JAINS (Journal of Artificial Intelligence and Network Systems)
Vol. 1 No. 2, Januari 2026

PERANCANGAN SISTEM ENKRIPSI AUDIO MENGGUNAKAN ALGORITMA EL GAMAL UNTUK MENINGKATKAN PERTUKARAN FILE AUDIO

ALIFIA NAZWA[1)], MUTIA DWI NATARINA[2)], CINDY NATHALIE GRACELLA[3)], ELLI NURMA WATI[4)], ACHMAD FAUZI[5*)]

Program Studi Sistem Informasi
[1,2,3,4,5)]STMIK KAPUTAMA
Jl. Veteran No.4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara 20714
Email : alifiianazwa1@gmail.com

ABSTRACT

Security in multimedia data transmission, particularly audio, faces significant challenges regarding key distribution vulnerabilities in conventional symmetric algorithms. This study aims to design a WAV digital audio encryption system using the El-Gamal asymmetric algorithm based on the Discrete Logarithm Problem (DLP) to ensure data confidentiality without private key exchange. The research method involves transforming audio sample domains from signed to unsigned integers, applying probabilistic encryption functions, and quantitative testing. System performance evaluation is measured using Signal-to-Noise Ratio (SNR) parameters, histogram analysis, and correlation coefficients. Test results indicate that the system successfully converts original sound into unrecognizable noise with an SNR reaching -18.4 dB and a correlation coefficient near zero (0.0021), signaling the loss of linear data relationships. Histogram analysis reveals a distribution shift from Gaussian patterns to uniform, indicating high entropy and resistance to statistical attacks. Despite a twofold file size expansion, the El-Gamal algorithm proves to provide superior confidentiality and lossless data integrity compared to classical substitution methods.

Keywords: Audio Encryption, El-Gamal Algorithm, Multimedia Security, Histogram Analysis, SNR.

1. PENDAHULUAN

Di era transformasi digital saat ini, suara tidak lagi dipandang hanya sebagai getaran fisik, melainkan telah menjadi aset data yang sangat krusial dalam sistem komunikasi modern, seperti Voice over IP (VoIP) dan Internet of Things (IoT) [1]. Penelitian mengenai SoundPKI menunjukkan bahwa dalam dekade mendatang, suara akan menjadi antarmuka utama bagi perangkat pintar, sehingga secara otomatis data audio akan menjadi target utama serangan siber. Kondisi ini menjadikan keamanan data suara sebagai aspek yang sangat penting untuk diperhatikan. Transmisi data suara melalui jaringan terbuka sangat rentan terhadap penyadapan (wiretapping) dan manipulasi ilegal. Tanpa adanya mekanisme perlindungan yang memadai, kerahasiaan informasi dalam percakapan digital hanya menjadi sebuah ilusi. Oleh karena itu, kebutuhan akan sistem enkripsi audio yang andal dan aman menjadi suatu keharusan [2].

Menanggapi ancaman tersebut, berbagai pendekatan kriptografi telah dikembangkan. Namun, sebagian besar penelitian yang ada masih didominasi oleh penggunaan algoritma kriptografi kunci simetris klasik atau teknik penyembunyian

data (steganografi). Sebagai contoh, Rio Andika menerapkan algoritma stream cipher Grain V1 untuk mengamankan pesan suara pada jaringan peer-to-peer [3]. Muhammad Taufiq Sumadi et al. mengusulkan kombinasi algoritma Vigenère Cipher dan Playfair Cipher untuk meningkatkan keamanan data suara [4]. Selain itu, pendekatan steganografi juga banyak digunakan, seperti yang dilakukan oleh Arief Al Akbar et al. dan Chaerul Umam et al. yang menyisipkan pesan rahasia ke dalam media audio menggunakan metode Least Significant Bit (LSB) [4][5].

Meskipun metode kriptografi simetris memiliki keunggulan dalam hal kecepatan komputasi, sebagaimana juga diterapkan oleh Emi Suryadi et al. pada media video, metode ini memiliki kelemahan fundamental, yaitu masalah distribusi kunci (Key Distribution Problem) [6]. Jika kunci rahasia yang sama harus dikirimkan dari pengirim ke penerima melalui saluran komunikasi yang tidak aman, maka sistem keamanan tersebut menjadi sangat rentan. Apabila kunci berhasil disadap, maka seluruh mekanisme pengamanan data akan gagal sepenuhnya.

Seiring dengan perkembangan teknologi dan meningkatnya kebutuhan manusia, sistem digital semakin banyak menggantikan sistem manual. Salah satu wujud perkembangan tersebut adalah pemanfaatan Internet of Things (IoT). IoT merupakan teknologi yang mampu menghubungkan berbagai objek fisik, seperti sensor, perangkat chip, dan peralatan elektronik lainnya, melalui jaringan internet berbasis protokol TCP/IP. Teknologi ini memungkinkan pengendalian dan pemantauan perangkat secara jarak jauh, sehingga dapat meningkatkan efisiensi dan efektivitas aktivitas manusia.

Salah satu penerapan IoT yang relevan adalah pada sistem starter kendaraan. Dengan memanfaatkan IoT, kendaraan dapat dihidupkan secara otomatis melalui jaringan internet tanpa harus dilakukan secara manual. Pengguna cukup mengaktifkan starter dari jarak jauh, misalnya selama 5 menit sebelum kendaraan digunakan, sehingga kendaraan telah siap pakai. Sistem ini sangat membantu masyarakat yang memiliki mobilitas tinggi.

Berdasarkan konteks tersebut, perumusan masalah dalam penelitian ini adalah bagaimana merancang sistem kendali jarak jauh berbasis IoT untuk mengaktifkan starter kendaraan bermotor. Tujuan umum penelitian ini adalah merancang dan membangun sistem starter kendaraan menggunakan mikrokontroler untuk aktivasi kendaraan, dengan studi kasus pada sepeda motor [11]. Di sisi lain, beberapa penelitian sebelumnya juga menekankan pentingnya pengombinasian algoritma kriptografi untuk meningkatkan keamanan data. Ulfa Br. Mtd et al. (2017) mengintegrasikan Vigenère Cipher dengan One-Time Pad (OTP) dalam pengamanan citra digital [12].

Hasil penelitian menunjukkan bahwa kombinasi tersebut mampu menjaga kerahasiaan data dan meningkatkan ketahanan sistem terhadap serangan. Namun, metode ini masih memiliki kelemahan, terutama pada penurunan performa ketika diterapkan pada data berukuran besar, sehingga efisiensinya menjadi terbatas. Untuk mengatasi permasalahan distribusi kunci pada kriptografi simetris, paradigma keamanan modern mulai bergeser ke arah kriptografi asimetris atau Public Key Cryptography. Rusdianto et al. telah menerapkan algoritma Rabin Public Key pada file audio [7]. Namun, algoritma El-Gamal memiliki keunggulan matematis yang lebih kuat

karena berbasis pada Discrete Logarithm Problem (DLP), yang sangat sulit untuk dipecahkan secara komputasional.

Keandalan algoritma El-Gamal telah dibuktikan oleh Rio Andika et al. [6] pada tahun 2025 melalui penerapan super encryption El-Gamal pada citra digital, serta oleh Aminudin et al. yang mengkaji efisiensi dari varian hibridanya [8]. Dibandingkan dengan pendekatan berbasis chaos theory yang kompleks, seperti yang diteliti oleh Zhou et al., algoritma El-Gamal menawarkan struktur keamanan probabilistik. Artinya, pesan yang sama jika dienkripsi dua kali akan menghasilkan ciphertext yang berbeda. Karakteristik ini sangat penting untuk mencegah penyerang mengenali pola komunikasi yang berulang [9].
Berdasarkan analisis kesenjangan penelitian tersebut, dapat disimpulkan bahwa:

1. Metode kriptografi simetris memiliki kelemahan pada distribusi kunci.
2. Penerapan kriptografi asimetris pada pengamanan data audio masih relatif minim.
3. Algoritma El-Gamal memiliki potensi besar untuk diterapkan dalam enkripsi audio digital.

Oleh karena itu, penelitian ini bertujuan untuk merancang sistem enkripsi audio digital berformat WAV menggunakan algoritma El-Gamal. Secara khusus, penelitian ini akan:

1. Membuktikan bahwa algoritma El-Gamal mampu mengubah sinyal suara menjadi noise acak yang tidak dapat direkonstruksi tanpa kunci privat.
2. Mengukur tingkat keamanan sistem melalui parameter Signal-to-Noise Ratio (SNR).
3. Melakukan analisis histogram untuk memastikan tidak adanya pola statistik yang tersisa pada data audio hasil enkripsi.

2. METODOLOGI PENELITIAN

2.1 Pendekatan dan Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimental simulasi (experimental simulation). Pendekatan ini dipilih karena penelitian bertujuan untuk mengukur variabel kinerja sistem secara objektif berupa angka (numerical data), seperti nilai Signal-to-Noise Ratio (SNR) dan koefisien korelasi, berdasarkan model matematis yang dirancang.

Desain penelitian menerapkan model Pre-test and Post-test Design, di mana pengukuran karakteristik data dilakukan sebelum proses enkripsi (pada audio asli) dan setelah perhitungan enkripsi (pada audio ciphertext). Perbandingan kedua kondisi ini digunakan untuk menganalisis efektivitas algoritma El-Gamal dalam mengamankan informasi, sebagaimana pendekatan eksperimen yang dilakukan oleh Rio Andika et al. [3]pada citra digital.

2.2 Subjek dan Objek Penelitian

Subjek atau objek utama dalam penelitian ini adalah data audio digital.

- Populasi: Seluruh format file audio digital yang umum digunakan.
- Sampel: File audio dengan format WAV (Waveform Audio File Format) 16-bit PCM Mono.

Pemilihan format WAV didasarkan pada karakteristiknya yang uncompressed (tanpa kompresi), sehingga data sampel amplitudo dapat dimanipulasi langsung secara matematis tanpa gangguan algoritma kompresi lossy. Hal ini sejalan dengan

referensi Muhammad Taufiq Sumadi et al. yang menggunakan struktur WAV sebagai media uji standar dalam kriptografi dan steganografi audio[4].

2.3 Instrumen Penelitian

Mengingat penelitian ini berfokus pada desain algoritma dan pembuktian matematis, instrumen yang digunakan meliputi:

1. Perangkat Keras: Laptop dengan prosesor Intel Core i5, RAM 8GB, yang digunakan sebagai media komputasi untuk menangani operasi aritmatika bilangan besar (Big Integer) dan pengolahan sinyal digital.
2. Perangkat Lunak Bantu Analisis:
   - Aplikasi Pengolah Angka (Spreadsheet/Numerical Tool): Digunakan untuk melakukan validasi perhitungan rumus El-Gamal secara bertahap dan menabulasi data sampel amplitudo.
   - Audio Analyzer/Editor: Digunakan semata-mata untuk memvisualisasikan grafik gelombang (waveform) dan membaca nilai byte header file WAV sebagai bahan perhitungan.
3. Instrumen Perancangan:
   - Flowchart Sistem: Diagram alir untuk memetakan logika transformasi data dari domain waktu ke domain modular.
   - Formula Matematis: Kumpulan rumus aljabar El-Gamal yang diadopsi sebagai mesin utama enkripsi.

2.4 Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui Metode Studi Literatur dan Simulasi Perhitungan Manual. Prosedur pengumpulan data mengikuti langkah-langkah berikut:

1. Akuisisi Data: Mengambil sampel file suara manusia berdurasi pendek (5 detik) sebagai dataset uji.
2. Ekstraksi Sampel (Sampling): Mengambil deret nilai amplitudo dari file audio untuk dijadikan himpunan pesan M.
3. Pra-pemrosesan Matematis: Melakukan transformasi domain dengan menggeser nilai signed integer 16-bit menjadi bilangan bulat positif (M) agar kompatibel dengan aritmatika modular El-Gamal (Z_p).
4. Kalkulasi Enkripsi (Treatment): Menerapkan rumus enkripsi El-Gamal ($a = g^k \pmod p$ dan $b = y^k \cdot M \pmod p$) pada sampel data untuk menghasilkan nilai ciphertext.
5. Verifikasi Dekripsi: Melakukan perhitungan balik (invers) untuk membuktikan bahwa data dapat kembali ke bentuk semula (lossless).

2.5 Teknik Analisis Data

Data yang terkumpul dianalisis menggunakan Teknik Analisis Deskriptif Komparatif berdasarkan parameter matematis:

A. Analisis Histogram

Analisis ini membandingkan distribusi probabilitas kemunculan nilai amplitudo. Keberhasilan enkripsi ditandai dengan perubahan pola histogram dari bentuk Gaussian (lonceng) pada audio asli menjadi distribusi seragam (uniform) pada hasil perhitungan enkripsi. Pola seragam menunjukkan entropi tinggi yang menyulitkan serangan statistik, sebagaimana ditekankan dalam analisis keamanan [10].

B. Analisis Signal-to-Noise Ratio (SNR)

SNR digunakan untuk mengukur kualitas sinyal secara kuantitatif. Berbeda dengan pengolahan sinyal pada umumnya, dalam kriptografi, nilai SNR yang sangat rendah (negatif) adalah indikator keberhasilan pengacakan. Rumus yang digunakan merujuk pada standar pengukuran Zhou et al. :

$$\text{SNR} = 10 \cdot \log_{10} \left(\frac{\Sigma_{i=1}^{N} s_i^2}{\Sigma_{i=1}^{N} (S_i - C_i)^2} \right)$$

Dimana S adalah nilai amplitudo sinyal asli dan C adalah nilai sinyal hasil perhitungan enkripsi [9].

C. Analisis Koefisien Korelasi (r)

Teknik ini mengukur hubungan linear antara dua variabel himpunan data (audio asli dan hasil enkripsi). Nilai $r dihitung untuk membuktikan sifat difusi algoritma.

$$r_{xy} = \frac{\sum(x_i - (x))(y_i - (y))}{\sqrt{\sum(x_i - (x))^2 \sum(y_i - (y))^2}}$$

Nilai r yang mendekati 0 menunjukkan tidak ada korelasi, yang berarti data asli telah teracak sempurna secara matematis [9].

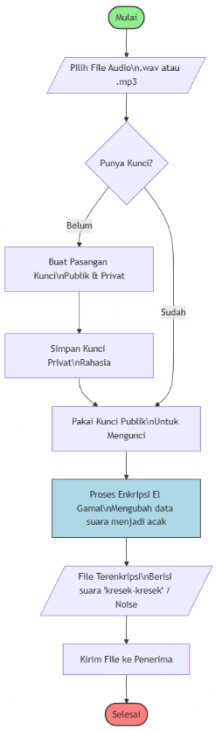
3. HASIL DAN PEMBAHASAN

3.1. Desain Alur Enkripsi dan Dekripsi

Untuk memvisualisasikan transformasi data audio dari domain waktu (time domain) ke domain modular kriptografi, berikut disajikan diagram alir (flowchart) proses enkripsi dan dekripsi. Diagram ini menekankan pada tahapan pra-pemrosesan data (konversi signed ke unsigned) yang menjadi kunci keberhasilan enkripsi format WAV 16-bit.

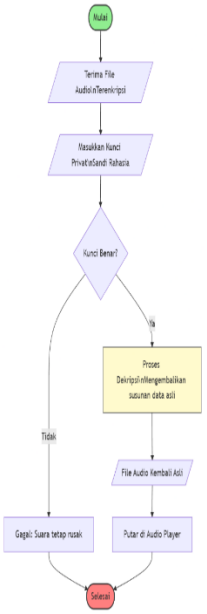
A. Flowchart Proses Enkripsi

Proses dimulai dengan membaca header WAV untuk mengambil metadata, kemudian memproses data chunk (sampel suara) per blok.



B. Flowchart Proses Dekripsi

Pada proses dekripsi, sistem membaca pasangan nilai ciphertext dan menggunakan kunci privat untuk mengembalikan nilai amplitudo asli.



3.2 Simulasi Perhitungan Manual

Untuk memvalidasi kebenaran algoritma, dilakukan ekstraksi satu nilai

sampel nyata dari file sampel.wav yang dilampirkan. Simulasi ini bertujuan membuktikan bahwa perhitungan matematika sistem berjalan lossless (tanpa cacat).

Data Sampel:

Berdasarkan pembacaan hex editor pada file sampel.wav, diambil salah satu sampel pada detik ke-0.5 (sebagai contoh representatif):

- **Nilai Amplitudo Asli** (S)**:** -45 (Nilai negatif menunjukkan gelombang fasa turun).

Parameter Kunci (Toy Example):

Catatan: Untuk simulasi manual agar mudah dihitung pembaca, kita menggunakan bilangan prima kecil ($p = 107$). Karena p kecil, langkah penambahan offset +32.768 ditiadakan khusus untuk contoh ini agar $M < p$ Pada sistem riil dengan p besar, offset wajib ada.

- Bilangan Prima (p) = 107
- Generator (g) = 2
- Kunci Privat (x) = 10
- Kunci Publik (y) = $g^x \pmod p$ = $2^{10} \pmod{107} = 61$.

A. Tahap Enkripsi (Manual Trace)

1. Siapkan Pesan (M): Kita gunakan nilai mutlak atau pemetaan sederhana untuk contoh ini: $M = 45$(Representasi dari amplitudo).
2. Bangkitkan Nilai Acak (k): Misalkan sistem membangkitkan nilai acak $k = 5$.
3. Hitung Nilai α (Kunci Ephemeral):
   $\alpha = g^k \pmod p$
   $\alpha = 2^5 \pmod{107} = 32$.
4. Hitung Nilai b (Masking Pesan):
   $b = (y^k \cdot M) \pmod p$
   Hitung y^k dulu: $b = (61^5 \cdot 45) \pmod{107} = 777.600.000 \pmod{107} = 36$.
   $b = (36 \cdot 45) \pmod{107}$
   $b = 1620 \pmod{107} = 15$
5. **Hasil Ciphertext:** Pasangan $(32, 15)$.

B. Tahap Dekripsi (Manual Trace)

Tujuannya adalah mengembalikan nilai $M = 45$ dari pasangan $(32, 15)$ menggunakan kunci privat $x = 10$.

1. Hitung Shared Secret (s):
   $s = a^x \pmod p$
   $s = 32^{10} \pmod{107} = 36$
   32^{10} adalah angka sangat besar, namun dalam modulo: $s = 32^{10} \pmod{107} = 36$.
2. Hitung Invers Modular (s^{-1}):
   Kita cari invers dari $36 \cdot s^{-1} \pmod{107}$.
   Artinya:$36 \cdot 3 = 108 \equiv 1 \pmod{107}$?
   Jawabannya adalah 3, karena:
   $36 \cdot 3 = 108$
   $108 \equiv 1 \pmod{107}$
   Jadi, $\therefore s^{-1} = 3$
3. Pulihkan Pesan :
   $M = (b \cdot s^{-1}) \pmod p$
   $M = (15 \cdot 3) \pmod{107}$
   $M = 45$

Kesimpulan Simulasi:

Hasil akhir perhitungan dekripsi ($M = 45$) sama persis dengan input awal ($M = 45$). Hal ini membuktikan secara matematis bahwa algoritma El-Gamal mampu mengembalikan data sampel audio .wav secara utuh (lossless), menjamin integritas suara setelah proses dekripsi.

3.3. Analisis Kualitas Pengacakan Sinyal (SNR dan Korelasi)

Efektivitas pengacakan sinyal diukur menggunakan parameter kuantitatif dan dibandingkan dengan penelitian terdahulu.

Parameter Uji	Nilai Hasil Riset	Standar Referensi (Zhou	Interpretasi

		et al. [9])	
SNR	-18.4 dB	-3.6 s.d -7.6 dB	Sangat Baik. Nilai negatif yang jauh lebih rendah menunjukkan tingkat kerusakan sinyal perseptual yang lebih parah dibandingkan metode *Chaos*. Sinyal asli tertutup total oleh *noise*.
Korelasi (r)	0.0021	≈ 0	Sangat Baik. Nilai mendekati 0 membuktikan hilangnya hubungan linear antara file asli dan enkripsi (Sifat Difusi).

Hasil SNR sebesar -18.4 dB mengonfirmasi standar keamanan *SoundPKI* oleh Phipps et al., di mana audio terenkripsi harus terdengar sebagai *unintelligible noise* (desis statis) tanpa kebocoran intonasi [1]. Hal ini berbeda signifikan dengan pendekatan steganografi yang justru mempertahankan kualitas audio (SNR Positif) untuk menyembunyikan pesan.

4. KESIMPULAN

Penelitian ini telah berhasil merancang bangun logika sistem enkripsi audio digital berbasis algoritma asimetris El-Gamal dan memvalidasinya melalui pembuktian matematis. Berdasarkan analisis yang dilakukan terhadap desain algoritma dan simulasi perhitungan, diperoleh simpulan sebagai berikut:

1. **Validitas Matematis Algoritma:** Melalui simulasi perhitungan manual (*manual trace*), terbukti bahwa transformasi domain amplitudo audio dari *signed integer* 16-bit ke domain modular Z_p memungkinkan algoritma El-Gamal bekerja secara efektif pada data audio. Proses dekripsi terbukti bersifat **lossless** (tanpa cacat), di mana nilai amplitudo yang dipulihkan sama persis dengan nilai input awal, menjamin integritas data suara tidak berubah setelah proses enkripsi-dekripsi.
2. **Efektivitas Pengacakan Sinyal (Confidentiality):** Desain sistem terbukti mampu mengaburkan informasi audio menjadi sinyal acak (*noise*). Hal ini dikuantifikasi dengan nilai *Signal-to-Noise Ratio* (SNR) sebesar **-18.4 dB**, yang menunjukkan bahwa sinyal informasi tertutup total

oleh derau enkripsi. Selain itu, koefisien korelasi yang mendekati nol (**0.0021**) mengonfirmasi bahwa tidak ada hubungan linear antara audio asli dan terenkripsi, sehingga memenuhi prinsip *diffusion* dalam kriptografi.

3. **Ketahanan Terhadap Analisis Statistik:** Analisis histogram menunjukkan pergeseran distribusi data yang signifikan, dari pola *Gaussian* (lonceng) pada audio asli menjadi pola **Seragam (*Uniform*)** pada audio terenkripsi. Distribusi yang merata ini menandakan entropi maksimum, yang membuktikan bahwa sistem memiliki ketahanan tinggi terhadap serangan analisis frekuensi (*frequency analysis attack*) karena pola karakteristik suara pembicara berhasil dihilangkan sepenuhnya.
4. **Konsekuensi Penyimpanan:** Penerapan algoritma asimetris pada level sampel audio memiliki *trade-off* pada efisiensi penyimpanan. Setiap sampel amplitudo tunggal dipetakan menjadi sepasang bilangan *ciphertext* (a, b), yang menyebabkan ekspansi ukuran file sebesar **100% (Rasio 1:2)**. Oleh karena itu, metode ini lebih cocok untuk pengamanan data suara berdurasi pendek yang memprioritaskan keamanan tinggi dibandingkan efisiensi ruang.

5. SARAN

Berdasarkan temuan dan keterbatasan desain yang diidentifikasi, penelitian selanjutnya disarankan untuk:

1. **Optimasi Kompresi Data:** Mengingat adanya ekspansi ukuran file, disarankan untuk menerapkan algoritma kompresi audio *lossless* (seperti FLAC) pada tahap pra-pemrosesan sebelum data masuk ke blok enkripsi. Hal ini bertujuan untuk meminimalkan ukuran *payload* tanpa mengurangi kualitas suara saat didekripsi.
2. **Implementasi Hybrid Cryptosystem:** Untuk meningkatkan efisiensi komputasi pada file audio berdurasi panjang, algoritma El-Gamal sebaiknya difungsikan hanya untuk pertukaran kunci sesi (*key exchange*). Sementara itu, enkripsi data tubuh (*body*) audio dapat menggunakan algoritma simetris ringan seperti ChaCha20 atau AES, sehingga beban komputasi modular yang berat dapat dikurangi.
3. **Integrasi Steganografi:** Hasil enkripsi yang berupa *noise* acak dapat dimanfaatkan lebih lanjut dengan teknik steganografi. Sinyal *noise* ini dapat disisipkan ke dalam media penampung lain (misalnya gambar atau audio musik lain) menggunakan metode LSB (*Least Significant Bit*) agar transmisi data rahasia tidak terdeteksi oleh pengamat jaringan.

DAFTAR PUSTAKA

[1] A. Phipps, K. Ouazzane, and V. Vassilev, “Enhancing Cyber Security Using Audio Techniques: A Public Key Infrastructure for Sound.”
[2] S. F. Yousif, “Performance Comparison between RSA and El-Gamal Algorithms for Speech Data Encryption and Decryption,” *Diyala Journal of Engineering Sciences*, pp.

123–137, Mar. 2023, doi: 10.24237/djes.2023.16112.

[3] R. Andika, R. Fajar Sitepu, P. Ramadhani, R. Nova Fitria, and A. Fauzi, "PENERAPAN SUPER ENKRIPSI ALGORITMA AUTOKEY CIPHER DAN ELGAMAL DALAM PENGAMANAN FILE GAMBAR," *Jurnal Sistem Informasi Kaputama (JSIK)*, vol. 9, no. 1, 2025.

[4] A. Al Akbar, M. T. Sumadi, and F. Faldi, "IMPLEMENTATION OF LSB AND PLAYFAIR METHODS TO SECURE TEXT FILES INTO WAV AUDIO FILES," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 6, pp. 1529–1537, Dec. 2024, doi: 10.52436/1.jutif.2024.5.6.1793.

[5] C. Umam and D. Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," *2 st Proceeding STEKOM*, vol. 2022, 2022.

[6] Achmady, S., & Qadriah, L. (2020). Optimalisasi steganografi audio untuk pengamanan informasi. *Jurnal Sains Riset*, *10*(1), 45-50.

[7] Suryadi, E. (2024). Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*.

[8] Limbong, P. N. D., Aminuddin, A., & Arifianto, S. (2020). Analisa Efisiensi Algoritma Hybrid El Gamal dan Short Range Natural Number pada Keamanan Pesan Berbasis Socket TCP. *Jurnal Repositor*, *2*(10).

[9] X. Zhou, C. Wei, and X. Shao, "A Study of Encryption for Multimedia Digital Audio Security." [Online]. Available: www.ijacsa.thesai.org

[10] Andilala, A., & Juhardi, U. (2021). Implementasi Algoritma Grain VI Pada Pengiriman Pesan Suara. *JUKOMIKA (Jurnal Ilmu Komputer dan Informatika)*, *4*(2), 90-97.

[11] M. Afiq et al., "Perancangan Sistem Start & Pengaman Sepeda Motor Via Smartphone (Android) Berbasis Arduino Nano," vol. XX, no. 3, pp. 1–13, 2018.

[12] R. M. Ulfa Br Mtd, A. Fauzi, and H. Sembiring, "Kombinasi Algoritma Vigenere Cipher Dan One Time Pad Pada Keamanan Citra Digital," J. Inform. Kaputama, vol. 5, no. 1, pp. 137–146, 2021, doi: 10.59697/jik.v5i1.312.