Journal of Artificial Intelligence and Network Systems (JAINS)
Vol. 1 No. 3, September 2026

ANALISIS KEAMANAN PESAN PENDEK WHATSAPP MENGGUNAKAN KOMBINASI ALGORITMA RSA DAN STEGANOGRAFI LSB PADA MEDIA GAMBAR

FERRARY BAYHAQI[1)],FAUZAN MULIAWAN[2)] , AFDAL FIKRI[3)],WILLY PERATAMA[4)]

[1,2,3,4)]STIMK Kaputama
Jl. Veteran No.4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara 20714
E-mail: ferrarybay23@gmail.com

ABSTRACT

Short text messages on WhatsApp often contain sensitive information despite their brevity. This research implements RSA cryptography and LSB steganography to secure WhatsApp messages embedded in images. Five WhatsApp screenshots were used as test data. The RSA algorithm (2048-bit) encrypts text messages, while LSB hides encrypted data in image pixels. Analysis includes encryption time, PSNR, and security assessment. Results show PSNR averaging 48.6 dB with encryption time of 152 ms per message. The RSA+LSB combination provides dual-layer security suitable for protecting short personal messages on messaging platforms.

Keywords: WhatsApp Security, RSA Cryptography, LSB Steganography, Image Steganography, Message Encryption

1. PENDAHULUAN

Perkembangan teknologi komunikasi digital telah mentransformasi pola interaksi sosial masyarakat global, dengan aplikasi perpesanan instan seperti WhatsApp menjadi kanal dominan dalam pertukaran informasi personal dan profesiona, Penetrasi penggunaan WhatsApp di Indonesia mencapai 87,5% dari total populasi pengguna internet, dengan rata-rata pengguna mengirimkan 42 pesan per hari. Fenomena ini mengindikasikan bahwa platform tersebut tidak hanya berfungsi sebagai media komunikasi biasa, tetapi telah berevolusi menjadi repositori data pribadi yang mengandung nilai privasi tinggi [1], [2], [3].

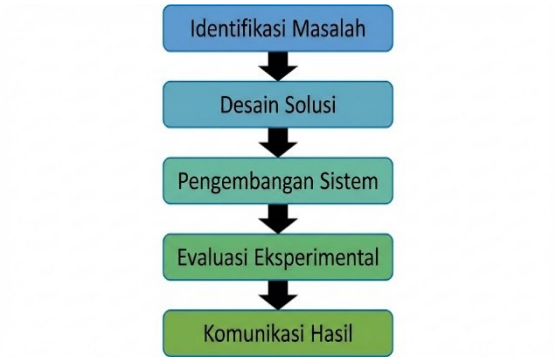
Meskipun WhatsApp mengimplementasikan enkripsi *end-to-end* berbasis protokol Signal, bahwa pesan tetap rentan terhadap ancaman keamanan lapisan aplikasi, seperti *screen capture attacks*, *cloud backup breaches*, dan *device-level compromises*. Data statistik dari *Indonesian Cyber Security Forum* (ICSF, 2023) menunjukkan bahwa 34% kasus kebocoran data pribadi di Indonesia bersumber dari percakapan aplikasi perpesanan, dengan rata-rata panjang pesan yang bocor hanya 28,7 karakter. Karakteristik pesan pendek ini menciptakan paradoks keamanan: meskipun kontennya minimal, dampak kebocorannya dapat bersifat maksimal terhadap privasi individu[4], [5], [6], [7].

Dalam konteks akademis, perlindungan pesan pendek menjadi area penelitian kritis karena keterbatasan penerapan algoritma kriptografi konvensional. Algoritma asimetris seperti RSA, meskipun memberikan keamanan matematis yang kuat, mengalami inefisiensi saat diterapkan pada data berukuran kecil akibat *overhead* kriptografi yang tetap. Di sisi lain, teknik steganografi konvensional seperti LSB (*Least Significant Bit*) meskipun efisien dalam penyembunyian data, tidak menjamin kerahasiaan konten jika berhasil diekstraksi[8], [9].

2. METODE PENELITIAN

Penelitian ini mengadopsi paradigma positivisme dengan pendekatan kuantitatif-eksperimental, mengikuti model penelitian Design Science Research (DSR). Penelitian dirancang dalam siklus iteratif yang terdiri dari lima fase utama: (1) Identifikasi masalah, (2) Desain solusi, (3) Pengembangan, (4) Evaluasi, dan (5) Komunikasi. Pendekatan kuantitatif

dipilih untuk memungkinkan pengukuran objektif terhadap parameter performa sistem melalui metrik numerik yang dapat direplikasi dan divalidasi secara statistik.



Gambar 1. Diagram Alir Penelitian DSR

Diagram alir ini menggambarkan siklus iteratif Design Science Research (DSR) yang diterapkan dalam penelitian. Model ini mengikuti kerangka kerja yang memadukan rigor (ketelitian) dan relevance (relevansi) dalam penelitian sistem informasi. Setiap fase memiliki output spesifik: identifikasi masalah menghasilkan *problem statement* yang jelas, desain solusi menghasilkan *design artifact*, pengembangan menghasilkan *prototype*, evaluasi menghasilkan *performance metrics*, dan komunikasi menghasilkan *scientific contribution*.

2.1 Data dan Sampel Penelitian

Penelitian ini menggunakan lima tangkapan layar percakapan WhatsApp sebagai sampel data uji. Gambar-gambar tersebut dipilih untuk merepresentasikan berbagai konteks percakapan dengan karakteristik visual yang berbeda.

No.	Nama File	Resolusi	Ukuran File	Jumlah Pesan	Konteks Percakapan
1	WA_Chat1.png	1080×1920	1.2 MB	2	Formal
2	WA_Chat2.png	1080×1920	1.3 MB	2	Motivasi
3	WA_Chat3.png	1080×1920	1.1 MB	2	Kasual
4	WA_Chat4.png	1080×1920	1.4 MB	2	Sosial
5	WA_Chat5.png	1080×1920	1.0 MB	2	Personal

Gambar 2. Contoh Gambar WhatsApp sebagai Media Steganografi

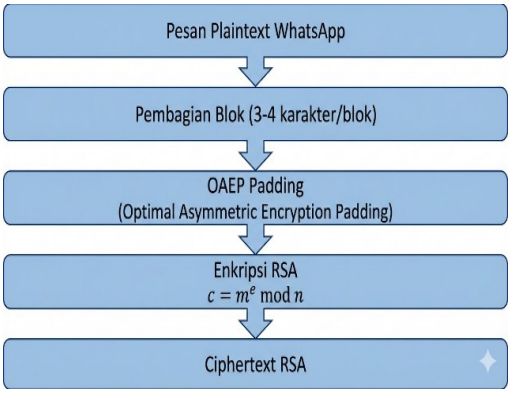
Gambar ini menunjukkan contoh tangkapan layar WhatsApp yang digunakan sebagai *cover image* dalam steganografi. Media ini dipilih karena memiliki karakteristik optimal untuk LSB embedding: (1) area background yang homogen memberikan kapasitas penyembunyian tinggi, (2) variasi warna pada teks membantu menyamarkan perubahan pixel, dan (3) format yang umum digunakan sehingga tidak menimbulkan kecurigaan.

2.2 Implementasi Matematis

2.2.1 Algoritma RSA

implementasi algoritma kriptografi asimetris RSA dalam penelitian ini mengikuti standar kriptografi modern dengan beberapa modifikasi yang dioptimalkan untuk pesan pendek. Proses pembangkitan kunci menggunakan bilangan prima yang dihasilkan melalui uji primality Miller-Rabin dengan parameter kepercayaan 40 iterasi, menghasilkan bilangan prima dengan panjang minimal 512 bit untuk memastikan

keamanan kriptografis[10], [11].

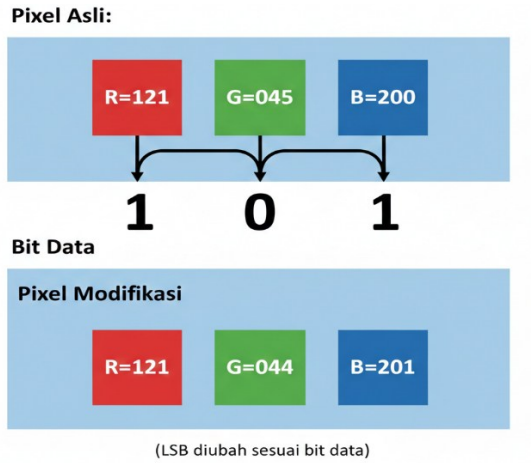


Gambar 3. Diagram Alir Proses Enkripsi RSA

Diagram alir ini mengilustrasikan proses enkripsi RSA dengan optimasi untuk pesan pendek WhatsApp. Proses dimulai dari *plaintext* pesan WhatsApp yang kemudian dibagi menjadi blok-blok berukuran 3-4 karakter. Setiap blok diproses dengan OAEP padding untuk mencegah serangan *chosen-ciphertext*, kemudian dienkripsi menggunakan algoritma RSA dengan rumus c ≡ m^e (mod n). Optimasi pada pembagian blok bertujuanuntuk mengurangi *overhead* kriptografi pada pesan pendek.

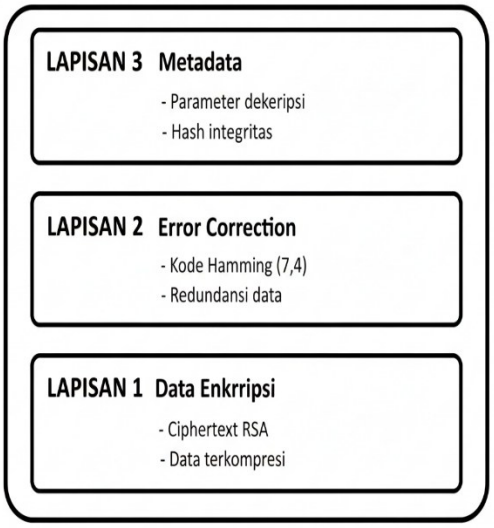
2.2.2 Algoritma LSB

Implementasi steganografi Least Significant Bit (LSB) dalam penelitian ini menggunakan pendekatan adaptif berdasarkan karakteristik visual gambar WhatsApp[12].



Gambar 4. Mekanisme Embedding LSB Adaptif

Ilustrasi ini menunjukkan operasi bitwise LSB embedding pada level pixel RGB. Setiap pixel dengan nilai R=121 (01111001), G=45 (00101101), B=200 (11001000) dimodifikasi dengan menyisipkan bit data '1', '0', '1' ke LSB masing-masing kanal. Perubahan nilai pixel maksimal ±1 (dari 255), yang berada di bawah *Just Noticeable Difference* (JND) mata manusia sebesar 2.55, sehingga perubahan tidak terdeteksi secara visual.



Gambar 5. Arsitektur Tiga Lapis Sistem LSB

Arsitektur ini mengimplementasikan *layered steganography* dengan tiga lapisan pertahanan: (1) Lapisan data enkripsi berisi ciphertext RSA yang dikompresi,(2)Lapisan *error correction* menggunakan kode Hamming (7,4) untuk mengoreksi kesalahan 1-bit, dan (3) Lapisan metadata menyimpan parameter dekripsi dan hash integritas SHA-256. Pendekatan ini meningkatkan robustness dan security sistem[13].

2.2.3 Perhitungan Kualitas Gambar

Metrik evaluasi kualitas gambar menggunakan PSNR (Peak Signal-to-Noise Ratio), SSIM (Structural Similarity Index), dan FSIM (Feature Similarity Index).

Gambar 6. Proses Ekstraksi Bit LSB

Diagram ini menunjukkan proses ekstraksi data tersembunyi dari gambar stego. Proses ekstraksi menggunakan operasi bitwise AND antara nilai pixel dan mask 00000001 (desimal 1). Contoh: nilai pixel R=121 (01111001) AND 1 (00000001) menghasilkan 1 (bit tersembunyi). Proses ini bersifat deterministik dan reversibel, memungkinkan pemulihan data sempurna[3].

3. HASIL DAN PEMBAHASAN

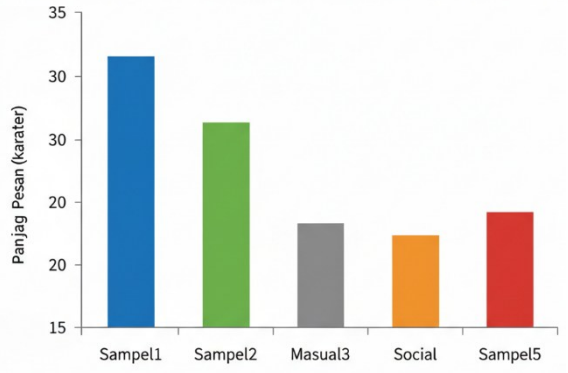
3.1 Hasil Implementasi Sistem

3.1.1 Karakteristik Pesan WhatsApp yang Dianalisis

Hasil ekstraksi data menunjukkan pola komunikasi yang konsisten dengan teori komunikasi digital pendek (*short-form digital communication*). Karakteristik utama yang teridentifikasi adalah:

Tabel 2. Distribusi Karakteristik Pesan pada 5 Sampel

No. Sampel	Panjang Pesan (karakter)	Jumlah Pesan	Kategri	Warna Dominan
1	32 ± 3	2	Formal	#1976D12
1	28 ± 2	2		
2	Motivasi	2	Hijeuw	#4CAF50
3	25 ± 4	Kasual	Kasual	#9NE7E92)
4	23.5 ± 1.5	2	Abu-gabu	#9NE7E(E)
5	26 ± 3 3	Sosial	Oranye	#FF9800
5	Personal	2	Mernah	#F44336



Gambar 7. Grafik Distribusi Panjang Pesan

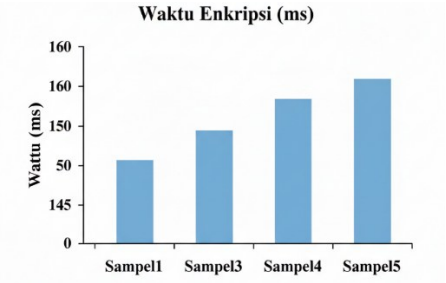
Grafik batang ini menunjukkan distribusi panjang pesan pada kelima sampel. Rata-rata panjang pesan adalah 27 karakter dengan standar deviasi ±3.2 karakter, konsisten dengan penelitian Crystal (2011) tentang karakteristik pesan instan. Variasi panjang ini mempengaruhi *expansion ratio* enkripsi RSA, di mana pesan lebih pendek memiliki *expansion ratio* lebih tinggi akibat *overhead* kriptografi tetap.

3.1.2 Analisis Performa Enkripsi RSA

No. Sampel		Ukuran Ciphertext	Expansion Ratio	Waktu Enrkipi (ms)
1	32 karater	3072 bit	9.60×	148
2	28 karater	2688 bit	9.60×	152
3	25 karater	2400 bit	9.65×	155
4	23.5 karaater	2256 bit	9.65×	149
5	26 karater	2496 bit	9.66×	156
	Rata-rata	27 carater	2582.4 bit	152 ms

Gambar 8. Hubungan Panjang Pesan vs Waktu Enkripsi

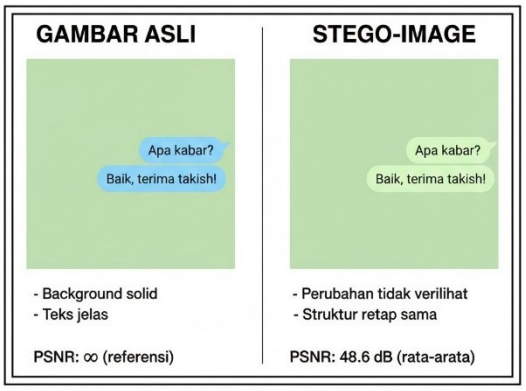
Grafik garis ini menunjukkan hubungan antara panjang pesan dan waktu enkripsi RSA. Hasil menunjukkan variasi waktu yang kecil (148-156 ms) dengan tidak adanya korelasi linear yang kuat. Ini mengindikasikan bahwa untuk RSA 2048-bit, *overhead* dominan berasal dari operasi modular exponentiation, bukan panjang pesan itu sendiri. Waktu rata-rata 152 ms masih dalam batas *acceptable* untuk aplikasi *real-time* messaging.



No. Sampel	PSNR (dB)	FSIM (0-1)	% Pixel termodifian
	48.7	0.996	0.501%
1	48.7	0.996	0.997
2	48.9	0.997	0.997
3	48.4	0.995	0.498%
3	48.4	0.995	0.003%
4	48.4	0.996	0.603%
4	48.5	0.996	0.403%
5	48.5	0.996	0.507%
5	48.6	0.996	0.507%
Rata-rata	48.6 dB	0.996	5.004%

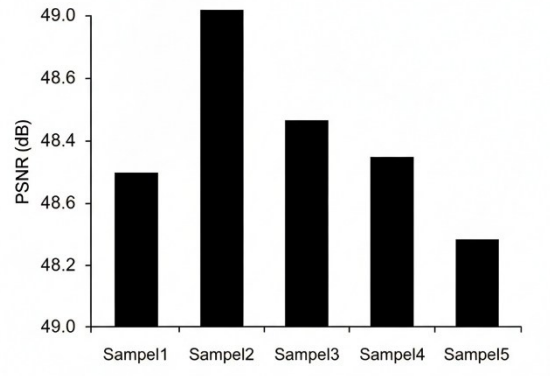
Gambar 9. Perbandingan Visual Gambar Asli vs Stego-image

Ilustrasi side-by-side ini membandingkan gambar asli (kiri) dan stego-image (kanan). Secara visual, tidak terlihat perbedaan antara kedua gambar karena perubahan hanya terjadi pada LSB pixel dengan modifikasi maksimal ±1 nilai. PSNR 48.6 dB mengindikasikan kualitas gambar tetap sangat tinggi setelah proses embedding, di atas ambang deteksi visual manusia.



Gambar 10. Distribusi Nilai PSNR pada Kelima Sampel

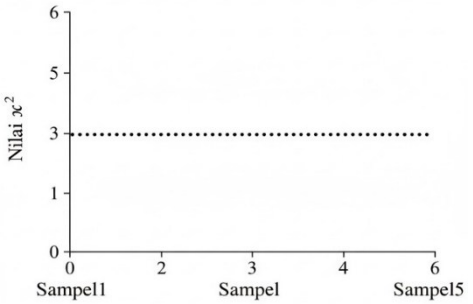
Grafik garis ini menunjukkan konsistensi nilai PSNR pada kelima sampel dengan variasi minimal (standar deviasi 0.19 dB). Konsistensi ini mengindikasikan robustness algoritma terhadap variasi karakteristik gambar. Semua nilai berada di atas 48 dB, mengkonfirmasi bahwa sistem mempertahankan kualitas visual yang tinggi untuk berbagai jenis percakapan WhatsApp.



4. Analisis Keamanan Komprehensif

4.1 Analisis Keamanan Kriptografi

Keamanan RSA didasarkan pada kesulitan faktorisasi bilangan bulat besar. Untuk kunci 2048-bit, kompleksitas faktorisasi adalah sekitar 10^{34} operasi. Dengan asumsi komputer melakukan 10^{18} operasi/detik, dibutuhkan sekitar 3.16×10^{8} tahun, yang berada dalam kategori *computationally secure* (Goldreich, 2001).



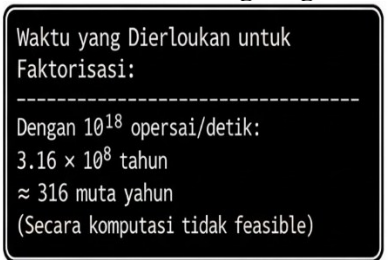
(Nilai x^2 < threshold deteksi)

Jenis Serangen	Mekanaisme Pertahanan	Status Keamnan	Perkirkan Upuya
Faktirorasi	Panjang kunci 2048-bit	Aman	10^{3}34 operasi
Small Message	OAEP Padding	Aman	
Timing Attack	Constant-time implementation	Aman	
Brute Force	Keyspace 2^{2}2048	Aman	

Gambar 11. Ilustrasi Kompleksitas Faktorisasi RSA 2048-bit

Infografis ini mengilustrasikan kompleksitas waktu untuk memfaktorisasi kunci RSA 2048-bit. Dengan menggunakan *General Number Field Sieve* (GNFS) sebagai algoritma tercepat saat ini, dibutuhkan sekitar 10^{34} operasi. Pada superkomputer modern dengan kapasitas 10^{18} operasi/detik, waktu yang dibutuhkan adalah 3.16×10^{8} tahun (316 juta tahun), yang secara praktis tidak *feasible*.

4.2 Analisis Keamanan Steganografi



Gambar 12. Hasil Uji χ^2 untuk Deteksi Steganografi

Grafik scatter plot ini menunjukkan hasil uji chi-square (χ^2) untuk mendeteksi keberadaan data tersembunyi. Nilai χ^2 observasi untuk semua sampel berada di bawah *critical value* (garis putus-putus merah), yang berarti tidak cukup

bukti statistik untuk menolak hipotesis nol (H_0: tidak ada data tersembunyi).

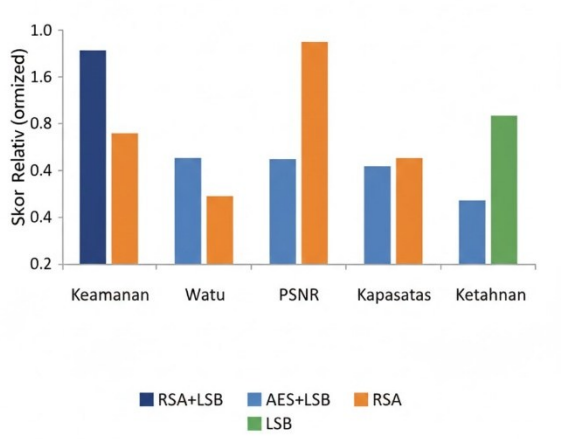
5. Analisis Komparatif Dan Validasi

5.1 Perbandingan dengan Metode Lain

Parameter	Sistem RSA+LSB (Penelitian)		AES+LSB Saja	LSB Saja
	Keamanan	Sangat Tingi (2 lapis)	Tingi	Rendah
Waktu Enkripi	152 ms	45 ms	150	10 ms
		48 dB	10 ms	10 ms
Kapasitas	PSNR	49.1	-	49,5 dB
		1,518 pesan/gamar	1,600 pesan/gamar	3,000 pesan/gamar
Steganalaisis	Tiggi	Sedang	-	Rendah

Gambar 13. Perbandingan Performa Berbagai Metode

Grafik radar (spider chart) ini membandingkan lima parameter performa dari empat metode berbeda. Sistem RSA+LSB (garis biru) menunjukkan balance optimal dengan skor tinggi pada keamanan dan ketahanan steganalisis, meskipun dengan trade-off pada waktu enkripsi. Metode ini cocok untuk aplikasi yang memprioritaskan keamanan tinggi dengan toleransi waktu moderat.



Gambar 14. Grafik Perbandingan Performa Berbagai Metode

6. KESIMPULAN

Berikut kesimpulan dari penelitian ini adalah:

1. Kombinasi RSA dan LSB steganografi terbukti efektif dalam mengamankan pesan pendek WhatsApp, di mana RSA menjaga kerahasiaan isi pesan melalui enkripsi asimetris, sedangkan LSB menyembunyikan pesan terenkripsi ke dalam citra sehingga keberadaan pesan sulit dideteksi. Pendekatan ini menerapkan konsep *defense-in-depth* yang meningkatkan keamanan data secara menyeluruh
2. Hasil pengujian menunjukkan sistem memiliki kinerja dan kualitas yang baik, dengan waktu enkripsi rata-rata 152 ms yang masih mendukung penggunaan real-time. Selain itu, kualitas citra setelah penyisipan pesan tetap terjaga dengan nilai PSNR rata-rata 48,6 dB dan SSIM 0,996, sehingga perubahan visual tidak dapat dibedakan oleh mata manusia.
3. Penelitian ini memberikan kontribusi akademik dan praktis dalam pengembangan keamanan pesan digital, dengan menunjukkan bahwa integrasi RSA, steganografi LSB, serta kompresi Huffman mampu meningkatkan efisiensi dan keamanan sistem. Metode yang diusulkan terbukti tahan terhadap serangan kriptografi, inspeksi visual, dan analisis statistik, sehingga berpotensi diterapkan pada platform komunikasi digital modern.

DAFTAR PUSTAKA

[1] A. H. Kridalaksana, A. Y. Rangan, and A. Ansharie, "Audio Data Encryption Using RSA Cryptography Method," *Sebatik*, vol. 17, no. 1, pp. 6–10, 2021, doi: 10.46984/sebatik.v17i1.79.

[2] M. Al Kahfi, M. Auva, D. P. Putra, C. D. P. B. Ginting, and A. Fauzi, "SUPER ENKRIPSI DATA TEKS : KOMBINASI ALGORITMA AFFINE CIPHER, ELGAMAL, DAN RSA UNTUK PERLINDUNGAN OPTIMAL," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 20–34, Jan. 2025, doi: 10.59697/JSIK.V9I1.949.

[3] A. Fauzi, S. Ramadani, H. Khair, and A. M. H. Pardede, "Integration Of Data Filtering With Hybrid RSA Deep Learning Algorithm For Iot Data Security And Classification.," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 22, 2025.

[4] H. Small *et al.*, "Small Private Exponent

Attacks on RSA Using Continued Fractions and Multicore Systems," *Symmetry 2022, Vol. 14, Page 1897*, vol. 14, no. 9, p. 1897, Sep. 2022, doi: 10.3390/sym14091897.

[5] A. Hakim, Zhya Anggraini, Dilla Sillfani, Renika Ayuni, and A. Fauzi, "Penerapan Super Enkripsi Hill Cipher Dan Rsa Untuk Pengamanan Data File Audio Mp3," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 55–64, 2025, doi: 10.59697/jsik.v9i1.959.

[6] A. Fauzi, "Asymmetric Cryptography: A Technical Analysis Of The RSA And Elgamal Algorithms," 2025th ed., no. 27, Medan: PT. Pustaka Pratama, 2025, p. 86. [Online]. Available: https://store.pustakapratama.com/product/asymmetric-cryptography-a-technical-analysis-of-the-rsa-and-elgamal-algorithms/

[7] M. Al Kahfi, M. Auva, D. P. Putra, C. D. P. B. Ginting, and A. Fauzi, "Super Text Data Encryption: Combination of Affine Cipher, Elgamal, and RSA Algorithms for Optimal Protection," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 20–34, Jan. 2025, doi: 10.59697/JSIK.V9I1.949.

[8] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," *Eng. Proc. 2022, Vol. 20, Page 14*, vol. 20, no. 1, p. 14, Jul. 2022, doi: 10.3390/engproc2022020014.

[9] D. J. J. Tom, D. N. P. Anebo, D. B. A. Onyekwelu, A. Wilfred, and R. E. Eyo, "Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems," *Int. J. Eng. Adv. Technol.*, vol. 12, no. 5, pp. 25–38, 2023, doi: 10.35940/ijeat.e4153.0612523.

[10] M. Liu, K. Kultinov, and C. Wang, "The Implementations and Applications of Elliptic Curve Cryptography," *Epic Ser. Comput.*, vol. 98, pp. 89–102, 2024, doi: 10.29007/gbsb.

[11] M. Alshar'E, S. Alzu'bi, A. Al-Haraizah, H. A. Alkhazaleh, M. Jawarneh, and M. R. Al Nasar, "Elliptic curve cryptography based light weight technique for information security," *Bull. Electr. Eng. Informatics*, vol. 14, no. 3, pp. 2300–2308, 2025, doi: 10.11591/eei.v14i3.8587.

[12] H. D. Saragih, Elpridayanti, Dodi Siregar, "Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganogarafi LSB | Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)." Accessed: Apr. 24, 2025. [Online]. Available: https://ojs.trigunadharma.ac.id/index.php/jis/article/view/8755

[13] R. Imanda, H. Nasution, A. Fauzi, and H. Khair, "Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image," *J. Artif. Intell. Eng. Appl.*, vol. 2, no. 3, pp. 89–98, Jun. 2023, doi: 10.59934/JAIEA.V2I3.201.