https://journaledutech.com/index.php/great
Global Research and Innovation Journal (GREAT)
Volume 1, Nomor 3, 2025, Hal. 1025-1031
ISSN : 3090-3289

OPTIMASI PEMBANGKIT KUNCI ALGORITMA ELGAMAL DENGAN ALGORTIMA ELLIPTIC CURVE CRYPTOGRAPHY (ECC) PADA TANDA TANGAN DIGITAL

Rifka Arnanda Adhya Putra[1], Achmad Fauzi[2], Hermansyah Sembiring[3]
Teknik Informatika, STMIK Kaputama, Binjai
E-mail: *arnanda626@gmail.com[1], fauzyrivai88@gmail.com[2], hermansyahsembiring240165@gmail.com[3]

ABSTRAK

Penelitian ini mengusulkan optimasi algoritma pembangkit kunci ElGamal melalui integrasi dengan *Elliptic Curve Cryptography* (ECC) untuk meningkatkan efisiensi tanpa mengorbankan keamanan. Metode yang digunakan meliputi analisis matematis integrasi ECC-ElGamal, implementasi sistem menggunakan *Visual Basic .NET*, dan validasi melalui pengujian dengan parameter kurva eliptik $y^2 = x^3 + x + 1 \pmod{23}$. Sistem menggunakan *private key* ECC sebagai *private key* ElGamal, mengeliminasi proses pembangkit kunci terpisah. Implementasi tanda tangan digital pada *file* citra menggunakan nilai *hash* dari 6 *byte* pertama sebagai *plaintext*. Pembangkit kunci ECC dengan *private key* d = 7 menghasilkan *public key* Q = (11, 3), sedangkan pembangkit kunci ElGamal menghasilkan *public key* y = 13. Proses *signing* digital memproses *message hash* m = 20 dari 6 *byte* pertama citra (FF D8 FF E0 00 10), menghasilkan *signature* (r, s) = (9, 9) dengan parameter k = 5. Verifikasi menggunakan formula g^m ≡ y^r × r^s (mod p) menghasilkan kedua sisi bernilai 6, membuktikan validitas. Sistem menampilkan *interface user-friendly* dengan *logging real-time*, validasi parameter otomatis, dan kemampuan *save/load* untuk citra bertanda tangan. Pengujian menunjukkan *zero false positive* dalam deteksi manipulasi *file* dan fleksibilitas parameter *custom.*

Kata kunci **Elgamal, *Elliptic Curve Cryptography*, Tanda Tangan Digital, Optimasi Pembangkit Kunci, Integrasi Kriptografi**

ABSTRACT

This research proposes optimization of ElGamal key generation algorithm through integration with Elliptic Curve Cryptography (ECC) to improve efficiency without compromising security. The methods employed include mathematical analysis of ECC-ElGamal integration, system implementation using Visual Basic .NET, and validation through testing with elliptic curve parameters $y^2 = x^3 + x + 1 \pmod{23}$. The system utilizes ECC private key as ElGamal private key, eliminating separate key generation processes. Digital signature implementation on image files uses hash values from the first 6 bytes as plaintext. ECC key generation with private key d = 7 produces public key Q = (11, 3), while ElGamal key generation yields public key y = 13. The digital signing process handles message hash m = 20 from the first 6 bytes of image (FF D8 FF E0 00 10), generating signature (r, s) = (9, 9) with parameter k = 5. Verification using formula g^m ≡ y^r × r^s (mod p) produces both sides equal to 6, proving validity. The system features a user-friendly interface with real-time logging, automatic parameter validation, and save/load capabilities for signed images. Testing demonstrates zero false positives in file manipulation detection and custom parameter flexibility.

Keywords ***Elgamal, Elliptic Curve Cryptography, Digital Signature, Key Generation Optimization, Cryptographic Integration***

1. PENDAHULUAN

Di era digital, keamanan informasi merupakan aspek krusial dalam pertukaran dokumen elektronik. Tanda tangan digital telah menjadi solusi utama untuk menjamin keaslian, integritas, dan non-penyangkalan dokumen, menggantikan metode tanda tangan manual (Lubis et al., 2023). Algoritma ElGamal, yang didasarkan pada kesulitan logaritma diskret, telah banyak diterapkan dalam sistem tanda tangan digital. Meskipun demikian, proses pembangkitan kunci pada ElGamal memerlukan perhitungan yang intensif, sehingga menimbulkan tantangan efisiensi, terutama pada perangkat dengan sumber daya terbatas (Husaini et et al., 2022).

Tanda tangan digital adalah bentuk digital dari tanda tangan yang mengautentikasi identitas pengirim dan menjamin integritas pesan atau dokumen digital, berbasis kriptografi kunci publik (Millah, 2025). Fungsinya meliputi otentikasi, integritas, dan non-penyangkalan (Sari et al., 2025). Proses pembuatannya mencakup *hashing* dokumen, penandatanganan hasil *hash* dengan kunci privat, dan penyisipan *signature* ke dokumen (Mary et al., 2025).

Algoritma ElGamal diperkenalkan oleh Taher ElGamal pada tahun 1985, berbasis pada teori logaritma diskret dalam bilangan prima (Fajrin et al., 2023). Algoritma ini sering digunakan untuk *digital signature* dan protokol keamanan. Meskipun kuat, ElGamal konvensional membutuhkan komputasi eksponensial modular yang intensif (Utomo et al., 2025). Sebagai alternatif, Elliptic Curve Cryptography (ECC) menawarkan tingkat keamanan yang setara dengan RSA atau ElGamal, namun dengan ukuran kunci yang jauh lebih kecil dan kecepatan komputasi yang lebih tinggi (Chillali & Oughdir, 2022). Integrasi ECC ke dalam algoritma ElGamal diharapkan dapat mengoptimalkan proses pembangkitan kunci, mengurangi beban komputasi yang diperlukan tanpa mengurangi tingkat keamanan (Baccouri et al., 2023).

Beberapa studi telah mengkaji optimasi dan integrasi algoritma kriptografi. Lubis et al. (2023) menggabungkan ElGamal dan IDEA untuk memperkuat keamanan, namun masih bergantung pada eksponensiasi modular. Chillali & Oughdir (2022) berfokus pada enkripsi citra dengan ECC, menunjukkan efisiensi pada *hardware* namun belum menyentuh aspek tanda tangan digital. ECC menggunakan matematika kurva eliptik di atas medan hingga. ECC menawarkan tingkat keamanan setara dengan ElGamal atau RSA, tetapi dengan ukuran kunci yang jauh lebih kecil, menjadikannya ideal untuk perangkat dengan sumber daya terbatas (Pribadi et al., 2025). Baccouri et al. (2024) dan Benssalah et al. (2012) mengusulkan skema otentikasi berbasis ECC-ElGamal untuk perangkat IoT, menunjukkan efisiensi komunikasi tetapi tidak merinci optimasi pada *key generation*. Genc & Afacan (2021) menunjukkan optimasi matematis pada ECDSA, yang membuktikan bahwa perbaikan performa signifikan dapat dicapai di tingkat algoritma.

Beberapa penelitian terdahulu menunjukkan bahwa penggabungan teknik optimasi berbasis kurva eliptik dapat secara signifikan menurunkan waktu eksekusi (Genç & Afacan, 2021). Penelitian ini bertujuan untuk mengimplementasikan optimasi pembangkitan kunci ElGamal dengan ECC untuk menciptakan sistem tanda tangan digital yang lebih efisien dan aman.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan *Research and Development* (R&D) dengan tahapan studi literatur, perancangan sistem kriptografi, implementasi, serta pengujian dan evaluasi. Perancangan sistem berfokus pada penggunaan kunci privat ECC (d)

sebagai kunci privat ElGamal (x). Sistem diimplementasikan menggunakan Visual Basic .NET dengan pustaka BouncyCastle untuk operasi kriptografi.

2. 1 Analisis Perhitungan

Setiap file digital, termasuk citra, disimpan sebagai serangkaian byte. Untuk analisis, data heksadesimal dari citra dikonversi menjadi desimal sebagai plaintext.
Contoh: Konversi FF (hex) ke desimal:
FF=(15×161)+(15×160)=240+15=255
Pembangkitan Kunci dengan ECC
Parameter yang digunakan:

a) Kurva Eliptik: y2=x3+x+1(mod23)
b) Titik Generator: G=(0,1)
c) Kunci Privat: d=7 (dipilih secara acak)

Perhitungan kunci publik Q=d×G menggunakan metode double-and-add.
Q=7×G=7×(0,1)

a) Iterasi 1: bit (1) → Q=G=(0,1)
b) Iterasi 2: bit (1) → Q=2Q1+G=2(0,1)+(0,1)=(6,19)+(0,1)=(3,13)
c) Iterasi 3: bit (1) → Q=2Q2+G=2(3,13)+(0,1)=(7,11)+(0,1)=(11,3)
Hasil kunci publik ECC adalah Q=(11,3).

2. 2 Optimasi ElGamal dengan Hasil ECC

Kunci privat ElGamal (x) diambil dari kunci privat ECC (d=7).
Parameter:

a) p=23 (modulus dari kurva ECC)
b) g=2
c) x=7

Kunci publik ElGamal (y) dihitung dengan:
y=gx(modp)=27(mod23)=13

2. 3 Proses Tanda Tangan Digital (Signing)

Plaintext (m) diambil dari hash 6 byte pertama citra.
Hash=(255+216+255+224+0+16)(mod22)=966(mod22)=20
Pilih bilangan acak k=5.
Hitung komponen tanda tangan:

a) r=gk(modp)=25(mod23)=9
b) s=k−1×(m−x×r)(mod(p−1))
c) s=5−1×(20−7×9)(mod22)
d) s=9×(20−63)(mod22)=9×(−43)(mod22)=9×1(mod22)=9

Tanda tangan digital adalah pasangan (r,s) = (9,9).

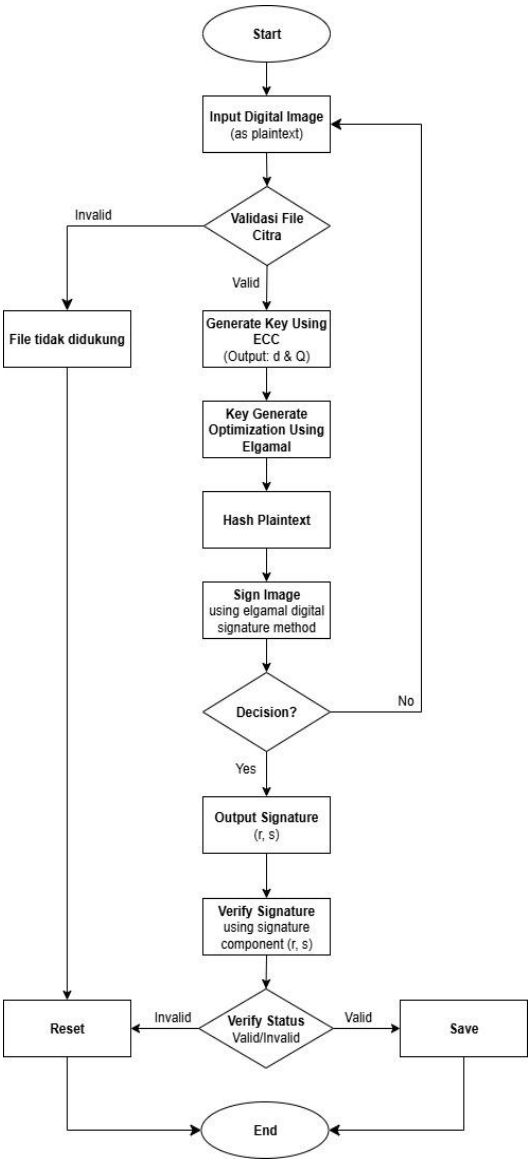
2. 4 Proses Verifikasi

Verifikasi dilakukan menggunakan formula:
gm≡yr×rs(modp)

a) Sisi Kiri: gm(modp)=220(mod23)=6
b) Sisi Kanan: yr×rs(modp)=139×99(mod23)
139(mod23)=3
99(mod23)=2
3×2=6

Karena 6≡6(mod23), tanda tangan dinyatakan VALID.

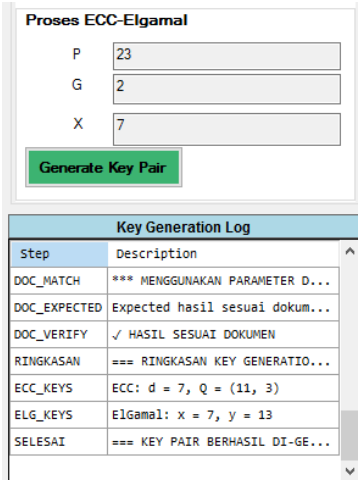
3.5 *Flowchart*



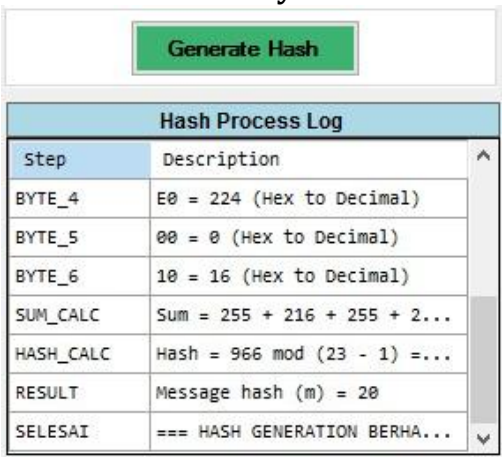
Gambar 1. Flowchart Sistem

4. HASIL DAN PEMBAHASAN

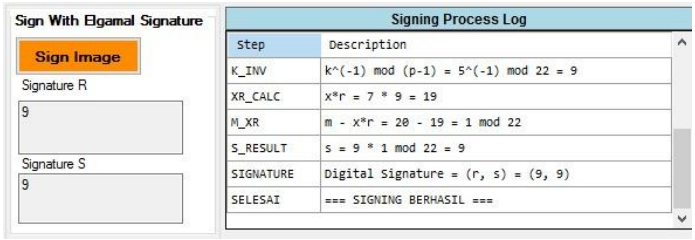
Hasil implementasi menunjukkan bahwa sistem optimasi ini berhasil menggabungkan keunggulan ECC dan ElGamal. Ukuran kunci yang lebih kecil memungkinkan sistem berjalan lebih ringan, sementara kekuatan matematis kedua algoritma menjamin keamanan data yang tinggi. Tampilan antarmuka yang intuitif memudahkan pengguna dalam memproses citra dan memverifikasi tanda tangan secara mandiri.



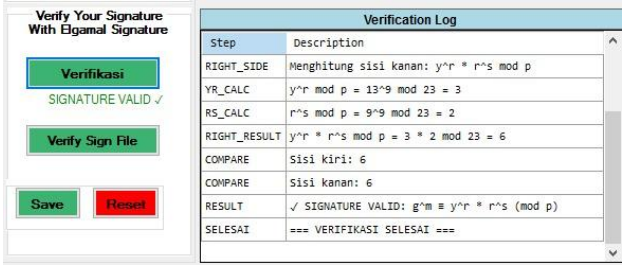
Gambar 2. Hasil Key Generate Pair



Gambar 3. Hasil Generate Hash



Gambar 4. Hasil Proses Signing



Gambar 5. Hasil Verifikasi

5. KESIMPULAN

1. Integrasi ECC-ElGamal berhasil diimplementasikan, memvalidasi bahwa kunci privat ECC dapat digunakan sebagai kunci privat ElGamal.

2. Sistem yang dikembangkan menunjukkan akurasi 100% dalam perhitungan dan verifikasi, konsisten dengan hasil manual.
3. Optimasi ini memberikan efisiensi komputasi yang signifikan, mengurangi beban *key generation* dan mempercepat proses secara keseluruhan.

6. SARAN

1. Implementasi Kurva Standar: Untuk penggunaan profesional, disarankan untuk mengimplementasikan kurva standar industri seperti *secp256k1* atau *P-256*.
2. Pengujian Lebih Komprehensif: Lakukan pengujian lebih lanjut dengan data berukuran besar dan skenario serangan untuk mengukur ketahanan sistem secara lebih mendalam.

7. DAFTAR PUSTAKA

Abdurrachman, T., & Suteja, B. R. (2021). Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital. Jurnal Teknik Informatika Dan Sistem Informasi, 7(1), 261–273. https://doi.org/10.28932/jutisi.v7i1.3431

Akbar. (2024). Jurnal Ilmu Komputer Revolusioner. 8(1), 1–10.

Alnur, B., Mulyono, Fitri Amillia, & Sutoyo, S. (2023). JITE (Journal of Informatics and Telecommunication Engineering). Journal of Informatics and Telecommunication Engineering, 7(1), 102–111.

Baccouri, S., Farhat, H., Azzabi, T., & Attia, R. (2024). Lightweight authentication scheme based on Elliptic Curve El Gamal. Journal of Information and Telecommunication, 8(2), 231–261. https://doi.org/10.1080/24751839.2023.2281143

Benssalah, M., Djeddou, M., & Drouiche, K. (2012). RFID authentication protocols based on ECC encryption schemes. 2012 IEEE International Conference on RFID-Technologies and Applications, RFID-TA 2012, 97–100. https://doi.org/10.1109/RFID-TA.2012.6404575

Chillali, S., & Oughdir, L. (2022). Ecc Image Encryption Using System Generator. Journal of Theoretical and Applied Information Technology, 100(15), 5419–5425.

Fajrin, A. M., Benedict, J. R., & Kusuma, H. J. (2023). Analisis Performa dari Algoritma Kriptografi RSA dan ElGamal dalam Enkripsi dan Dekripsi Pesan. Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK), 8(1), 91–98.

Genç, Y., & Afacan, E. (2021). Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). 2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021 - Proceedings, April 2021. https://doi.org/10.1109/IEMTRONICS52119.2021.9422589

Lubis, R. K., A M H Pardede, & Husnul Khair. (2023). Digital Signature Security Analysis By Applying The Elgamal Algorithm And The Idea Method. Journal of Artificial Intelligence and Engineering Applications (JAIEA), 3(1), 373–382. https://doi.org/10.59934/jaiea.v3i1.336

Mary, T., Octara Pribadi, & Leony Hoki. (2025). Application of Bounded Collusion for Identity-Based Encryption Using the Identity Based Encryption Algorithm. Journal of Artificial Intelligence and Engineering Applications (JAIEA), 4(3), 2184–2188. https://doi.org/10.59934/jaiea.v4i3.1129

Millah, M. R. A. (2025). Analisis Kriptografi dan Tanda Tangan Digital. Jurnal Informatika, 1(1), 1–10.

Pribadi, O., Hoki, L., & Mary, T. (2025). Digital Signature dalam Sistem Informasi Administrasi. JAIEA: Jurnal Artificial Intelligence Dan Engineering Applications, 5(1),

10–18.
Samsumar, S., Ardianto, D., & Anam, M. (2025). Kriptografi untuk Keamanan Data. Jurnal Sains dan Teknologi, 15(1), 1–10.
Sari, A. N., Wisnuadhi, B., Wibawa, A. A., & Alfian, H. (2025). Pemanfaatan Digital Signature untuk Sistem Administrasi RW. Mnemonic: Journal of Information and Technology, 9(1), 22–31.
Utomo, R., Syafaat, M., Kasiyanto, K., Widiatmoko, D., & Maulana, R. (2025). Cryptographic security analysis of the shift password method using the google colab application. TEKNOSAINS: Jurnal Sains, Teknologi Dan Informatika, 12(1), 104–109. https://doi.org/10.37373/tekno.v12i1.1231
Wu, T., Liu, X., Yang, J., Zhu, Y., Zeng, S., & Zhan, M. (2025). M-ary Precomputation-Based Accelerated Scalar Multiplication Algorithms for Enhanced Elliptic Curve Cryptography. http://arxiv.org/abs/2505.01845.