Jurnal Elektronik Ilmu Komputer Udayana
Volume 14, No 2. November 2025

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Pengamanan Pesan Menggunakan Algoritma ElGamal dengan Public Key Infrastructure Berbasis Website

Gary Melvin Lie[a1], Luh Gede Astuti[a2], I Gusti Ngurah Anom Cahyadi Putra[a3], Ida Ayu Gde Suwiprabayanti Putra[a4]

[a]Teknik Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jl. Kampus Bukit Jimbaran Computer Science Building Jurusan Ilmu Komputer, Jimbaran, Badung, Badung Regency, Bali 80361, Indonesia
[1]garymelvinlie@gmail.com
[2]lg.astuti@unud.ac.id
[3]anom.cp@unud.ac.id
[4]iagsuwiprabayantiputra@unud.ac.id

Abstract

In today's digital era, ensuring the security of data and messages is crucial. Sensitive information transmitted over the internet is vulnerable to interception and manipulation by unauthorized parties. This study implements the elgamal cryptographic algorithm in combination with a public key infrastructure (PKI) to secure message exchanges over a web-based platform. The system enables users to perform end-to-end encryption and decryption, ensuring that only authorized recipients can access the messages. The developed website supports key generation, message encryption and decryption, and digital certificate management. Security testing was carried out using black box testing and penetration tests, including SQL Injection and cross-site scripting (XSS). The evaluation results show that the system effectively maintains message confidentiality and performs encryption and decryption accurately.

Keywords: *Cryptography, ElGamal, PKI, Message Security, Web Application, Encryption, Digital Certificate*

1. Pendahuluan

Di era digital saat ini, kebutuhan akan pengamanan informasi menjadi semakin krusial seiring meningkatnya pertukaran data melalui jaringan terbuka seperti internet. Pesan yang dikirim melalui aplikasi web sering kali mengandung informasi sensitif, mulai dari data pribadi hingga rahasia perusahaan, yang sangat rentan terhadap penyadapan, pemalsuan, maupun modifikasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan suatu sistem yang mampu menjamin kerahasiaan, integritas, dan autentikasi pesan.

Salah satu solusi yang umum digunakan dalam pengamanan komunikasi digital adalah penerapan kriptografi. Public Key Infrastructure (PKI) merupakan infrastruktur yang mendukung sistem kriptografi kunci publik untuk mengelola distribusi kunci dan sertifikat digital. PKI memastikan bahwa identitas pihak yang terlibat dalam komunikasi dapat dipercaya melalui verifikasi sertifikat digital. Sementara itu, algoritma kriptografi ElGamal digunakan sebagai metode enkripsi asimetris yang mampu menyediakan keamanan probabilistik, serta mendukung penerapan tanda tangan digital dan pertukaran kunci rahasia.

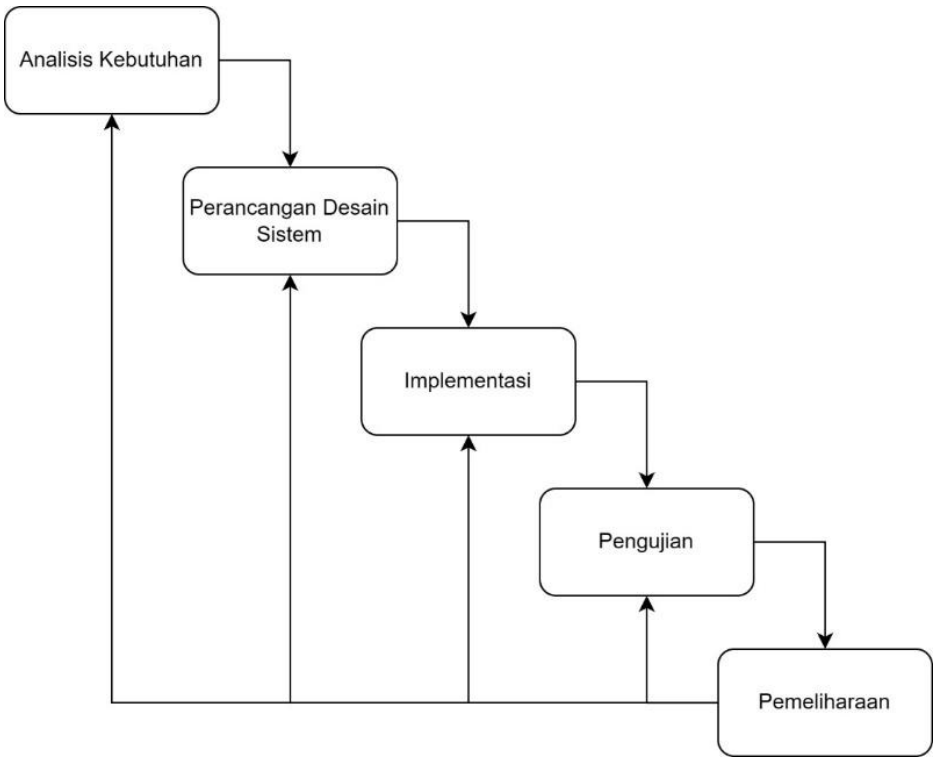
Penelitian ini bertujuan untuk mengembangkan aplikasi web yang mampu mengamankan pertukaran pesan dengan menggabungkan algoritma ElGamal dan PKI. Dalam sistem ini, setiap pesan akan dienkripsi menggunakan kunci publik penerima yang telah tervalidasi melalui sertifikat digital, dan hanya dapat didekripsi menggunakan kunci privat yang sah. Dengan pendekatan ini, pesan yang dikirim akan terlindungi dari akses pihak ketiga yang tidak berwenang.

Beberapa penelitian sebelumnya telah mengkaji implementasi kriptografi pada pengamanan pesan berbasis web, seperti penggunaan algoritma RSA pada sistem email terenkripsi [1] atau kombinasi algoritma Vigenere dan ElGamal untuk enkripsi dokumen digital [2]. Namun, penelitian-penelitian tersebut belum menyajikan integrasi langsung antara PKI dan ElGamal dalam lingkungan website yang user-friendly serta tidak mendukung proses validasi sertifikat secara otomatis. Pada penelitian ini menekankan pada integrasi PKI dan ElGamal secara langsung dalam lingkungan website dengan antarmuka pengguna yang mudah diakses dan berfokus pada kemudahan validasi sertifikat serta proses enkripsi secara otomatis.

Struktur artikel ini disusun sebagai berikut: bagian kedua menjelaskan metode penelitian dan perancangan sistem, bagian ketiga memaparkan hasil implementasi dan pengujian, dan bagian keempat berisi kesimpulan serta saran untuk pengembangan sistem ke depan.

2. Metode Penelitian

Penelitian ini akan menggunakan metode waterfall. Metode penelitian ini menjelaskan pengembangan perangkat lunak yang bersifat linear dan terstruktur, di mana setiap tahap harus diselesaikan sepenuhnya sebelum melanjutkan ke tahap berikutnya [3]. Gambaran dari langkah-langkah yang akan dilakukan dalam penelitian ini terdapat pada Gambar 1.

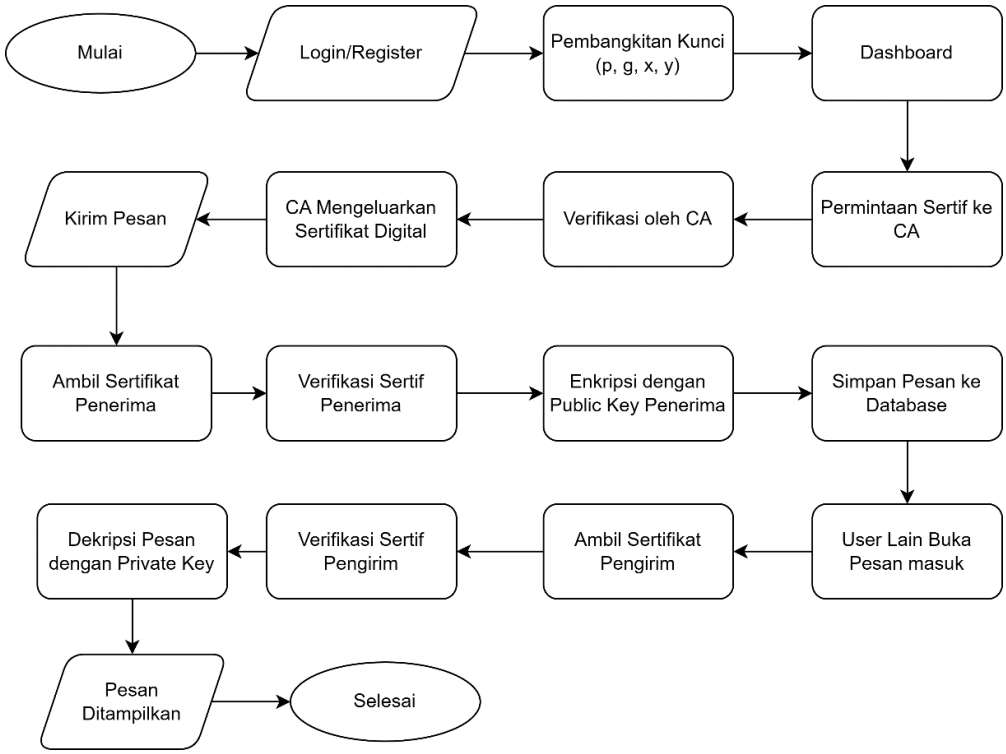


Gambar 1. Metode Waterfall

2.1 Perancangan Desain Sistem

Dilakukan pemetaan dan visualisasi terhadap seluruh proses utama yang terdapat dalam aplikasi SecureChat ElGamal. Perancangan ini bertujuan untuk memberikan gambaran yang jelas mengenai alur kerja sistem, interaksi antar komponen, serta mekanisme keamanan yang diterapkan, khususnya dalam implementasi algoritma ElGamal dan Public Key Infrastructure (PKI). Adapun perancangan desain system yang akan dibangun pada penelitian ini dinyatakan pada Gambar 2 di bawah ini.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



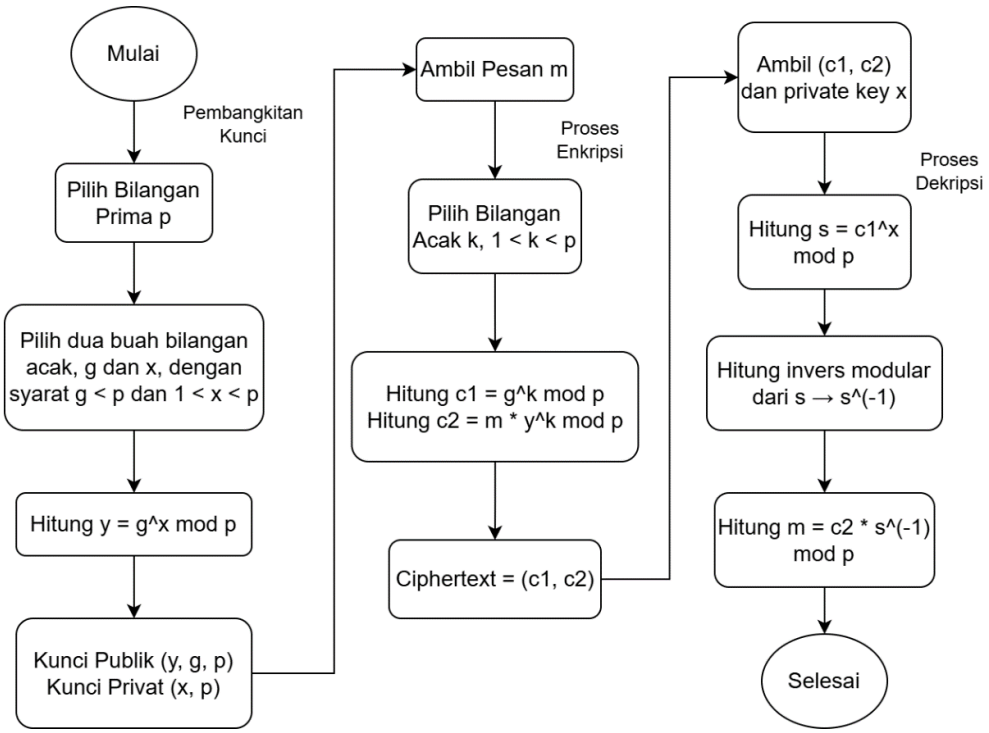
Gambar 2. Perancangan Desain Sistem

2.2 Implementasi Sistem

Sistem dikembangkan dengan teknologi web sebagai berikut:

- **Frontend**: HTML, CSS, Bootstrap, dan Jinja2.
- **Backend**: Python + Flask, bertanggung jawab untuk proses logika sistem seperti pembangkitan kunci, validasi sertifikat, dan pemrosesan pesan.
- **Database**: SQLite untuk penyimpanan data, dengan SQLAlchemy sebagai ORM.

2.3 Algoritma ElGamal



Gambar 3. Algoritma ElGamal

Algoritma ElGamal terdiri dari 3 tahap utama, yaitu pembangkitan kunci, proses enkripsi, dan proses dekripsi (Kromodimoeljo, 2009).

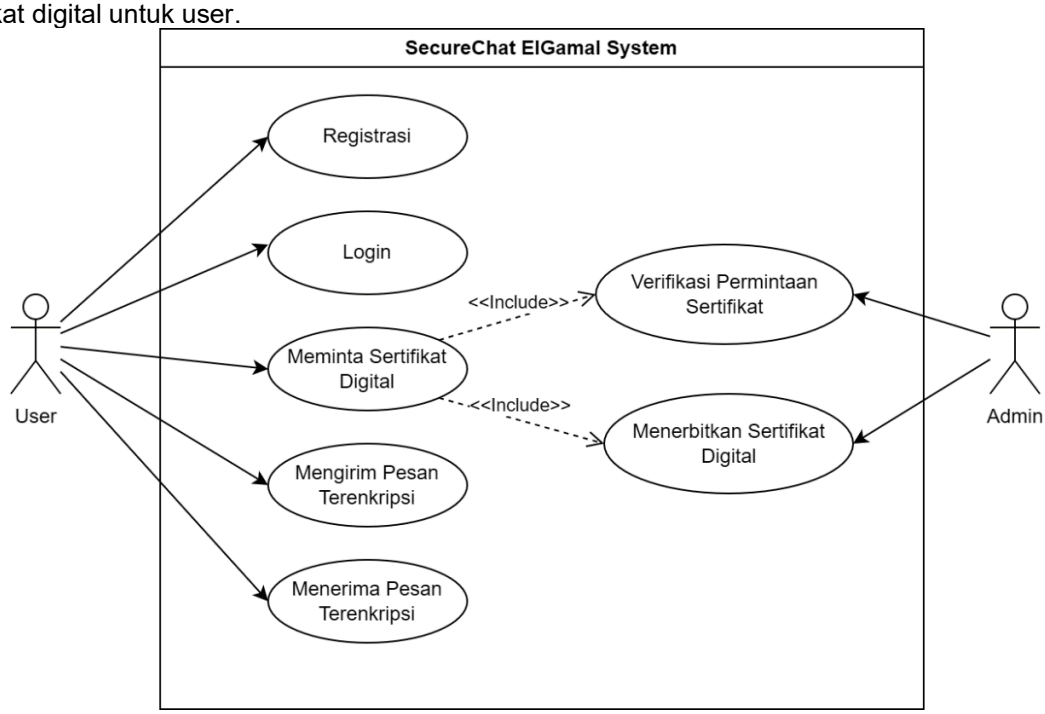
Pada tahap pembangkitan kunci, sistem terlebih dahulu memilih sebuah bilangan prima (p), kemudian memilih dua bilangan acak (g) dan (x) dengan syarat (g < p) dan (1 < x < p). Selanjutnya, nilai (y) dihitung dengan rumus (y = g^x \mod p). Kunci publik yang digunakan untuk enkripsi adalah ((y, g, p)), sedangkan kunci privat untuk dekripsi adalah ((x, p)).

Pada tahap enkripsi, pengirim mengambil pesan (m) yang akan dienkripsi, lalu memilih bilangan acak (k) dengan (1 < k < p). Dua nilai ciphertext dihitung, yaitu (c_1 = g^k \mod p) dan (c_2 = m \times y^k \mod p). Ciphertext yang dikirimkan ke penerima adalah pasangan ((c_1, c_2)).

Pada tahap dekripsi, penerima menggunakan pasangan ciphertext ((c_1, c_2)) dan kunci privat (x). Pertama, nilai (s) dihitung dengan (s = c_1^x \mod p). Kemudian, invers modular dari (s) ((s^{-1})) dihitung. Pesan asli (m) dapat diperoleh kembali dengan rumus (m = c_2 \times s^{-1} \mod p).

2.4 Use Case Diagram

Use case diagram digunakan untuk menggambarkan interaksi antara aktor dan sistem secara visual. Diagram ini membantu mengidentifikasi fungsi-fungsi utama yang dapat dilakukan oleh masing-masing aktor dalam aplikasi SecureChat ElGamal, serta batasan sistem yang dikembangkan. Pada sistem ini, terdapat dua aktor utama, yaitu User dan Admin/Certificate Authority (CA). User dapat melakukan registrasi, login, meminta sertifikat digital, mengirim pesan terenkripsi, dan menerima pesan. Sementara itu, Admin/CA bertugas melakukan verifikasi permintaan sertifikat dan menerbitkan sertifikat digital untuk user.



Gambar 4. Use Case Diagram Sistem

Use case diagram pada Gambar 4 menggambarkan interaksi antara aktor utama, yaitu User dan Admin, dengan sistem SecureChat ElGamal. User memiliki beberapa fungsi utama, seperti melakukan registrasi, login, meminta sertifikat digital, mengirim pesan terenkripsi, dan menerima pesan terenkripsi. Pada saat user meminta sertifikat digital, proses akan selalu melibatkan verifikasi permintaan sertifikat oleh Admin, dan jika lolos verifikasi, sistem akan menerbitkan sertifikat digital. Relasi <> pada diagram menunjukkan bahwa proses verifikasi dan penerbitan sertifikat digital selalu menjadi bagian dari proses permintaan sertifikat digital. Admin berperan dalam memverifikasi permintaan sertifikat dan menerbitkan sertifikat digital untuk user yang telah memenuhi persyaratan.

3. Hasil dan Pembahasan

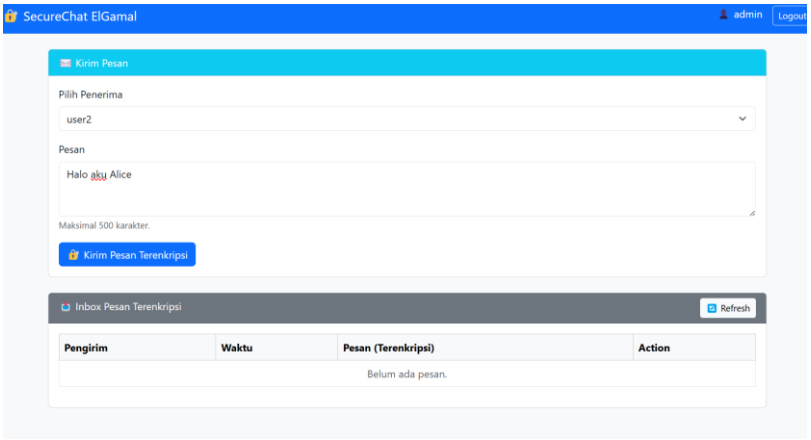
3.1 Fungsionalitas Sistem

p-ISSN: 2301-5373
e-ISSN: 2654-5101

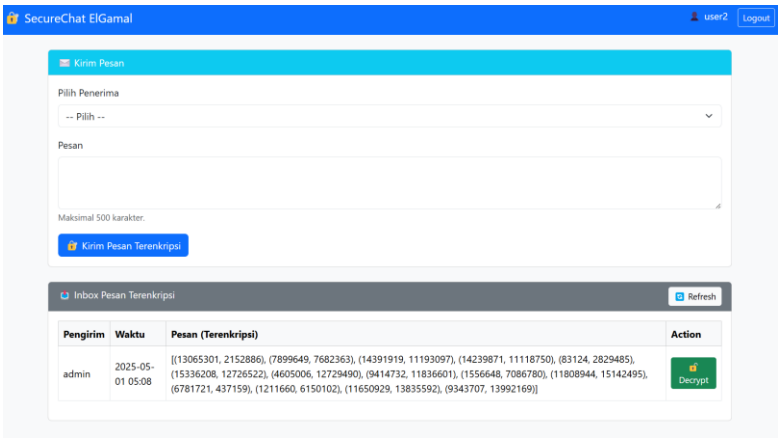
Sistem yang dikembangkan berhasil diimplementasikan sebagai platform berbasis web yang memungkinkan pertukaran pesan secara aman menggunakan algoritma kriptografi *ElGamal* dan *Public Key Infrastructure* (PKI). Beberapa fungsi utama yang tersedia dalam sistem antara lain:

- Pembangkitan Kunci: Sistem secara otomatis membangkitkan pasangan kunci publik dan privat menggunakan algoritma ElGamal saat pengguna melakukan pendaftaran.
- Penerbitan Sertifikat Digital: Modul Certificate Authority (CA) yang disimulasikan berfungsi untuk menerbitkan sertifikat digital guna memverifikasi keaslian kunci publik pengguna.
- Enkripsi dan Dekripsi Pesan: Pesan dienkripsi menggunakan kunci publik penerima, dan hanya dapat didekripsi oleh penerima menggunakan kunci privat yang sesuai.
- Validasi Sertifikat: Sistem memverifikasi validitas sertifikat digital sebelum proses komunikasi dilakukan.

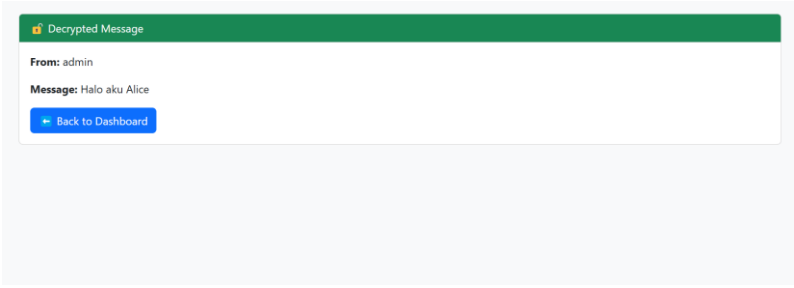
3.2 Implementasi Enkripsi



Gambar 5. Dashboard Enkripsi (admin)



Gambar 6. Tampilan Penerima (user2)



Gambar 7. Hasil Dekripsi

3.3 Pengujian Brute Force

Pada pengujian ini, dilakukan simulasi serangan dengan mencoba seluruh kemungkinan nilai kunci privat (private key) dan/atau nilai ephemeral key yang digunakan dalam proses enkripsi. Dalam pengujian ini, dilakukan simulasi serangan brute force pada beberapa ukuran kunci, yaitu 128, 256,

512, 1024, dan 2048 bit. Untuk kunci berukuran 128 hingga 512 bit, proses brute force dijalankan hingga selesai atau hingga waktu tertentu. Sedangkan untuk kunci berukuran 1024 dan 2048 bit, proses brute force hanya dijalankan dalam waktu singkat dan didokumentasikan melalui screenshot untuk menunjukkan bahwa proses tersebut tidak akan selesai dalam waktu yang wajar. Hal ini dilakukan untuk membuktikan secara empiris bahwa peningkatan panjang bit kunci secara signifikan meningkatkan waktu yang dibutuhkan untuk melakukan serangan brute force, bahkan hingga titik di mana serangan tersebut menjadi tidak praktis untuk dilakukan. Setiap percobaan dilakukan dengan parameter kunci yang berbeda, dan waktu yang dibutuhkan untuk menemukan kunci privat dicatat. Untuk kunci berukuran sangat besar, waktu brute force diekstrapolasi secara matematis berdasarkan hasil pengujian pada kunci yang lebih kecil. Data uji yang digunakan dalam pengujian sistem berupa pesan teks berukuran pendek (8–20 karakter).

Panjang Kunci (bit)	Waktu Brute Force (detik)	Status	Keterangan
128	390,5	Selesai	Kunci privat ditemukan
256	542,1	Selesai	Kunci privat ditemukan
512	1749,4	Selesai	Kunci privat ditemukan
1024	2.34 × 10^157	Tidak Selesai	Estimasi, proses diberhentikan manual
2048	4.22 × 10^465	Tidak Selesai	Estimasi, proses diberhentikan manual

Gambar 8. Hasil Pengujian Brute Force

Berdasarkan seluruh hasil pengujian, dapat disimpulkan bahwa algoritma ElGamal sangat rentan terhadap serangan brute force apabila menggunakan parameter kunci dengan panjang bit yang kecil, seperti 128 bit atau 256 bit. Namun, seiring bertambahnya panjang kunci, waktu yang dibutuhkan untuk melakukan serangan brute force meningkat secara eksponensial hingga mencapai tingkat yang tidak masuk akal untuk diselesaikan, bahkan dengan perangkat komputasi tercepat saat ini. Oleh karena itu, penggunaan kunci dengan panjang minimal 2048 bit sangat direkomendasikan untuk memastikan keamanan sistem terhadap serangan brute force.

3.4 Hasil Blackbox

Pengujian blackbox ini bertujuan untuk memastikan bahwa seluruh fungsi yang tersedia dapat berjalan sesuai dengan spesifikasi dan kebutuhan pengguna, tanpa memperhatikan detail implementasi kode program. Pengujian ini dilakukan berdasarkan skenario-skenario penggunaan dari perspektif pengguna dan administrator. Beberapa fitur yang diuji antara lain proses registrasi dan login pengguna, pembangkitan kunci publik dan privat, permintaan dan penerbitan sertifikat, pengiriman dan penerimaan pesan terenkripsi, serta fungsi dekripsi pesan di sisi penerima. gambar berikut merangkum fitur-fitur yang diuji, input yang diberikan, output yang diharapkan, serta hasil pengujian berdasarkan pelaksanaan skenario blackbox testing pada sistem

p-ISSN: 2301-5373
e-ISSN: 2654-5101

No	Fitur yang Diuji	Input	Expected Output	Hasil
1	Login pengguna	Email dan password yang valid	Pengguna berhasil masuk ke sistem	Sesuai
2	Pembangkitaan Kunci ElGamal	Klik tombol "Generate Key"	Kunci ElGamal berhasil dibuat dan disimpan	Sesuai
3	Permintaan sertifikat digital	Klik tombol "Request Certificate"	Sertifikat dikirim ke admin untuk diverifikasi	Sesuai
4	Verifikasi sertifikat oleh admin	Klik "Approve" pada permintaan pengguna	Sertifikat diterbitkan dan dapat digunakan	Sesuai
5	Enkripsi pesan	Pesan plaintext, pilih penerima	Pesan terenkripsi dan terkirim ke penerima	Sesuai
6	Dekripsi pesan	Pesan terenkripsi	Pesan berhasil didekripsi dan ditampilkan sebagai plaintext	Sesuai
7	Enkripsi/Dekripsi dengan sertifikat dicabut	Pesan plaintext, pilih penerima dengan sertifikat dicabut	Proses enkripsi/dekripsi gagal, muncul pesan error bahwa sertifikat tidak valid/dicabut	Sesuai
8	Update CRL oleh admin	Klik tombol "Revoke Certificate"	Sertifikat masuk daftar CRL, pengguna tidak bisa akses lagi	Sesuai
9	Logout	Klik tombol "Logout"	Sistem keluar ke halaman login	Sesuai

Gambar 9. Hasil Blackbox

4. Kesimpulan

Dalam simulasi brute force, kunci berukuran 2048-bit memerlukan waktu estimasi sekitar 4,22 × 10^465 detik untuk dipecahkan, yang secara praktis tidak mungkin dilakukan. Pengujian manajemen sertifikat digital juga berjalan sesuai prinsip PKI, termasuk penerbitan, verifikasi, dan pencabutan sertifikat. Sistem mampu mendeteksi dan menolak penggunaan sertifikat yang tidak valid atau telah dicabut. Sistem yang dibangun memungkinkan pengguna untuk melakukan pembangkitan kunci, enkripsi dan dekripsi pesan, serta validasi sertifikat digital secara otomatis dalam lingkungan web yang user-friendly.

Dari sisi fungsionalitas, hasil pengujian blackbox menunjukkan bahwa semua fitur utama sistem, seperti registrasi, login, pengiriman pesan terenkripsi, dekripsi pesan, dan manajemen sertifikat, telah bekerja sesuai dengan yang diharapkan.

References

[1] Agung, H. (n.d.). Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature.
[2] Alamsyah, H. (2021). Penerapan Sistem Keamanan WEB Menggunakan Metode WEB Aplication Firewall. Jurnal Amplifier Mei, 11.
[3] Binanto, I. (2014). ANALISA METODE CLASSIC LIFE CYCLE (WATERFALL) UNTUK PENGEMBANGAN PERANGKAT LUNAK MULTIMEDIA.

[4] Ariska, B., Endri, J., Studi Teknik Telekomunikasi Jurusan Teknik Elektro, P., Negeri Sriwijaya Palembang Jl Srijaya Negara Bukit Besar, P., Barat, I., & Palembang, K. (2018). RANCANGAN KRIPTOGRAFI HYBRID KOMBINASI METODE VIGENERE CIPHER DAN ELGAMAL PADA PENGAMANAN PESAN RAHASIA.
[5] Barker, E. (2020). Recommendation for key management: https://doi.org/10.6028/NIST.SP.800-57pt1r5
[6] Hermawan1, A., Hartati2, T., & Wijaya3, Y. A. (2022). Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. 7(3).
[7] Irmayanti. (2023). Perancangan Sistem Informasi Penyewaan Thermoking di PT. Moderen Prima dengan Flask Python. Jurnal Sistem Dan Teknologi Informasi Cendekia, 1(1), 19–28.
[8] Setiawan, A., & Farida Ariyani, P. (2023). 2 nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 21 Maret 2023-Jakarta (Vol. 2, Issue 1).