30/6-2026 |
| Sekretaris | : | Dr. Eti Dwi Wiraningsih, S.Pd., M.Si.<br>NIP. 198102032006042001 | | 30/6-2026 |
| Pembimbing I | : | Dr. Lukita Ambarwati, S.Pd., M.Si.<br>NIP. 197210262001122001 | | 30/6-2026 |
| Pembimbing II | : | Dr. Yudi Mahatma, M.Si.<br>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-Ekslusif 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 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, 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.*

# 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.*

# 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**

# DAFTAR ISI

# DAFTAR TABEL

# DAFTAR GAMBAR