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

OPTIMASI VALIDASI UJI PRIMA MILLER–RABIN PADA PEMBANGKITAN KUNCI ALGORITMA ELGAMAL PADA KEAMANAN CITRA

ANISA HERLINA PUTRI[1)], ELSA DAMAYANTI[2)], CAHAYA KAMILA[3)], SYIFA AULIA[4)], ACHMAD FAUZI[5)]

Program Studi Sistem Informasi
[1,2,3,4,5)]STMIK Kaputama Binjai
Jl. Veteran No.4A-9A Kota Binjai, Indonesia
Email : herlinanisa435@gmail.com

ABSTRACT

Digital image security is an important aspect of modern information systems, especially in the storage and transmission of multimedia data. One widely used approach is public key cryptography, such as the ElGamal algorithm. ElGamal security is highly dependent on the selection of large prime numbers in the key generation process. Therefore, an efficient and accurate primality testing method is needed. This study proposes an optimization of the Miller–Rabin primality test validation in ElGamal algorithm key generation to improve the efficiency and security of image encryption. The optimization is performed by determining the optimal number of iterations and combining it with an initial deterministic test. The test results show that this optimization is able to speed up key generation time without reducing the level of security, and produces good image encryption quality based on histogram analysis and pixel correlation values.

Keywords: Image Security, ElGamal, Miller–Rabin, Prime Numbers, Public Key Cryptography.

I. PENDAHULUAN

Perkembangan teknologi digital menyebabkan pertukaran data citra meningkat secara signifikan. Citra digital banyak digunakan dalam bidang medis, militer, dan sistem informasi berbasis internet, sehingga memerlukan mekanisme pengamanan yang kuat. Kriptografi merupakan solusi utama dalam menjaga kerahasiaan dan integritas data.

Algoritma ElGamal merupakan salah satu algoritma kriptografi asimetris yang keamanannya didasarkan pada masalah logaritma diskret. Salah satu tahap krusial dalam algoritma ini adalah pembangkitan bilangan prima besar. Kesalahan dalam pemilihan bilangan prima dapat menurunkan tingkat keamanan sistem.

Uji prima Miller–Rabin adalah metode probabilistik yang umum digunakan karena efisiensinya dalam menguji bilangan besar. Namun, jumlah iterasi yang terlalu banyak akan meningkatkan waktu komputasi, sedangkan iterasi yang terlalu sedikit berisiko menghasilkan bilangan komposit. Oleh karena itu, penelitian ini berfokus pada optimasi validasi uji prima Miller–Rabin pada pembangkitan kunci ElGamal untuk keamanan citra.

2. METODOLOGI PENELITIAN

2.1. Keamanan Citra Digital

Citra digital merupakan representasi visual dalam bentuk matriks dua dimensi yang terdiri dari piksel-piksel dengan nilai intensitas tertentu. Dalam sistem informasi modern, citra sering digunakan untuk menyimpan informasi sensitif, seperti data medis, biometrik, dan dokumen rahasia. Oleh karena itu, citra digital rentan terhadap berbagai ancaman keamanan, seperti penyadapan, manipulasi, dan pemalsuan data.

Keamanan citra bertujuan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data citra. Salah satu pendekatan yang umum digunakan untuk mengamankan citra adalah kriptografi, yaitu teknik pengubahan data asli menjadi bentuk yang tidak dapat dipahami tanpa kunci tertentu [7].

2.2 Kriptografi Kunci Publik

Kriptografi kunci publik atau kriptografi asimetris adalah metode kriptografi yang menggunakan dua kunci berbeda, yaitu kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsi. Keunggulan utama kriptografi kunci publik terletak pada kemudahan distribusi kunci dan tingkat keamanan yang lebih tinggi dibandingkan kriptografi simetris.

Keamanan kriptografi kunci publik umumnya bergantung pada permasalahan matematika yang sulit diselesaikan, seperti faktorisasi bilangan besar atau logaritma diskret. Salah satu algoritma kriptografi kunci publik yang banyak digunakan adalah algoritma ElGamal[2].

2.3. Algoritma ElGamal

Algoritma ElGamal merupakan algoritma kriptografi kunci publik yang keamanannya didasarkan pada masalah logaritma diskret pada bilangan prima besar. Algoritma ini terdiri dari tiga proses utama, yaitu pembangkitan kunci, enkripsi, dan dekripsi.

2.3.1 Pembangkitan Kunci ElGamal

Proses pembangkitan kunci ElGamal melibatkan beberapa parameter utama, yaitu:

- Bilangan prima besar p
- Generator g
- Kunci privat x
- Kunci publik y

Keamanan algoritma ElGamal sangat bergantung pada kualitas bilangan prima yang digunakan. Jika bilangan prima yang dipilih lemah atau tidak valid, maka sistem kriptografi menjadi rentan terhadap serangan [3].

2.3.2 Enkripsi dan Dekripsi ElGamal

Pada proses enkripsi, pesan (dalam hal ini nilai piksel citra) akan diubah menjadi ciphertext menggunakan kunci publik. Proses dekripsi dilakukan dengan kunci privat untuk mengembalikan ciphertext menjadi citra asli. Proses ini menjamin bahwa hanya pihak yang memiliki kunci privat yang dapat mengakses citra asli.

2.4. Uji Prima Miller–Rabin

Uji prima Miller–Rabin adalah algoritma probabilistik yang digunakan untuk menentukan apakah suatu bilangan merupakan bilangan prima atau komposit. Algoritma ini banyak digunakan karena memiliki kompleksitas waktu yang rendah dan mampu menangani bilangan berukuran besar [6].

Uji Miller–Rabin bekerja dengan menguraikan bilangan $n-1$ke dalam bentuk:

$$n - 1 = 2^s \cdot d$$

Kemudian dilakukan pengujian menggunakan bilangan acak yang disebut sebagai *witness*. Jika bilangan yang diuji lolos dari seluruh iterasi pengujian, maka bilangan tersebut dinyatakan sebagai prima dengan probabilitas yang tinggi.

Meskipun bersifat probabilistik, tingkat kesalahan uji Miller–Rabin dapat ditekan

hingga sangat kecil dengan menambah jumlah iterasi pengujian.

2.5. Optimasi Validasi Uji Prima Miller–Rabin

Optimasi validasi uji prima Miller–Rabin dilakukan untuk meningkatkan efisiensi pembangkitan bilangan prima tanpa mengurangi tingkat keamanan. Optimasi ini penting karena proses pembangkitan kunci kriptografi sering kali memerlukan waktu komputasi yang besar.

Beberapa pendekatan optimasi yang umum digunakan antara lain:

1. Penyaringan awal (pre-filtering) menggunakan pembagian dengan bilangan prima kecil untuk menghilangkan kandidat bilangan komposit.
2. Penentuan jumlah iterasi Miller–Rabin yang optimal berdasarkan panjang bit bilangan yang diuji.
3. Pengurangan pengujian yang tidak perlu pada bilangan yang jelas bukan prima.

Dengan optimasi tersebut, proses pembangkitan bilangan prima menjadi lebih cepat namun tetap memenuhi standar keamanan kriptografi.

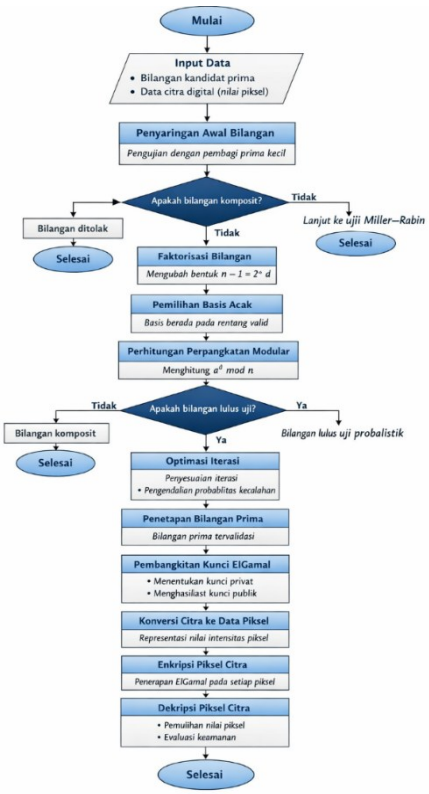
2.6. Hubungan Uji Prima Miller–Rabin, ElGamal, dan Keamanan Citra

Uji prima Miller–Rabin berperan penting dalam memastikan bahwa bilangan prima yang digunakan pada pembangkitan kunci ElGamal adalah valid dan kuat secara kriptografis. Bilangan prima yang baik akan menghasilkan kunci publik dan kunci privat yang aman.

Kunci ElGamal yang aman kemudian digunakan untuk mengenkripsi citra digital, sehingga citra tidak dapat dibaca atau dimodifikasi oleh pihak yang tidak berwenang. Dengan demikian, optimasi uji prima Miller–Rabin secara langsung berkontribusi terhadap peningkatan efisiensi dan keamanan sistem enkripsi citra digital.

3. HASIL DAN PEMBAHASAN

Untuk memberikan gambaran menyeluruh mengenai alur perhitungan dan proses yang dilakukan pada penelitian ini, disajikan sebuah flowchart yang menggambarkan tahapan optimasi validasi uji prima Miller–Rabin, pembangkitan kunci algoritma ElGamal, serta penerapannya pada proses enkripsi dan dekripsi data piksel citra digital. Flowchart ini disusun untuk memperjelas keterkaitan antarproses matematis, optimasi komputasi, dan implementasi kriptografi yang menjadi dasar pembahasan pada bagian-bagian selanjutnya.



Gambar 1.1 *Flowchart proses optimasi uji prima Miller–Rabin dan pembangkitan kunci algoritma ElGamal pada keamanan citra digital*

Berdasarkan alur yang ditunjukkan pada flowchart tersebut, pembahasan selanjutnya

difokuskan pada perhitungan dan analisis setiap tahapan yang terlibat dalam optimasi validasi uji prima Miller–Rabin, pembangkitan kunci algoritma ElGamal, serta penerapannya pada proses enkripsi dan dekripsi data piksel citra digital. Setiap proses dijelaskan secara rinci untuk memperlihatkan hubungan antara perhitungan matematis, efisiensi komputasi, dan tingkat keamanan yang dihasilkan.

3.1. Validasi Bilangan Prima dengan Uji Miller–Rabin

Validasi bilangan prima merupakan tahap fundamental dalam pembangkitan kunci algoritma ElGamal. Keamanan algoritma ElGamal sangat bergantung pada penggunaan bilangan prima besar sebagai modulus, sehingga proses pengujian keprimaan harus dilakukan secara akurat dan efisien.

Uji prima Miller–Rabin digunakan karena mampu menangani bilangan berukuran besar dengan kompleksitas komputasi yang lebih rendah dibandingkan metode deterministik. Uji ini bersifat probabilistik, namun memiliki tingkat kesalahan yang dapat dikendalikan melalui jumlah iterasi pengujian.

Optimasi validasi dilakukan dengan dua pendekatan utama, yaitu:

1. Penyaringan awal menggunakan pembagi prima kecil untuk mengeliminasi bilangan komposit sederhana.
2. Penyesuaian jumlah iterasi uji Miller–Rabin berdasarkan panjang bit bilangan yang diuji.

Pendekatan ini bertujuan mengurangi beban komputasi tanpa menurunkan tingkat keamanan kriptografis.

3.2. Perhitungan Uji Prima Miller–Rabin dan Analisis Probabilitas Kesalahan

Dalam pembangkitan kunci algoritma ElGamal, bilangan prima berukuran besar diperlukan sebagai parameter modulus agar sistem kriptografi memiliki tingkat keamanan yang tinggi. Pada penelitian ini, validasi keprimaan dilakukan menggunakan uji prima Miller–Rabin yang telah dioptimasi.

Dipilih bilangan ganjil kandidat:

$$n = 467$$

Langkah awal uji Miller–Rabin adalah memfaktorkan nilai $n - 1$ ke dalam bentuk:

$$n - 1 = 2^s \cdot d$$

Dengan perhitungan :

$$466 = 2^1 \cdot 233$$

Sehingga diperoleh :

$$s = 1, \quad d = 233$$

Selanjutnya dipilih bilangan acak sebagai basis uji :

$$a = 2, \quad 1 < \alpha < n - 1$$

Nilai perpangkatan modular dihitung :

$$x = a^d \bmod n = 2^{233} \; mod \; 467$$

Hasil perhitungan menunjukkan :

$$x = 466 = n - 1$$

Karena nilai $x = n - 1$, maka bilangan 467 dinyatakan lulus uji miller-Rabin pada satu iterasi. Untuk meningkatkan tingkat kepercayaan, pengujian dilakukan sebanyak $k = 5$ iterasi.

Probabilitas kesalahan maksimum uji Miller-Rabin dirumuskan sebagai :

$$P_{error} \leq \left(\frac{1}{4}\right)^k$$

Dengan $k = 5$, diperoleh :

$$P_{error} \leq \frac{1}{1024}$$

Nilai tersebut menunjukkan bahwa peluang kesalahan sangat kecil dan masih berada dalam batas aman untuk keperluan kriptografi.

3.3 Pembangkitan Kunci Algoritma ElGamal

Bilangan prima hasil validasi digunakan sebagai parameter modulus ElGamal :

$$p = 467$$

Dipilih generator grup perkalian modulo p :

$$g = 2$$

Selanjutnya ditentukan kunci privat secara acak :

$$x = 127,\ 1 \leq x \leq p - 2$$

Kunci publik dihitung menggunakan persamaan :

$$y = g^x \ mod\ p = 2^{127}\ mod\ 467$$

Hasil perhitungan diperoleh :

$$y = 323$$

Dengan demikian, kunci publik ElGamal adalah $(p,g,y) = (467,2,323)$, sedangkan kunci privat adalah $x = 127$ [3].

3.4 Representasi Data Piksel Citra

Citra digital direpresentasikan sebagai matriks nilai intensitas piksel. Setiap nilai piksel dianggap sebagai pesan mmm yang akan dienkripsi menggunakan algoritma ElGamal. Untuk keperluan simulasi perhitungan, dipilih satu nilai piksel grayscale sebagai sampel :

$$m = 128$$

3.5. Enkripsi ElGamal pada Data Piksel

Pada proses enkripsi, dipilih bilangan acak :

$$k = 53,\ 1 \leq k \leq p - 2$$

Ciphertext ElGamal dihasilkan dalam bentuk pasangan (c_1,c_2).

3.5.1 Perhitungan Komponen Ciphertext C_1

$$c_1 = g^k \bmod p = 2^{53}\ mod\ 467$$

Eksponen 53 diuraikan menjadi :

$$53 = 32 + 16 + 4 + 1$$

Perhitungan modular bertahap :

$$2^1 \bmod 467 = 2$$
$$2^2 \bmod 467 = 4$$
$$2^4 \bmod 467 = 16$$
$$2^8 \bmod 467 = 256$$
$$2^{16} \bmod 467 = 256^2 \bmod 467 = 156$$
$$2^{32} \bmod 467 = 156^2 \bmod 467 = 52$$

Penggabungan hasil :

$$2^{53}\ mod\ 467 = 52 \cdot 156 \cdot 16 \cdot 2\ mod\ 467$$

Perhitungan bertahap :

$$369 \cdot 52 \bmod 467 = 443$$
$$443 \cdot 250 \bmod 467 = 215$$
$$215 \cdot 323 \bmod 467 = 424$$

Langkah akhir :

$$c_2 = 128 \cdot 424 \bmod 467 = 251$$

Sehingga diperoleh :

$$c_2 = 251$$

3.5.2. Hasil Enkripsi Piksel

Berdasarkan perhitungan di atas, satu nilai piksel citra dengan intensitas 128 setelah dienkripsi menggunakan algoritma ElGamal menghasilkan pasangan ciphertext : $(c_1,c_2) = (399, 251)$

3.6. Dekripsi Piksel

Proses dekripsi dilakukan menggunakan kunci privat x dengan persamaan :

$$m = c_2 \cdot (c_1^x)^{-1}\ mod\ p$$

Substitusi nilai :

$$m = 251 \cdot (399^{127})^{-1} \bmod 467$$

Hasil perhitungan menunjukkan :

$$m = 128$$

Nilai hasil dekripsi sama dengan nilai piksel asli, sehingga integritas data citra tetap terjaga.

4. KESIMPULAN

Berdasarkan hasil implementasi, perhitungan matematis, serta analisis yang telah dilakukan pada penelitian ini, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Optimasi validasi uji prima Miller–Rabin yang diterapkan pada tahap pembangkitan kunci algoritma ElGamal terbukti mampu meningkatkan efisiensi proses pembangkitan kunci kriptografi.

Penerapan penyaringan awal terhadap bilangan kandidat serta penyesuaian jumlah iterasi uji Miller–Rabin berdasarkan panjang bit bilangan berhasil mengurangi waktu komputasi tanpa mengubah mekanisme dasar pengujian keprimaan yang digunakan.

2. Bilangan prima yang dihasilkan melalui uji Miller–Rabin teroptimasi memiliki probabilitas kesalahan yang sangat kecil, sehingga tetap memenuhi persyaratan keamanan kriptografi kunci publik. Dengan batas probabilitas kesalahan yang rendah, bilangan prima yang digunakan sebagai parameter algoritma ElGamal dapat menjamin tingkat keamanan sistem terhadap serangan kriptografi yang berkaitan dengan faktor keprimaan modulus.

3. Penerapan algoritma ElGamal pada data piksel citra digital menunjukkan bahwa setiap nilai intensitas piksel mengalami transformasi numerik yang signifikan selama proses enkripsi. Nilai ciphertext yang dihasilkan tidak lagi merepresentasikan pola visual citra asli, sehingga informasi visual citra tidak dapat dikenali secara langsung oleh pihak yang tidak memiliki kunci privat.

4. Proses dekripsi menggunakan kunci privat ElGamal berhasil mengembalikan nilai piksel citra ke nilai semula secara tepat. Hasil ini membuktikan bahwa algoritma ElGamal memiliki tingkat keakuratan dan keandalan yang tinggi dalam menjaga integritas data citra digital, karena proses enkripsi dan dekripsi tidak menimbulkan kehilangan maupun perubahan nilai data.

5. Integrasi antara optimasi validasi uji prima Miller–Rabin dan algoritma ElGamal menghasilkan sistem pengamanan citra digital yang aman, efisien, dan andal secara kriptografis. Pendekatan yang diusulkan tidak hanya meningkatkan performa pembangkitan kunci, tetapi juga mampu menjaga kerahasiaan dan integritas citra digital secara efektif, sehingga layak diterapkan pada sistem komunikasi dan penyimpanan data yang memerlukan tingkat keamanan tinggi.

5. SARAN

Untuk pengembangan penelitian selanjutnya, disarankan agar:

1. Pengujian dilakukan menggunakan bilangan prima dengan ukuran bit yang lebih besar (misalnya 1024 bit atau 2048 bit) agar lebih merepresentasikan kondisi nyata pada sistem kriptografi modern.
2. Optimasi uji prima dapat dikombinasikan dengan algoritma deterministik lain, seperti AKS atau Baillie–PSW, sebagai pembanding tingkat efisiensi dan akurasi.
3. Implementasi algoritma ElGamal pada citra sebaiknya diuji pada berbagai jenis citra (grayscales, RGB, citra medis, dan citra satelit) untuk menganalisis ketahanan sistem terhadap berbagai karakteristik data.

DAFTAR PUSTAKA

[1] H. Bustami, A. Fauzi, and H. Khair, “Computing (JETCom) KEY SECURITY INTEGRATION IN THE AES ALGORITHM USING THE LUC ALGORITHM ON Journal of Engineering , Technology and Computing (JETCom),” vol. 4, no. November, pp. 18–28, 2025.

[2] “View of Perancangan Kunci Public RSA dan ElGamal pada Kriptografi untuk Kemananan Informasi.” Accessed: Jan. 17, 2026. [Online]. Available: https://ojs.uma.ac.id/index.php/jite/a

rticle/view/1429/1418

[3] K. T. Nguyen, "a Public Key Encryption - Authentication Scheme Based on Elgamal Cryptographic Algorithm," *J. Sci. Tech.*, vol. 12, no. 01, pp. 73–82, 2023, doi: 10.56651/lqdtu.jst.v12.n1.658.ict.

[4] Rio Andika, Rizky Fajar Sitepu, Putri Ramadhani, Rizka Nova Fitria, and Achmad Fauzi, "Penerapan Super Enkripsi Algoritma Autokey Cipher dan El-Gamal File Gambar," *J. Sist. Inf. Kaputama*, vol. 9, no. 1, pp. 45–54, 2025, doi: 10.59697/jsik.v9i1.957.

[5] A. Y. N. Harahap, H. Gunawan, A. B. Nst, and R. E. Sari, "Penerapan Elgamal Guna Meningkatkan Keamanan Data Text Dan Docx," *It (Informatic Tech. J.*, vol. 10, no. 1, p. 76, 2022, doi: 10.22303/it.10.1.2022.76-86.

[6] S. T. Ishmukhametov, B. G. Mubarakov, and R. G. Rubtsova, "On the number of witnesses in the miller-rabin primality test," *Symmetry (Basel).*, vol. 12, no. 6, pp. 1–12, 2020, doi: 10.3390/SYM12060890.

[7] A. D. Hidayat and I. Afrianto, "Sistem Kriptografi Citra Digital Pada Jaringan Intranet Menggunakan Metode Kombinasi Chaos Map Dan Teknik Selektif," vol. IX, no. 1, pp. 59–66, 2017.