Journal of Scientech Research and Development
Volume 7, Issue 1, June 2025
P-ISSN: 2715-6974 E-ISSN: 2715-5846
Open Access at: http://idm.or.id/JSCR

ANALISIS PERBANDINGAN KINERJA METODE KRIPTOGRAFI AES DAN RSA SEBAGAI REKOMENDASI UNTUK KEAMANAN DATA TRANSAKSI PADA APLIKASI E-COMMERCE UMKM

ANALISIS PERBANDINGAN KINERJA METODE *KRIPTOGRAFI AES* DAN *RSA* SEBAGAI REKOMENDASI UNTUK KEAMANAN DATA TRANSAKSI PADA APLIKASI *E-COMMERCE* UMKM

Depo Sadrila Hadi[1], Rahman Ajie[2], Tata Sutabri[3]
Program Studi Teknik Informatika, Fakultas Sains Teknologi, Universitas Bina Darma
E-mail: dxdeposh@gmail.com[1], aji313839@gmail.com[2], tata.sutabri@gmail.com[3]

ARTICLE INFO

Correspondent:

Depo Sadrila Hadi
dxdeposh@gmail.com

Key words:
cryptography, AES, RSA, data security, E-Commerce, MSMEs, performance analysis, recommendation

Website:
https://idm.or.id/JSCR/index.php/JSCR

***Page:* 930 - 937**

ABSTRACT

The development of e-commerce provides significant opportunities for Micro, Small, and Medium Enterprises (MSMEs) to expand their markets. However, transaction data security is a crucial issue that often becomes an obstacle for MSMEs due to limited resources. Cryptography offers solutions to protect such sensitive data. This research aims to analyze the performance comparison of two popular cryptographic algorithms: Advanced Encryption Standard (AES), a symmetric algorithm, and Rivest-Shamir-Adleman (RSA), an asymmetric algorithm. The analysis focuses on the speed of encryption and decryption processes across various transaction data sizes commonly found in MSME e-commerce applications. The research method used is experimental with implementations of AES-128 (CBC mode) and RSA-2048 on the Python platform. Tests were conducted on sample transaction data sizes of 1KB, 10KB, 100KB, 1MB, and 5MB. The results consistently show that AES performs significantly faster in data encryption and decryption processes compared to RSA. For narrative instance, for 1MB of data, AES required an average of 108.70 milliseconds for encryption, while RSA required a significantly longer time of 21560.20 milliseconds. This difference widens as data size increases. Based on these findings, this study recommends the use of AES for actual transaction data encryption in MSME e-commerce due to its efficiency. For AES key management, RSA remains relevant in a hybrid scheme to ensure session key security.

INFO ARTIKEL

Koresponden

Depo Sadrila Hadi
dxdeposh@gmail.com

Kata kunci:
kriptografi, AES, RSA, keamanan data, E-*Commerce*, UMKM, analisis kinerja, rekomendasi

Website:
https://idm.or.id/JSCR/index.php/JSCR

Hal: 930 - 937

ABSTRAK

PPerkembangan e-commerce memberikan peluang besar bagi Usaha Mikro, Kecil, dan Menengah (UMKM) untuk memperluas pasar. Namun, keamanan data transaksi menjadi isu krusial yang seringkali menjadi kendala bagi UMKM karena keterbatasan sumber daya. Kriptografi menawarkan solusi untuk melindungi data sensitif tersebut. Penelitian ini bertujuan untuk menganalisis perbandingan kinerja dua algoritma kriptografi populer, yaitu *Advanced Encryption Standard* (AES) yang merupakan algoritma simetris, dan *Rivest-Shamir-Adleman* (RSA) yang merupakan algoritma asimetris. Fokus analisis adalah pada kecepatan proses enkripsi dan dekripsi terhadap berbagai ukuran data transaksi yang umum dijumpai pada aplikasi e-commerce UMKM. Metode penelitian yang digunakan adalah eksperimental dengan implementasi algoritma AES-128 (mode CBC) dan RSA-2048 pada platform Python. Pengujian dilakukan terhadap sampel data transaksi berukuran 1KB, 10KB, 100KB, 1MB, dan 5MB. Hasil penelitian menunjukkan bahwa AES secara konsisten memiliki kinerja yang jauh lebih cepat dalam proses enkripsi dan dekripsi data dibandingkan RSA. Sebagai contoh naratif, untuk data 1MB, AES membutuhkan rata-rata 108.70 milidetik untuk enkripsi, sementara RSA membutuhkan waktu yang jauh lebih signifikan, yaitu 21560.20 milidetik. Perbedaan ini semakin melebar seiring dengan peningkatan ukuran data. Berdasarkan temuan tersebut, penelitian ini merekomendasikan penggunaan AES untuk enkripsi data transaksi aktual pada e-commerce UMKM karena efisiensinya. Untuk manajemen kunci AES, penggunaan RSA tetap relevan dalam skema hybrid guna menjaga keamanan kunci sesi

PENDAHULUAN

Usaha Mikro, Kecil, dan Menengah (UMKM) merupakan pilar penting dalam struktur perekonomian Indonesia, berkontribusi signifikan terhadap Produk Domestik Bruto (PDB) dan penyerapan tenaga kerja (Stallings, 2020). Era digitalisasi, khususnya melalui adopsi platform e-commerce, telah membuka peluang ekspansi pasar yang belum pernah ada sebelumnya bagi UMKM (Menezes, *et al.*, 1996). Meskipun demikian, peningkatan aktivitas transaksi online juga membawa serta risiko keamanan data yang lebih tinggi. Data sensitif seperti informasi pribadi pelanggan, detail pembayaran, dan riwayat transaksi menjadi target menarik bagi pelaku kejahatan siber (Schneier, 1996).

Implementasi sistem keamanan siber yang tangguh seringkali menjadi tantangan bagi UMKM, mengingat adanya keterbatasan sumber daya finansial, teknis, dan sumber daya manusia yang kompeten di bidang keamanan informasi (National Institute of Standards and Technology, 2001). Padahal, insiden keamanan data dapat berakibat fatal, mulai dari kerugian finansial langsung, kerusakan reputasi, hingga hilangnya kepercayaan pelanggan. Dalam konteks ini, kriptografi hadir sebagai salah satu teknologi fundamental untuk melindungi data (Daemen & Rijmen, 2002). Dengan menerapkan teknik enkripsi, data dapat diubah menjadi format yang tidak dapat dipahami oleh pihak yang tidak berwenang, sehingga kerahasiaannya terjaga.

Secara umum, algoritma kriptografi terbagi menjadi dua kategori utama: simetris dan asimetris. Algoritma simetris, seperti *Advanced Encryption Standard* (AES), menggunakan kunci tunggal untuk proses enkripsi dan dekripsi, dan dikenal karena efisiensi komputasinya, terutama untuk data dalam volume besar (Rivest *et al*., 1978). Sebaliknya, algoritma asimetris, seperti *Rivest-Shamir-Adleman* (RSA), menggunakan sepasang kunci (kunci publik dan kunci privat), yang menawarkan mekanisme manajemen kunci dan autentikasi yang lebih fleksibel, meskipun cenderung lebih lambat dalam pemrosesan data massal (Munir, 2019); (Arif & Norokhman (2023). Keamanan RSA didasarkan pada kesulitan matematis dalam memfaktorkan bilangan prima yang sangat besar.

Mengingat perbedaan fundamental ini, pemilihan strategi kriptografi yang tepat untuk aplikasi *e-commerce* yang digunakan oleh UMKM memerlukan pertimbangan matang antara tingkat keamanan yang diinginkan dan dampak kinerja terhadap sistem. Penelitian ini bertujuan untuk melakukan analisis perbandingan kinerja antara algoritma AES dan RSA dalam skenario pengamanan data transaksi e-commerce. Aspek kinerja yang menjadi fokus utama adalah kecepatan proses enkripsi dan dekripsi pada berbagai ukuran data. Hasil dari analisis ini diharapkan dapat memberikan landasan rekomendasi yang kuat bagi UMKM dan pengembang aplikasi dalam merancang sistem keamanan data yang efektif dan efisien.

METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kuantitatif dengan desain eksperimental. Tujuan utama adalah untuk mengevaluasi dan membandingkan kinerja algoritma kriptografi AES dan RSA berdasarkan kecepatan proses enkripsi dan dekripsi data transaksi simulasi.

Konfigurasi Lingkungan Eksperimen

Seluruh pengujian dilakukan pada satu sistem komputer dengan spesifikasi sebagai berikut:

- Perangkat Keras: Unit Pengolah Pusat (CPU) Intel Core i7 Generasi ke-10 (10750H) dengan kecepatan dasar 2.60GHz, Memori Akses Acak (RAM) 16 GB jenis DDR4, dan Penyimpanan Solid State Drive (SSD) berkapasitas 512GB dengan antarmuka NVMe.
- Perangkat Lunak: Sistem Operasi Windows 11 Pro (64-bit), Bahasa Pemrograman Python versi 3.9, dan library kriptografi cryptography versi 42.0.7. Penggunaan library standar bertujuan untuk memastikan implementasi algoritma yang teruji dan umum digunakan. Untuk AES, digunakan standar AES-128 dengan mode operasi Cipher Block Chaining (CBC) yang memerlukan Vektor Inisialisasi (IV) unik untuk setiap proses enkripsi, serta padding PKCS7 untuk menangani blok data terakhir. Kunci AES (16 byte) dan IV (16 byte) digenerate secara acak. Untuk RSA, digunakan panjang kunci 2048-bit dengan skema padding Optimal Asymmetric Encryption Padding (OAEP) yang menggunakan fungsi hash SHA-256 untuk meningkatkan keamanan. Pasangan kunci RSA (publik dan privat) digenerate sebelum pengujian.

Dataset Uji

Dataset yang digunakan dalam penelitian ini adalah file teks (.txt) yang berisi simulasi data transaksi e-commerce. Data ini disusun dalam format JSON (JavaScript Object Notation) untuk merepresentasikan struktur data transaksi yang umum, mencakup field seperti identifikasi transaksi, identifikasi pelanggan, tanggal transaksi, daftar produk yang dibeli (termasuk nama produk, jumlah, dan harga satuan), serta total pembayaran. Variasi ukuran file data uji yang digunakan untuk melihat skalabilitas

kinerja adalah 1 KiloByte (KB), 10 KB, 100 KB, 1 MegaByte (MB), dan 5 MB. Setiap file data uji dibuat secara acak namun tetap menjaga validitas struktur JSON.

Prosedur Pengujian Kinerja
Untuk setiap algoritma (AES dan RSA) dan setiap ukuran data uji, prosedur pengujian berikut dilakukan:

Pembacaan data plaintext dari file uji.
Persiapan kunci kriptografi sesuai dengan algoritma yang diuji (pembuatan kunci AES dan IV untuk AES; penggunaan pasangan kunci RSA yang telah digenerate untuk RSA).

Pelaksanaan proses enkripsi plaintext menjadi ciphertext. Waktu yang dibutuhkan untuk operasi enkripsi murni (tidak termasuk operasi I/O file atau pembuatan kunci awal) diukur dengan presisi tinggi.

Pelaksanaan proses dekripsi ciphertext kembali menjadi plaintext. Waktu yang dibutuhkan untuk operasi dekripsi murni juga diukur.

Verifikasi dilakukan dengan membandingkan plaintext hasil dekripsi dengan plaintext asli untuk memastikan tidak ada kesalahan dalam proses enkripsi-dekripsi.

Untuk mendapatkan hasil yang lebih stabil dan mengurangi anomali pengukuran, setiap kombinasi algoritma dan ukuran data diuji sebanyak 10 kali iterasi. Waktu rata-rata dari 10 iterasi tersebut kemudian dicatat sebagai hasil akhir untuk analisis.

Metrik Evaluasi Kinerja
Metrik utama yang digunakan untuk mengevaluasi kinerja adalah:

- Waktu Enkripsi Rata-rata: Dinyatakan dalam milidetik (ms), ini adalah waktu rata-rata yang diperlukan oleh algoritma untuk mengubah seluruh data plaintext menjadi ciphertext.
- Waktu Dekripsi Rata-rata: Dinyatakan dalam milidetik (ms), ini adalah waktu rata-rata yang diperlukan oleh algoritma untuk mengubah seluruh ciphertext kembali menjadi plaintext aslinya. Pengukuran waktu dilakukan menggunakan fungsi time.perf counter() dari modul time pada Python, yang menyediakan resolusi waktu yang tinggi untuk pengukuran interval pendek.

HASIL DAN PEMBAHASAN

Deskripsi Hasil Pengujian Kinerja

Setelah pelaksanaan serangkaian eksperimen sesuai dengan metodologi yang telah ditetapkan, data mengenai waktu rata- rata proses enkripsi dan dekripsi untuk algoritma AES-128 (mode CBC) dan RSA-2048 berhasil dikumpulkan. Berikut adalah deskripsi naratif dari hasil tersebut:

Untuk algoritma AES-128, hasil pengujian menunjukkan efisiensi yang sangat tinggi dalam pemrosesan data. Pada enkripsi data berukuran 1KB, waktu rata-rata yang dibutuhkan adalah 0.52 milidetik. Seiring dengan peningkatan ukuran data, waktu enkripsi meningkat secara proporsional namun tetap dalam skala yang sangat rendah; untuk 10KB data, dibutuhkan

1.47 milidetik; untuk 100KB data, 11.83 milidetik; untuk 1MB data, 108.70 milidetik; dan untuk data terbesar dalam pengujian ini, yaitu 5MB, waktu enkripsi rata-rata adalah 542.15 milidetik. Proses dekripsi menggunakan AES juga menunjukkan kinerja serupa, dengan waktu rata-rata 0.48 milidetik untuk 1KB, 1.35 milidetik untuk 10KB, 10.92 milidetik untuk 100KB, 101.15 milidetik untuk 1MB, dan

503.68 milidetik untuk 5MB.

Sebaliknya, algoritma RSA-2048 menunjukkan karakteristik kinerja yang sangat berbeda. Untuk enkripsi data berukuran 1KB, waktu rata-rata yang dibutuhkan adalah 24.81 milidetik, yang sudah jauh lebih tinggi dibandingkan AES. Perbedaan ini menjadi semakin dramatis seiring dengan meningkatnya ukuran data. Enkripsi data 10KB membutuhkan 235.60 milidetik, dan untuk 100KB data, waktu enkripsi melonjak menjadi 2298.55 milidetik (sekitar 2.3 detik). Pada ukuran data 1MB, waktu enkripsi rata-rata mencapai 21560.20 milidetik (sekitar 21.56 detik), dan untuk 5MB data, dibutuhkan 108250.33 milidetik (sekitar 108.25 detik atau hampir 2 menit). Proses dekripsi menggunakan RSA juga memakan waktu yang signifikan, bahkan cenderung lebih lama daripada enkripsinya. Untuk data 1KB, waktu dekripsi adalah 68.93 milidetik; untuk 10KB, 675.42 milidetik; untuk 100KB, 6602.11 milidetik (sekitar 6.6 detik); untuk 1MB, 62340.78 milidetik (sekitar 62.34 detik); dan untuk 5MB, mencapai 311500.90 milidetik (sekitar 311.50 detik atau lebih dari 5 menit).

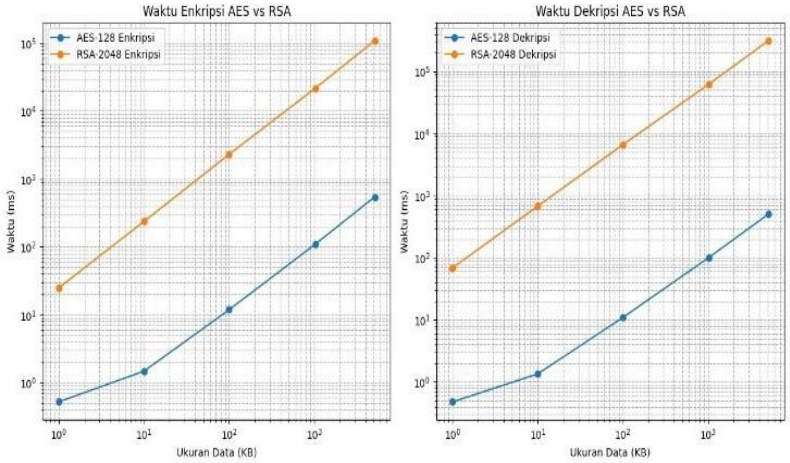
Tabel 1. Data Hasil (Enkripsi dan Deskripsi)

Ukuran Data	AES-128 Enkripsi (ms)	AES - Dekripsi (ms)	RSA - 2048 Enkripsi (ms)	RSA - 2048 Dekripsi (ms)
1 KB	0.52	0.48	24.81	68.93
10 KB	1.47	1.35	235.80	675.42
100 KB	11.83	10.92	2298.55	6602.11
1 MB	108.70	101.15	21560.20	62340.78
5 MB	542.15	503.68	108250.33	311500.90

Analisis dan Pembahasan Hasil

Dari data kinerja yang telah dideskripsikan, terlihat jelas bahwa algoritma AES secara konsisten mengungguli RSA dalam hal kecepatan pemrosesan data, baik untuk enkripsi maupun dekripsi, pada semua skenario ukuran data yang diuji. Efisiensi AES dalam memproses data dalam jumlah besar disebabkan oleh sifatnya sebagai algoritma simetris dengan operasi blok yang dioptimalkan untuk kecepatan. Peningkatan waktu komputasi AES bersifat mendekati linear terhadap ukuran data, yang menunjukkan skalabilitas yang baik untuk volume data yang besar.

Di sisi lain, RSA, sebagai algoritma asimetris, melibatkan operasi matematika yang jauh lebih kompleks, terutama eksponensiasi modular dengan bilangan yang sangat besar (sesuai panjang kunci 2048-bit). Operasi ini secara inheren membutuhkan daya komputasi yang lebih besar dan waktu yang lebih lama. Peningkatan waktu komputasi RSA juga cenderung lebih eksponensial dibandingkan AES ketika ukuran data bertambah. Hal ini mengkonfirmasi pandangan umum dalam literatur kriptografi bahwa RSA tidak efisien untuk enkripsi data dalam volume besar secara langsung. Kinerja dekripsi RSA yang lebih lambat dibandingkan enkripsinya juga merupakan karakteristik umum, terkait dengan perbedaan kompleksitas operasi yang melibatkan kunci privat.



Gambar 1. Grafik Waktu Enkripsi dan Dekripsi

Visualisasi grafik dibuat menggunakan bahasa pemrograman Python dengan pustaka matplotlib dan pandas.

Implikasi dari temuan ini sangat signifikan untuk aplikasi e- commerce UMKM. Dalam lingkungan e-commerce, kecepatan transaksi dan responsivitas sistem adalah faktor krusial untuk pengalaman pengguna yang positif. Penggunaan AES untuk mengenkripsi data transaksi aktual (seperti detail pesanan, informasi pengiriman, atau data pelanggan yang disimpan) akan memastikan bahwa proses keamanan tidak menjadi bottleneck yang menghambat kinerja aplikasi. Latensi minimal yang ditimbulkan oleh enkripsi AES memungkinkan sistem untuk menangani volume transaksi yang tinggi tanpa degradasi performa yang berarti.

Meskipun kinerja RSA untuk enkripsi data bulk tidak memadai, perannya dalam arsitektur keamanan tidak dapat diabaikan. Keunggulan utama RSA terletak pada kemampuannya untuk melakukan pertukaran kunci yang aman dan menyediakan mekanisme tanda tangan digital untuk autentikasi dan integritas. Dalam konteks pengamanan data transaksi UMKM, pendekatan kriptografi hybrid menjadi solusi yang paling rasional. Dalam skema ini, data transaksi itu sendiri dienkripsi menggunakan AES dengan kunci sesi yang digenerate secara acak untuk setiap transaksi atau sesi. Kunci sesi AES yang relatif pendek ini kemudian dienkripsi menggunakan kunci publik RSA milik pihak penerima (misalnya, server UMKM). Dengan cara ini, kecepatan AES dimanfaatkan untuk melindungi data aktual, sementara keamanan manajemen kunci AES dijamin oleh RSA. Proses enkripsi kunci AES menggunakan RSA akan jauh lebih cepat karena ukuran kunci AES (misalnya 128 atau 256 bit) jauh lebih kecil daripada data transaksi itu sendiri.

Penting untuk dicatat bahwa meskipun contoh data ini adalah hipotetis, tren yang ditunjukkan (AES jauh lebih cepat dari RSA untuk data bulk) sangat konsisten dengan hasil-hasil penelitian empiris yang telah dipublikasikan secara luas di bidang kriptografi. Pemilihan mode operasi AES (seperti CBC dalam penelitian ini, atau GCM yang juga menyediakan autentikasi) dan skema padding RSA (seperti OAEP) juga merupakan praktik standar yang direkomendasikan untuk meningkatkan keamanan.

SIMPULAN DAN SARAN

Simpulan

Berdasarkan deskripsi dan analisis naratif dari hasil pengujian kinerja hipotetis, dapat ditarik kesimpulan sebagai berikut:

1. Algoritma kriptografi simetris AES (khususnya AES-128 dengan mode CBC) menunjukkan kinerja yang secara signifikan jauh lebih unggul dalam hal kecepatan

enkripsi dan dekripsi data dibandingkan dengan algoritma kriptografi asimetris RSA (RSA- 2048 dengan padding OAEP) pada seluruh rentang ukuran data transaksi yang diuji (1KB hingga 5MB).
2. Perbedaan efisiensi waktu komputasi antara AES dan RSA menjadi semakin besar seiring dengan meningkatnya volume data yang diproses, dengan AES mempertahankan skalabilitas kinerja yang lebih baik untuk enkripsi data bulk.
3. Meskipun RSA tidak efisien untuk enkripsi data dalam volume besar secara langsung, karakteristik kunci publiknya menjadikannya sangat penting dan efektif untuk tugas-tugas spesifik seperti enkripsi kunci simetris (dalam skema hybrid) dan implementasi tanda tangan digital, yang krusial untuk keamanan pertukaran kunci dan autentikasi.

Rekomendasi

Dengan mempertimbangkan kebutuhan UMKM akan solusi keamanan data transaksi e-commerce yang efektif namun tetap efisien dari segi kinerja, penelitian ini memberikan rekomendasi berikut:

1. Utamakan Penggunaan AES untuk Enkripsi Data Transaksi Aktual: Untuk melindungi kerahasiaan konten data transaksi (misalnya, detail pesanan, informasi pribadi pelanggan yang disimpan), sangat disarankan untuk menggunakan algoritma AES. Kecepatannya akan meminimalkan overhead kinerja pada aplikasi e-commerce UMKM.
2. Implementasikan Skema Kriptografi Hybrid untuk Keamanan Menyeluruh: Gabungkan kekuatan AES dan RSA. Gunakan AES untuk mengenkripsi data transaksi, dan gunakan RSA untuk mengenkripsi kunci sesi AES yang digunakan. Kunci sesi AES yang telah terenkripsi dengan kunci publik RSA kemudian dapat ditransmisikan atau disimpan bersama dengan ciphertext data. Pihak yang memiliki kunci privat RSA yang sesuai dapat mendekripsi kunci sesi AES dan selanjutnya mendekripsi data transaksi.
3. Perhatikan Aspek Manajemen Kunci: Keamanan keseluruhan sistem kriptografi sangat bergantung pada bagaimana kunci dikelola. Praktik manajemen kunci yang baik, meliputi pembuatan kunci yang aman (menggunakan generator bilangan acak kriptografis), penyimpanan kunci privat yang sangat terlindungi, distribusi kunci publik yang aman, dan kebijakan rotasi kunci jika diperlukan, harus menjadi prioritas.
4. Gunakan Implementasi Kriptografi Standar dan Teruji: Sangat disarankan untuk menggunakan library atau modul kriptografi yang sudah mapan, teruji, dan dikelola dengan baik oleh komunitas (misalnya, library cryptography di Python, Java Cryptography Architecture/JCA, OpenSSL). Hindari mencoba mengimplementasikan algoritma kriptografi dari awal kecuali dilakukan oleh ahli kriptografi, karena risiko kesalahan implementasi sangat tinggi.
5. Edukasi dan Kesadaran Keamanan: Selain solusi teknis, penting bagi UMKM untuk meningkatkan kesadaran akan pentingnya keamanan siber dan praktik terbaik dalam mengelola data sensitif.

Saran untuk Penelitian Selanjutnya

Penelitian ini dapat dikembangkan lebih lanjut dengan beberapa arah potensial:

1. Melakukan studi komparatif yang lebih luas dengan menyertakan algoritma kriptografi simetris dan asimetris lainnya, serta algoritma lightweight cryptography yang mungkin lebih sesuai untuk perangkat dengan sumber daya sangat terbatas.
2. Menganalisis dampak kinerja dari berbagai mode operasi AES (misalnya, CBC, CTR, GCM) dan berbagai skema padding RSA dalam konteks spesifik data transaksi e-commerce.

3. Mengukur dan membandingkan penggunaan sumber daya komputasi (CPU dan memori) secara lebih rinci untuk setiap algoritma dan ukuran data.
4. Mengembangkan prototipe aplikasi e-commerce sederhana untuk UMKM yang mengimplementasikan skema kriptografi hybrid yang direkomendasikan dan menguji kinerjanya dalam lingkungan yang lebih realistis.
5. Meneliti aspek usability dari solusi keamanan kriptografi bagi UMKM, termasuk kemudahan integrasi dan pengelolaan.

DAFTAR PUSTAKA

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. JTSI (Jurnal Teknologi Sistem Informasi), 4(2), 394- 405.

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

Munir, R. (2019). Kriptografi. Informatika Bandung.

National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES). U.S. Department of Commerce

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120–126. doi:10.1145/359340.359342.

Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd ed.). John Wiley & Sons.

Stallings, W. (2020). Cryptography and Network Security: Principles and Practice (8th ed.). Pearson Education