IMPLEMENTASI ENKRIPSI DATA TRANSAKSI KREDIT DENGAN KOMBINASI ALGORITMA RSA DAN AES 256 (Studi Kasus: PT. KAMPUNG MARKETERINDO BERDAYA)

LAPORAN TUGAS AKHIR

NIZAR NAUFAL

41519120083

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2025

IMPLEMENTASI ENKRIPSI DATA TRANSAKSI KREDIT DENGAN KOMBINASI ALGORITMA RSA DAN AES 256 (Studi Kasus: PT. KAMPUNG MARKETERINDO BERDAYA)

LAPORAN TUGAS AKHIR

NIZAR NAUFAL

41519120083

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2025

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama	: Nizar Naufal
NIM	: 41519120083
Program Studi	: Teknik Informatika
Judul Laporan Skripsi	: Implementasi Enkripsi Data Transaksi Kredit Dengan Kombinasi Algoritma RSA dan AES 256

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 19 Juli 2025

Nizar Naufal

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh:

Nama	:	Nizar Naufal
NIM	:	41519120083
Program Studi	:	Teknik Informatika
Judul Laporan Skripsi	:	Implementasi Enkripsi Data Transaksi Kredit Dengan Kombinasi Algoritma RSA dan AES 256 (Studi Kasus : PT. Kampung Marketerindo Berdaya)

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing	: Lukman Hakim, S.T., M.Kom	( )
NIDN	: 0327107701	
Ketua Penguji	: Dr. Hadi Santoso, S.Kom, M.Kom	( )
NIDN	: 0225067701	
Penguji 1	: Siti Maesaroh, S.Kom., M.TI	( )
NIDN	: 0413059003	
Penguji 2	: Roy Mubarak, S.T., M.Kom	( )
NIDN	: 0310027402	

Jakarta, 25 July 2025

Mengetahui,

Dekan	Ketua Program Studi
Dr. Bambang Jokonowo, S.Si., MTI	Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0320037002	NIDN : 0225067701

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT, Tuhan yang Maha Esa, Karena atas berkat dan Rahmat-nya, Saya dapat menyelesaikan Laporan Skripsi Ini.

Penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Oleh karena itu, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Bapak Lukman Hakim, S.T., M.Kom. selaku dosen pembimbing tugas akhir yang telah menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan tugas akhir ini terjadwal dengan baik.
5. Ayu Untari Yudha Putri selaku istri penulis yang telah memberikan semangat dukungan dan doa dalam melakukan penyusunan skripsi.
6. Bapak Satriyo Budi Utomo selaku CTO & Co-Founder Divisi Area PT Kampung Marketerindo Berdaya yang telah memberikan izin kepada saya dalam melakukan sebuah penelitian ini.
7. Serta Rekan-Rekan PT. Kampung Marketerindo Berdaya yang tidak dapat diberikan Namanya satu persatu

Akhir kata, Saya berharap Allah SWT, Tuhan Yang Maha Esa Berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Laporan Skripsi ini membawa manfaat bagi pengembangan ilmu

Jakarta, 19 Juli 2025

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama	:	Nizar Naufal
NIM	:	41519120083
Program Studi	:	Teknik Informatika
Judul Laporan Skripsi	:	Implementasi Enkripsi Data Transaksi Kredit Dengan Kombinasi Algoritma RSA dan AES 256 (Studi Kasus: PT Kampung Marketerindo Berdaya)

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).
Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/ Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 19 Juli 2025
Yang menyatakan,

Nizar Naufal

ABSTRAK

Nama	:	Nizar Naufal
NIM	:	41519120083
Program Studi	:	Teknik Informatika
Judul Proposal Penelitian	:	Implementasi Enkripsi Data Transaksi Kredit Dengan Kombinasi Algoritma RSA Dan AES 256 (Studi Kasus: PT. Kampung Marketerindo Berdaya)
Pembimbing	:	Lukman Hakim, S.T., M.Kom.

Keamanan data menjadi salah satu prioritas utama di era digital, terutama di industri keuangan yang memiliki risiko tinggi terhadap ancaman siber seperti pencurian data, peretasan, dan akses tidak sah. PT.Kampung Marketerindo Berdaya sebagai perusahaan yang bergerak di sektor pembiayaan membutuhkan sistem keamanan yang mampu melindungi data transaksi kredit agar tetap aman dan terjaga kerahasiaannya. Dengan semakin kompleksnya ancaman keamanan siber, diperlukan metode enkripsi data yang kuat dan andal untuk menjaga integritas serta kerahasiaan informasi transaksi. Penelitian ini bertujuan untuk mengimplementasikan enkripsi data transaksi kredit menggunakan kombinasi algoritma RSA dan AES 256, yang diharapkan dapat memberikan lapisan keamanan tambahan serta meminimalkan risiko penyusupan pada sistem.

Pada penelitian ini, algoritma RSA digunakan sebagai enkripsi kunci dan AES 256 diterapkan untuk enkripsi data transaksi. RSA dikenal sebagai algoritma kriptografi asimetris yang memungkinkan enkripsi dan dekripsi kunci secara aman, sedangkan AES 256 adalah algoritma simetris yang efektif untuk enkripsi data berkecepatan tinggi dengan tingkat keamanan yang sangat tinggi. Kombinasi RSA dan AES 256 ini dipilih untuk memanfaatkan keunggulan masing-masing algoritma, di mana RSA memberikan keamanan kunci yang lebih kuat, sementara AES 256 menawarkan efisiensi tinggi dalam pengamanan data transaksi.

Proses penelitian dilakukan dengan mengimplementasikan sistem enkripsi pada simulasi transaksi kredit, di mana data terenkripsi dan didekripsi untuk menguji keandalan serta performanya dalam kondisi real-time. Pengujian ini melibatkan analisis waktu proses enkripsi-dekripsi, ukuran data setelah enkripsi, dan tingkat keamanan terhadap berbagai jenis ancaman. Analisis kinerja dilakukan untuk memastikan bahwa kombinasi algoritma RSA dan AES 256 mampu beroperasi dengan efisien tanpa menghambat proses transaksi. Pengujian keamanan juga dilakukan untuk menilai ketahanan sistem terhadap upaya peretasan, memastikan bahwa akses tidak sah dapat diminimalisir.

Hasil dari penelitian ini menunjukkan bahwa kombinasi RSA dan AES 256 mampu meningkatkan keamanan data transaksi secara signifikan. Sistem yang dikembangkan dapat melindungi data transaksi dari akses tidak sah dengan efektif, serta memungkinkan manajemen kunci yang aman. Kinerja sistem enkripsi ini berada pada kisaran waktu yang dapat diterima untuk transaksi kredit secara real-time, menjadikannya cocok untuk diterapkan dalam industri keuangan. Penelitian ini juga merekomendasikan optimalisasi lebih lanjut untuk meningkatkan efisiensi

algoritma, serta pengembangan sistem keamanan berbasis enkripsi kombinasi ini pada skala yang lebih besar.

Secara keseluruhan, implementasi kombinasi algoritma RSA dan AES 256 pada data transaksi kredit di PT. Kampung Marketerindo Berdaya terbukti memberikan perlindungan data yang kuat dan efektif, serta menjadi solusi yang potensial untuk menghadapi berbagai ancaman siber di masa depan.

Kata Kunci: Enkripsi Data, RSA, AES 256, Keamanan Transaksi,

ABSTRACT

Name	:	Nizar Naufal
NIM	:	41519120083
Study Program	:	Informatics Engineering
Title Thesis	:	Implementation of Credit Transaction Data Encryption Using a Combination of RSA and AES 256 Algorithms (Case Study: PT. Kampung Marketerindo Berdaya)
Counsellor	:	Lukman Hakim, S.T., M.Kom.

In the digital era, data security is a top priority, especially in the financial industry, which faces high risks from cyber threats like data theft, hacking, and unauthorized access. PT. Kampung Marketerindo Berdaya, as a company operating in the finance sector, requires a security system capable of protecting credit transaction data to ensure its safety and confidentiality. Given the increasing complexity of cyber threats, a robust and reliable data encryption method is essential to maintain the integrity and confidentiality of transaction information. This study aims to implement credit transaction data encryption using a combination of RSA and AES 256 algorithms, expected to provide an additional layer of security and minimize intrusion risks.

In this research, the RSA algorithm is utilized for key encryption, while AES 256 is applied for transaction data encryption. RSA is known as an asymmetric cryptographic algorithm that allows secure encryption and decryption of keys, while AES 256 is a symmetric algorithm that is efficient for high-speed data encryption with a high level of security. This combination of RSA and AES 256 leverages the advantages of each algorithm, with RSA providing stronger key security and AES 256 offering high efficiency in securing transaction data.

The research process involves implementing the encryption system on a credit transaction simulation, where encrypted and decrypted data are tested for reliability and performance under real-time conditions. Testing includes analyzing encryption-decryption processing time, data size after encryption, and security level against various types of threats. Performance analysis ensures that the combination of RSA and AES 256 can operate efficiently without hindering transaction processes. Security testing evaluates the system's resilience against hacking attempts, ensuring that unauthorized access can be minimized.

The results of this study show that the RSA and AES 256 combination significantly enhances transaction data security. The developed system effectively protects transaction data from unauthorized access while enabling secure key management. The encryption system's performance is within an acceptable range for real-time credit transactions, making it suitable for financial industry applications. This study also recommends further optimization to improve algorithm efficiency, as well as the potential development of this combined encryption-based security system on a larger scale.

Overall, the implementation of the RSA and AES 256 algorithm combination on credit transaction data at PT. Kampung Marketerindo Berdaya has proven to

provide strong and effective data protection, making it a viable solution for countering various cyber threats in the future.
Keywords: Data Encryption, RSA, AES 256, Transaction Security

DAFTAR ISI

HALAMAN JUDUL ..... **i**
HALAMAN PERNYATAAN ..... **ii**
HALAMAN PENGESAHAN ..... **iii**
KATA PENGANTAR ..... **iv**
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI ..... **v**
ABSTRAK ..... **vi**
ABSTRACT ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR TABEL ..... **xii**
DAFTAR GAMBAR ..... **xiii**
DAFTAR LAMPIRAN ..... **xiv**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Perumusan Masalah 4
1.3 Tujuan Penelitian 4
1.4 Manfaat Penelitian 4
1.5 Batasan Masalah 5
BAB II TINJAUAN PUSTAKA **7**
2.1 Penelitian Terlebih Dahulu 7
2.1.1 Gap Penelitian 30
2.2 Teori Pendukung 32
2.2.1 PT. Kampung Marketerindo Berdaya 32
2.2.2 Kriptografi 33
2.2.3 Algoritma Advanced Encryption Standard (AES) 36
2.2.4 Shared Preferences 40
2.2.5 Jadx 41
2.2.6 Android Studio 43
2.2.7 Java Development Kit 45
BAB III METODE PENELITIAN **47**
3.1 Jenis Penlitian 47

3.2 Tahapan Penelitian 48
3.2.1 Pendekatan Penelitian 48
3.2.2 Desain Penelitian 50
3.2.3 Subject Penelitian 50
3.2.4 Instrument Penelitian 50
3.2.5 Teknik Pengumpulan Data 54
3.2.6 Analisis Data 56
3.2.7 Prosedur Penelitian 59
3.2.8 Evaluasi Hasil Penelitian 62
3.2.9 Alur Penelitian 65
BAB IV HASIL DAN PEMBAHASAN 67
4.1 Perbandingan Hasil Metode 67
4.2 Dataset 68
4.2.1 Perangkat Lunak (Software) 68
4.2.2 Perangkat Keras (Hardware) 68
4.2.3 Tools 69
4.2.4 Element Terhadap Dataset 69
4.3 Analisis 71
4.3.1 Konfigurasi Dasar Gradle 71
4.3.2 Konfigurasi Dasar dan Implementasi Crypto Helper 72
4.3.3 Konfigurasi Dasar dan Mapping Card Payload 75
4.3.4 Konfigurasi Dasar Pada Room Database 76
4.3.5 Konfigurasi Dasar dan Implementasi Layout 80
4.3.6 Logcat Output 81
BAB V KESIMPULAN DAN SARAN 85
5.1 Kesimpulan 85
5.2 Saran 86
DAFTAR PUSTAKA 88
LAMPIRAN 91

DAFTAR TABEL

Tabel 2.1 Review Jurnal 1 7
Tabel 2.2 Review Jurnal 2 9
Tabel 2.3 Review Jurnal 3 11
Tabel 2.4 Review Jurnal 4 12
Tabel 2.5 Review Jurnal 5 15
Tabel 2.6 Review Jurnal 6 16
Tabel 2.7 Review Jurnal 7 18
Tabel 2.8 Review Jurnal 8 19
Tabel 2.9 Review Jurnal 9 21
Tabel 2.10 Review Jurnal 10 22
Tabel 2.11 Review Jurnal 11 24
Tabel 2.12 Review Jurnal 12 25
Tabel 2.13 Review Jurnal 13 27
Tabel 2.14 Review Jurnal 14 28
Tabel 2.15 Review Jurnal 15 30
Tabel 2.16 Review Jurnal 16 31
Tabel 2.17 Review Jurnal 17 32
Tabel 2.18 Review Jurnal 18 34
Tabel 2.19 Review Jurnal 19 35
Tabel 2.20 Review Jurnal 20 36
Tabel 2.21 Jumlah proses berdasarkan block bit dan kunci 44

Tabel 3.1 Tahap Identifikasi Kebutuhan Keamanan 65
Tabel 3.2 Tahap Perancangan Sistem Enkripsi 65
Tabel 3.3 Tahap Implementasi Enkripsi RSA dan AES 66
Tabel 3.4 Pengujian Keamanan dan Kinerja 67
Tabel 3.5 Proses Analisis Data Pengujian 67
Tabel 3.6 Evaluasi dan Pemeliharaan 68

Tabel 4.1 Tabel Peralatan Simulasi 78
Tabel 4.2 Pengukuran Kinerja Jaringan 78
Tabel 4.3 Konfigurasi Sistem 79
Tabel 4.4 Laporan Simulasi Penelitian 80
Tabel 4.5 Logs Database Cards `91
Tabel 4.6 Logs Database Transaction 92

DAFTAR GAMBAR

Gambar 2.1 PT.Kampung Marketerindo Berdaya 41
Gambar 2.2 Skema Enkripsi dan Dekripsi (Zuli dan Irawan, 2017: 5) 44
Gambar 2.3 Flowchart Enkripsi AES 47
Gambar 2.4 Flowchart Dekripsi AES 48
Gambar 2.5 Cara Kerja Shared Preferences 49
Gambar 2.6 Cara Kerja JADX 51
Gambar 2.7 Cara Kerja Android Studio 53

Gambar 3.1 Desain Penelitian 58
Gambar 3.2 Alur/Flowchart Penelitian 74

Gambar 4.1 Konfigurasi Gradle Dependencies 81
Gambar 4.2 Konfigurasi Get Or Create Key 87
Gambar 4.3 Konfigurasi Encrypt 88
Gambar 4.4 Konfigurasi Decrypt 89
Gambar 4.5 Konfigurasi Dan Mapping Card Payload 90
Gambar 4.6 Konfigurasi Dasar Pada Room Database Cards 91
Gambar 4.7 Konfigurasi Dasar Pada Room Database Transaction 92
Gambar 4.8 Konfigurasi Layout 95
Gambar 4.9 Logcat Output 96

DAFTAR LAMPIRAN

Lampiran 1 Bimbingan Skripsi 94
Lampiran 2 Bimbingan Skripsi 94
Lampiran 3 Bimbingan Skripsi 95
Lampiran 4 Lampiran Pendaftaran BNSP 95
Lampiran 5 Lampiran Bukti Uji Kompetisi BNSP 95
Lampiran 6 Surat Keterangan LSP Mercubuana 96
Lampiran 7 Lampiran Observasi Dan Wawancara Dengan Team PT. Kampung Marketerindo Berdaya 96
Lampiran 8 Proses Review Jurnal 96
Lampiran 9 Bukti Submission Jurnal 96
Lampiran 10 Naskah Artikel Jurnal 96
Lampiran 11 Naskah Artikel Jurnal 96
Lampiran 12 Naskah Artikel Jurnal 96
Lampiran 13 Naskah Artikel Jurnal 97
Lampiran 14 Hasil Turnitin Atau Parafrase Oleh TU Fasilkom 97
Lampiran 15 Curriculum Vitae 98
Lampiran 16 Halaman Persetujuan Laporan Tugas Akhir 98
Lampiran 17 Kartu Atensi TA Mahasiswa 98
Lampiran 18 Surat Pernyataan HAKI 99
Lampiran 19 Surat Pernyataan HAKI 99
Lampiran 20 Lampiran Halaman Pernyataan Luaran Tugas Akhir 99
Lampiran 21 Surat Izin Riset Kepada PT. Kampung Marketerindo Berdaya 99
Lampiran 22 Form Revisi Dosen Penguji 1 100
Lampiran 23 Form Revisi Dosen Penguji 2 100