DECODE: JURNAL PENDIDIKAN TEKNOLOGI INFORMASI
P-ISSN: 2775-2984 | E-ISSN: 2775-1813
Vol. 5, No 2, Juli 2025, Hal: 495-504
Doi: http://dx.doi.org/10.51454/decode.v5i2.1201
https://journal.umkendari.ac.id/index.php/decode

Kriptografi Hybrid Menggunakan OTP dan ElGamal Pada Web EMIS

Maghfira Aida[1*], Suhardi[1]
[1]Program Studi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara, Indonesia.

Artikel Info

Kata Kunci:

Avalanche Effect;
Character Error Rate;
EMIS;
ElGamal;
OTP.

Keywords:

Avalanche Effect;
Character Error Rate.;
EMIS;
ElGamal;
OTP.

Riwayat Artikel:

Submitted: 22 Juni 2025
Accepted: 27 Juli 2025
Published: 31 Juli 2025

Abstrak: Sistem yang berperan besar dalam pengelolaan data pendidikan di Indonesia adalah EMIS (Education Management Information System) yang proses loginnya menggunakan username, password dan verifikasi captcha dalam pengamanannya. Namun, keamanan captcha saja tidak cukup untuk mencegah terjadinya ancaman siber. Oleh karena itu, sistem ini membutuhkan lapisan keamanan tambahan agar tidak terjadi kebocoran data dan akses tidak sah. Dalam penelitian ini digunakanlah kriptografi hybrid One Time Pad (OTP) dan ElGamal yang menggabungkan dua jenis kriptografi yaitu simetris dan asimetris. Sistem akan otomatis menghasilkan kode OTP berupa 6 digit angka yang akan dienkripsi menggunakan One Time Pad. Lalu kunci dari One Time Pad akan dienkripsi lagi menggunakan ElGamal. Pengujian menggunakan Avalanche Effect dan Character Error Rate untuk melihat persentase tingkat keamanan data. Hasil penelitian Avalanche Effect sebesar 49,41% yang menandakan bahwa metode ini memiliki nilai Avalanche Effect yang bagus dikarenakan perubahan kecil pada plainteks dapat berdampak ke cipherteks dan Character Error Rate sebesar 0% yang menandakan hasil enkripsi yang sangat aman karena tingkat persentase yang rendah dan tingkat keberhasilan OTP yang dikirim pengguna 100% cocok dengan OTP yang dihasilkan oleh sistem. Kesimpulannya, model aplikasi pengamanan web EMIS ini dapat dijadikan rekomendasi bagi pengembang web emis dalam menerapkan sistem keamanan.

Abstract: *The system that plays a major role in managing education data in Indonesia is EMIS (Education Management Information System) whose login process uses username, password and captcha verification in its security. However, captcha security alone is not enough to prevent cyber threats. Therefore, this system requires an additional layer of security to prevent data leaks and unauthorized access. In this study, hybrid cryptography One Time Pad (OTP) and ElGamal were used, which combines two types of cryptography, namely symmetric and asymmetric. The system will automatically generate an OTP code in the form of 6 digits which will be encrypted using One Time Pad. Then the key from One Time Pad will be encrypted again using ElGamal. Testing uses Avalanche Effect and Character Error Rate to see the percentage of data security level. The results of the Avalanche Effect study were 49.41%, indicating that this method has a good Avalanche Effect value because small changes in the plaintext can affect the ciphertext and the Character Error Rate is 0%, indicating a very secure encryption result because the percentage is low and the success rate of the OTP sent by the user is 100% in accordance with the OTP generated by the system. In conclusion, this EMIS web security application model can be used as a recommendation for emis web developers in implementing a security system.*

Corresponding Author:
Maghfira Aida
Email: maghfira0701212205@uinsu.ac.id

PENDAHULUAN

Seiring dengan perkembangan zaman, mengharuskan manusia untuk menciptakan sebuah inovasi sistem terbaru agar dengan cepat menyelesaikan suatu permasalahan (Al Murod & Suhirman, 2024). Salah satu sistem yang berperan besar dalam pengelolaan data pendidikan adalah EMIS (Education Management Information System). EMIS dirancang agar dapat membantu lembaga pendidikan dalam pengelolaan data siswa, guru, sarana dan prasarana serta berbagai informasi lainnya. Proses login web EMIS saat ini menggunakan username, password dan verifikasi captcha dalam pengamanannya. Namun, semakin berkembangnya teknologi maka terjadi pula peningkatan serangan siber terutama dalam sistem login.

Berdasarkan penelitian oleh (Alameka, 2023) dalam penelitiannya yang berjudul "Sektor Serangan Siber dan Metode Pendeteksi Serangan Siber Pada Website Pelayanan Publik di Kalimantan Timur". Saat ini telah banyak terjadi kasus pembobolan captcha yang memungkinkan pihak tidak berwenang mengakses data pengguna. Pada tahun 2022 Provinsi Kalimantan Timur tercatat telah terjadi sebanyak 40.432 kasus serangan siber jenis captcha-web. Hal ini menunjukkan bahwa sistem keamanan seperti captcha tidak lagi cukup untuk mencegah ancaman siber. Semakin meningkatnya angka kejahatan di tingkat nasional, menunjukkan bahwa keamanan menjadi aspek yang sangat penting dalam operasional berbagai sektor (Marentek et al., 2025).

Salah satu platform media sosial terbesar di dunia seperti Instagram telah menerapkan Two-Factor Authentication (2FA) untuk melindungi akun penggunanya dari ancaman peretasan dan akses tidak sah. Namun, hingga saat ini EMIS belum menerapkan sistem keamanan 2FA. Kurangnya lapisan keamanan tambahan ini dapat meningkatkan terjadinya kebocoran data dan akses tidak sah yang dapat berdampak serius pada privasi dan integritas data pendidikan (Siregar et al., 2024).

Berdasarkan penelitian sebelumnya mengenai algoritma One Time Pad oleh (A. A. Permana et al., 2021) dalam penelitiannya yang berjudul "Implementasi Aplikasi Pengamanan Pesan Gambar Menggunakan Algoritma One Time Pad". One Time Pad adalah metode yang terbukti memiliki tingkat keamanan tinggi secara matematis karena menggunakan kunci yang unik dan hanya sekali pakai untuk setiap pesan sehingga sangat sulit untuk dipecahkan. Namun, One Time Pad juga memiliki kelemahan dimana pada pendistribusian kunci antara pengirim dan penerima dapat terjadi kebocoran pada saat pertukaran informasi.

Penelitian sebelumnya mengenai algoritma ElGamal yang dilakukan oleh (Harahap et al., 2022) dengan judul "Penerapan ElGamal Guna Meningkatkan Keamanan Data Text dan Docx" bahwa algoritma kriptografi asimetris yang mampu mengatasi masalah pendistribuasian kunci yaitu ElGamal. Kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda. Kunci publik yang disebarluaskan digunakan untuk mengenkripsi pesan, sementara kunci privat tetap dirahasiakan oleh penerima dan digunakan untuk mendekripsi pesan.

Penelitian-penelitian sebelumnya yang relavan telah menunjukkan penggunaan algoritma One Time pad maupun ElGamal mampu memberikan tingkat keamanan yang yang tinggi. Studi yang dilakukan (Thu et al., 2020) membahas tentang pengamanan pesan menggunakan kriptografi hibrid One Time Pad dan AES. Hasil menunjukkan tingkat avalanche effect pada AES hanya 34%, sedangkan OTP-AES sebesar 98%. Algoritma OTP-AES memberikan persentase avalanche effect yang lebih tinggi dari pada algoritma AES asli. Penelitian lain yang dilakukan (Rihartanto et al., 2024) membahas tentang penggunaan One Time Pad untuk meningkatkan keamanan informasi menggunakan LSB dengan pola spiral. Penggunaan angka acak sebagai OTP berhasil mengubah data tersembunyi secara signifikan, ditunjukkan dengan nilai avalanche effect di atas 50%. Penelitian yang dilakukan (Nisa et al., 2020) membahas tentang kombinasi antara algoritma Diffie-Hellman dan ElGamal untuk mengamankan

pesan teks dan citra. Pada file teks diperoleh nilai avalanche effect sebesar 85.18%. Sedangkan pada file citra, diperoleh nilai avalanche effect sebesar 84.46%.

Berdasarkan narasi diatas, untuk memberikan keamanan yang tinggi pada sistem login website EMIS tidak cukup hanya mengandalkan verifikasi captcha. Peneliti merekomendasikan kriptografi hybrid dengan menggabungkan One Time Pad dan ElGamal. Alasan peneliti menggunakan kriptografi hybrid One Time Pad dan ElGamal karena penggabungan antara metode simetris dan asimetris yang bertujuan untuk menutupi dari kelemahan masing-masing algoritma. Dengan demikian, pada web EMIS sistem yang dibangun merupakan model aplikasi untuk pengamanan tanpa membahas pendataan web EMIS dengan jumlah OTP yang dihasilkan dibatasi hingga 100 kunci acak (jika seluruh kunci OTP telah habis digunakan, sistem akan menghasilkan ulang 100 kunci baru secara otomatis). Serta pengamanan sistem login web hanya pada proses pengamanan data login (username dan password).

LANDASAN TEORI

One Time Pad

Menurut Alam & Pasaribu dalam (Ulfa et al., 2021) kriptografi berasal dari bahasa Yunani "kryptos" yang berarti tersembunyi dan "graphein" yang berarti menulis. Secara umum terdapat dua jenis kriptografi yang dapat digunakan untuk mengamankan informasi, yaitu simetris dan asimetris. Menurut Al-Shabi dalam (Suseno et al., 2021) penggunaan satu jenis kriptografi simetris ataupun asimetris masih rentan terhadap penyerangan siber. Oleh karena itu, untuk mengatasi beberapa ancaman kelemahan pada masing-masing jenis kriptografi dapat dilakukan penggabungan antara kedua jenis kriptografi tersebut yang disebut dengan metodologi hybrid.

Algoritma One Time Pad (OTP) adalah metode enkripsi simetris yang menggunakan kunci (key) secara acak, sepanjang pesan (plainteks) yang akan dienkripsi, dan hanya digunakan sekali untuk satu pesan. One time pad ditemukan oleh gilbert vernam dan biasa dikenal dengan algoritma vernam. Pada One Time Pad terdapat 2 metode untuk mengenkripsi pesan. Pertama dapat menggunakan metode modulo dan yang kedua menggunakan biner (XOR). Untuk melakukan pengenkripsian menggunakan modulo, setiap karakter diubah menjadi nilai numerik dalam alfabet (Syaifuddin et al., 2021). Proses enkripsi dan dekripsi dapat dilakukan dengan cara substitusi angka/matematis (Iyengar, 2022).

Pengenkripsian menggunakan One Time Pad yang kedua dapat menggunakan metode biner (XOR) dengan kunci harus sepanjang plainteks, kunci benar-benar acak seluruhnya, kunci hanya digunakan sekali setiap melakukan enkripsi, dan hanya terdapat dua salinan dari kunci, yaitu satu untuk pengirim dan satunya lagi untuk penerima (Anwar & Sriani, 2025). Hal yang perlu diperhatikan pada penerapan XOR adalah operasi logika yang menghasilkan TRUE (1) jika dua digit berbeda dan FALSE (0) jika sama (Purnama et al., 2022).

ElGamal

Algoritma ElGamal pertama kali diciptakan pada tahun 1985 oleh ilmuwan asal mesir, Taher ElGamal. Algoritma ElGamal adalah salah satu algoritma pada kriptografi yang tergolong sebagai algoritma asimetris karena menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Kunci publik yang disebarluaskan digunakan untuk mengenkripsi pesan, sementara kunci privat tetap dirahasiakan oleh penerima dan digunakan untuk mendekripsi pesan.

Terdapat beberapa tahapan untuk mencapai enkripsi dan dekripsi pada algoritma ElGamal (Harahap et al., 2022). Tahapan tersebut, yaitu:

a. Memilih sembarang bilangan prima.
b. Memilih dua bilangan acak, g dan x dimana $g < p$ dan $1 \leq x \leq p-2$.
c. Pembentukan pasangan kunci yaitu kunci publik dan kunci privat.
d. Memasukkan teks asli/plainteks yang akan dienkripsi.
e. Melakukan enkripsi dengan kunci publik.
f. Hasil proses enkripsi berupa cipherteks.

g. Untuk melakukan dekripsi gunakan kunci privat.

Setelah mengetahui tahapan tersebut, terdapat 3 bentuk persamaan umum pada algoritma ElGamal, yaitu pembentukan/pembangkitan kunci, enkripi dan dekripsi (Nugraha, 2024).

Avalanche Effect

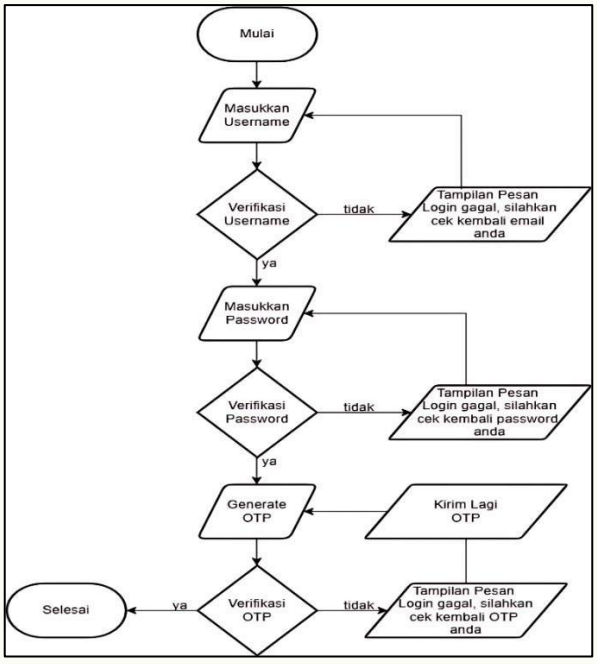
Avalanche effect merupakan metode untuk mengetahui seberapa banyak jumlah bit atau persen yang berubah pada cipherteks saat satu bit plainteks diubah. Pengujian avalanche effect dianggap baik jika menunjukkan hasil persentase antara 45-60%. Perubahan sebanyak itu akan mengakibatkan para pembobol cukup sulit untuk melakukan serangan (Pinuyut et al., 2024).

Character Error Rate

Character error rate merupakan metode untuk mengukur tingkat akurasi pada hasil enkripsi dengan mencocokkan dan membandingkan karakter pada plainteks dengan plainteks yang diubah (Karima et al., 2024). Semakin rendah tingkat persentase maka semakin bagus hasil enkripsi, begitu juga sebaliknya (Muslih & Handoko, 2022).

METODE

Jenis penelitian ini menggunakan metodologi penelitian kuantitatif yang bersifat matematis serta memiliki struktur dan tahapan yang jelas untuk menggambarkan suatu kejadian. Metode penelitian ini diawali dengan tahapan identifikasi yang dilakukan oleh peneliti untuk mengidentifikasi permasalahan keamanan pada sistem login EMIS yang meliputi analisis potensi ancaman, serta evaluasi kerentanan pada autentikasi username dan password. Kemudian tahap kajian pustaka yang dilakukan oleh peneliti untuk mencari atau menemukan penelitian terdahulu yang membahas tentang penggunaan One Time Pad (OTP) dan ElGamal pada sistem keamanan yang selanjutnya akan dijadikan dasar perancangan rencana penelitian. Kemudian tahap perancangan yang meliputi pengembangan diagram alir sistem dari input username sampai dengan verifikasi OTP yang hanya membahas pemilihan algoritma yang tepat dan efisien. Terakhir, model aplikasi akan diuji dan dijalankan. Berikut ini merupakan perancangan flowchart sistem yang harus dilakukan untuk melengkapi penelitian ini yang dapat dilihat pada Gambar 1.



Gambar 1. Flowchart Sistem

Berdasarkan flowchart sistem diatas, pengguna akan mengisi email dan password di form login. Setelah itu pengguna akan diarahkan ke form pembuatan OTP. Sistem akan menghasilkan OTP acak sebanyak 6 digit yang dikirim melalui Gmail. OTP ini sebelumnya telah dienkripsi terlebih dahulu menggunakan One Time Pad dan kunci dari One Time Pad akan dienkripsi lagi menggunakan ElGamal. OTP yang telah dienkripsi akan ditampilkan di antarmuka, bersama dengan batas waktu 45 detik. Setelah pengguna memasukkan OTP, maka sistem akan mendekripsi menggunakan ElGamal dengan private key yang sesuai. Lalu OTP yang terenkripsi dengan One Time Pad akan didekripsi dengan kunci yang dihasilkan saat pembuatan OTP. Jika OTP cocok, maka pengguna akan berhasil login. Jika tidak cocok, maka pengguna tidak berhasil login.

```
FUNCTION generate_otp_list(conn, total = 100)
    // Parameter ElGamal
    p = 467        // Bilangan prima
    g = 2          // Generator
    x = 5          // Kunci privat
    y = g^x MOD p  // Kunci publik

    FOR i FROM 0 TO total - 1 DO
        otp = RANDOM(100000, 999999)         // OTP 6 digit
        otp_key = RANDOM(1, p - 1)           // OTP key acak < p

        // Enkripsi pertama: XOR OTP dengan otp_key
        otp_xored = otp XOR otp_key

        // Enkripsi kedua: ElGamal mengenkripsi otp_key
        k  = RANDOM(1, p - 2)
        c1 = g^k MOD p
        s  = y^k MOD p
        c2 = (otp_key * s) MOD p

        // Simpan atau kirim: otp_xored, c1, c2
    END FOR
END FUNCTION
```

Gambar 2. Pseudocode Enkripsi One Time Pad dan ElGamal

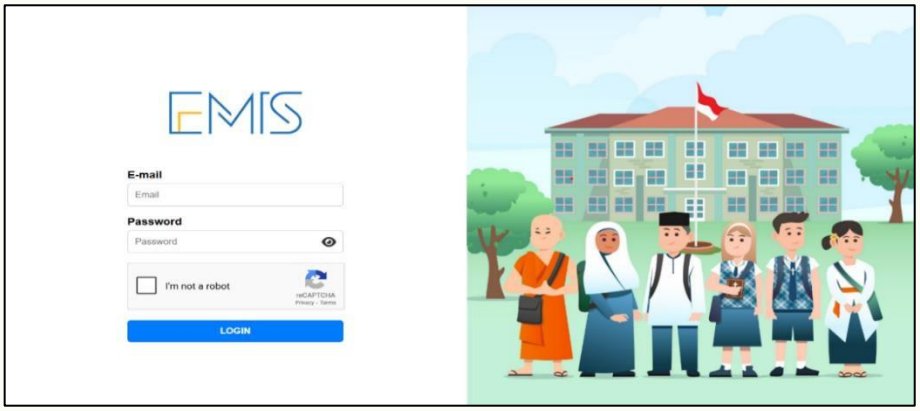
```
FUNCTION decrypt_elgamal(c1, c2, x = 5, p = 467, g = 2) RETURNS INTEGER
    // Hitung s = c1^x mod p
    s = 1
    FOR i FROM 0 TO x - 1 DO
        s = (s * c1) MOD p
    END FOR

    // Hitung invers dari s mod p
    s_inv = mod_inverse(s, p)

    // Kembalikan hasil dekripsi: m = (c2 * s_inv) mod p
    RETURN (c2 * s_inv) MOD p
END FUNCTION


FUNCTION mod_inverse(a, m) RETURNS INTEGER
    a = a MOD m
    FOR x FROM 1 TO m - 1 DO
        IF (a * x) MOD m = 1 THEN
            RETURN x
        END IF
    END FOR
    RETURN 1 // fallback jika tidak ditemukan
END FUNCTION
```

Gambar 3. Pseudocode Dekripsi One Time Pad dan ElGamal

Pada Gambar 2. Pseudocode enkripsi menggunakan One Time Pad dan ElGamal dalam aplikasi yang dibuat. Pada Gambar 3. merupakan gambar pseudocode untuk mendekripsi menggunakan One Time Pad dan ElGamal.

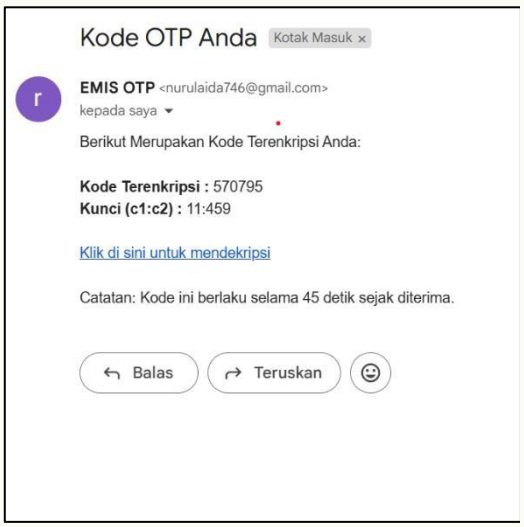
HASIL DAN PEMBAHASAN

Pada gambar 4. dibawah ini menunjukkan ketika program dijalankan maka akan menampilkan halaman depan EMIS.



Gambar 4. Halaman Web EMIS

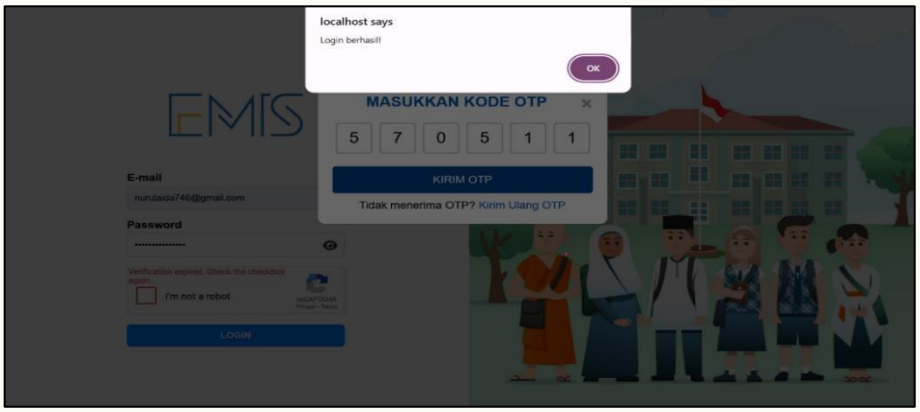
Pada gambar 5. Pengguna memasukkan E-mail dan Password yang sudah terdaftar, serta centang verifikasi captcha. Kemudian kode OTP beserta kunci yang sudah dienkripsi akan dikirim ke G-mail pengguna. Kode ini berlaku selama 45 detik sejak diterima pengguna. Lalu untuk mendekripsikan kode OTP tersebut dengan mengklik link yang sudah dikirim. Pada gambar 6. Setelah link diklik, maka akan menampilkan halaman Dekripsi OTP. Pengguna memasukkan kode terenkripsi beserta kunci. Setelah itu klik tombol Dekripsi. OTP asli akan keluar dan OTP inilah yang digunakan untuk login ke website EMIS.



Gambar 5. Kode OTP G-mail

Gambar 6. Dekripsi OTP

Pada gambar 7. Masukkan kode OTP yang telah didekripsi dan Kirim OTP. Setelah itu sistem akan mencocokkan kode, jika sesuai maka akan ada pemberitahuan berhasil login



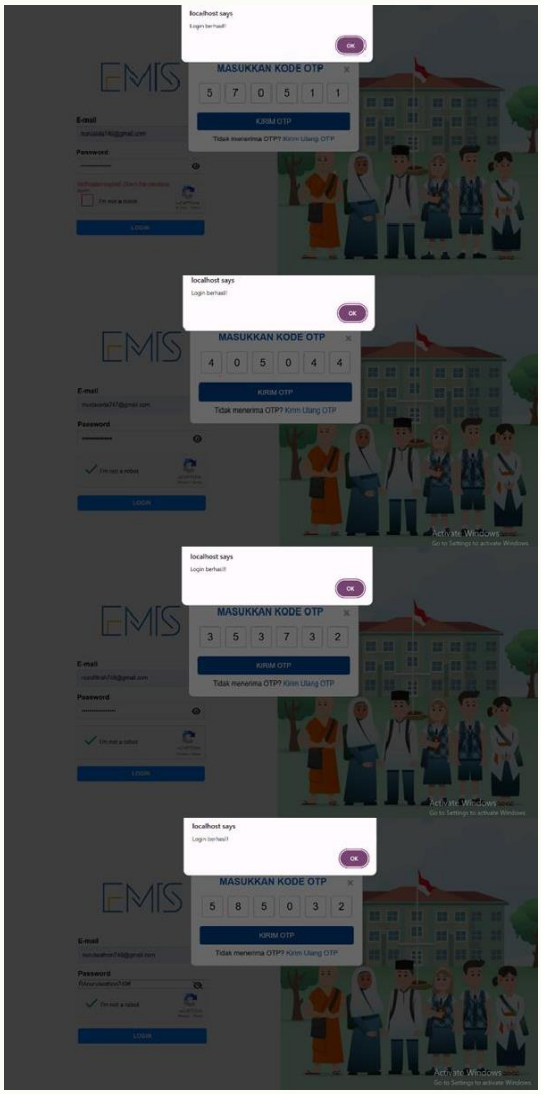
Gambar 7. Pengguna Berhasil Login

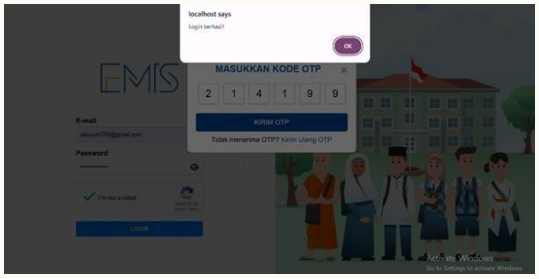
Pada gambar 8. Merupakan model sederhana tampilan awal apabila pengguna berhasil login.

Gambar 8. Tampilan Awal

Kemudian dilakukanlah pengujian tingkat keberhasilan OTP yang dikirim ke pengguna dengan OTP yang dihasilkan sistem yang dapat dilihat pada Tabel 1. Berikut:

Tabel 1. Pengujian OTP

No	OTP yang Dihasilkan	Proses Pengujian	Hasil
1	570511		OTP cocok
2	405044		OTP cocok
3	353732		OTP cocok
4	585032		OTP cocok

5	214199		OTP cocok

Berdasarkan pengujian pada Tabel 1. Pengguna berhasil login karena OTP yang telah didekripsi dan dimasukkan oleh pengguna sesuai dengan OTP yang dihasilkan oleh sistem dan tersimpan di database. Maka, tingkat keberhasilan OTP yang dikirim dan diterima oleh pengguna adalah 100% sesuai dengan OTP yang dihasilkan oleh sistem. Hal ini juga dibuktikan dengan Character Error Rate bernilai 0% karena tidak memiliki perbedaan pada OTP asli setelah dienkripsi dan didekripsi hasilnya tetap kembali ke OTP asli.

Lalu untuk menguji tingkat keamanan, dilakukanlah pengujian avalanche effect untuk a dengan hasil dapat dilihat pada Tabel 2. Berikut:

Tabel 2. Hasil Avalanche Effect untuk a

No	Nilai a	Nilai m	Nilai k	Perubahan Nilai a	Perubahan Nilai m	Perubahan Nilai k	Perbedaan bit	Total bit	Avalanche Effect (a)
1	11	292	141	176	293	145	6	8	75%
2	269	71	343	71	75	344	4	9	44,44%
3	172	104	312	344	105	313	6	9	66,66%
4	275	360	233	465	361	234	3	9	33,33%
5	32	305	5	256	308	8	2	9	22,22%
6	178	13	335	142	18	345	4	8	50%
7	360	18	12	52	15	32	5	9	55,55%
8	427	321	277	387	327	278	2	9	22,22%
9	394	214	228	387	219	278	2	9	22,22%
10	212	51	76	295	55	79	7	9	77,77%

Dari perhitungan avalanche effect untuk a diatas, dapat dilihat bahwa pengamanan menggunakan One Time Pad dan ElGamal menghasilkan nilai rata-rata avalanche effect sebesar 46,94%. Lalu pengujian avalanche effect untuk b dapat dilihat pada Tabel 3. Berikut:

Tabel 3. Hasil Avalanche Effect untuk b

No	Nilai b	Nilai m	Nilai k	Perubahan Nilai b	Perubahan Nilai m	Perubahan Nilai k	Perbedaan bit	Total bit	Avalanche Effect (b)
1	459	292	141	83	293	145	4	9	44,44%
2	372	71	343	38	75	344	4	9	44,44%
3	12	104	312	92	105	313	2	7	28,57%
4	437	360	233	123	361	234	6	9	66,66%
5	357	305	5	303	308	8	3	9	33,33%
6	414	13	335	49	18	345	7	9	77,77%
7	240	18	12	440	15	32	3	9	33,33%
8	232	321	277	357	327	278	5	9	55,55%
9	48	214	228	72	219	278	4	7	57%
10	55	51	76	396	55	79	7	9	77,77%

Dari perhitungan avalanche effect untuk b diatas, dapat dilihat bahwa pengamanan menggunakan One Time Pad dan ElGamal menghasilkan nilai rata-rata avalanche effect sebesar

51,88%. Maka hasil penjumlahan dari rata-rata nilai a dan b, tingkat akurasi avalanche effect sebesar 49,41%.

KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah dihasilkan dalam penelitian ini, dapat disimpulkan bahwa keamanan tambahan menggunakan One Time Pad dan ElGamal yang diimplementasikan ke dalam kunci OTP berhasil diimplementasikan, baik menggunakan enkripsi maupun dekripsi. Tingkat keberhasilan OTP yang dikirim dan diterima oleh pengguna adalah 100% sesuai dengan OTP yang dihasilkan oleh sistem. Hasil pengujian menunjukkan bahwa rata-rata tingkat Avalanche Effect pada One Time Pad dan Elgamal adalah 49,41%. Hasil tersebut dapat dikatakan baik karena Avalanche Effect dikategorikan baik jika berkisar antara 45-60% dan hasil pengujian Character Error Rate adalah 0% yang menunjukkan hasil baik jika nilainya mendekati 0 dan persentase yang rendah serta tingkat keberhasilan OTP yang dikirim pengguna 100% cocok dengan OTP yang dihasilkan oleh sistem.

Sebagai saran untuk pengembangan penelitian lebih lanjut, untuk mengoptimalisasi keamanan dan mempercepat proses enkripsi pada kriptografi dapat menggunakan variasi algoritma kriptografi hybrid yang berbeda agar menghasilkan avalanche effect yang lebih baik (>50%). Serta penggunaan platform modern untuk pengiriman kode OTP dapat menggunakan platform media sosial seperti Whatsapp, Telegram atau media sosial lainnya yang menggunakan ponsel atau android karena sifatnya yang lebih praktis dibandingkan dengan pengiriman melalui G-mail. Untuk pengujian dapat melakukan simulasi pengiriman lebih dari 25-100 OTP untuk menguji kecepatan dan kegagalan pengiriman kode OTP.

DAFTAR PUSTAKA

Al Murod, S., & Suhirman, S. (2024). Aplikasi Keamanan E-Voting Pemilihan Ketua Osis Menggunakan Metode AES 128 Berbasis Android (Studi Kasus: MTSN 3 Poso). *Decode: Jurnal Pendidikan Teknologi Informasi*, *4*(3), 1142–1154. https://doi.org/10.51454/decode.v4i3.818

Alameka, D. (2023). Systematic Literature Review: Sektor Serangan Siber Dan Metode Pendeteksi Serangan Siber Pada Website Pelayanan Publik Di Kalimantan Timur. http://eprints.ipdn.ac.id/id/eprint/14989

Anwar, C., & Sriani, S. (2025). Implementasi Algoritma OTP dan HMAC untuk Two-Factor Authentication Sistem Login Relawan Pemilu. *TEKNIKA*, *19*(1), 83–94. https://doi.org/10.5281/zenodo.13862454

Harahap, A. Y. N., Gunawan, H., Nst, A. B., & Sari, R. E. (2022). Penerapan Elgamal Guna Meningkatkan Keamanan Data Text dan Docx. *It (Informatic Tech. J*, *10*(1), 76. https://doi.org/10.22303/it.10.1.2022.76-86

Karima, N. A., Aisyah, A. N., Silla, H. V., Handoko, L. B., & Sani, R. R. (2024). Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit. *Jurnal Masyarakat Informatika*, *15*(1), 1–13. https://doi.org/10.14710/jmasif.15.1.60836

Marentek, B., Triyono, G. (2025). *Sistem Pendukung Keputusan Pemeringkatan Pengamanan menggunakan AHP dan TOPSIS*. *Decode: Jurnal Pendidikan Teknologi Informasi*, *5*(1), 92–105. https://doi.org/10.51454/decode.v5i1.891

Muslih, M., & Handoko, L. B. (2022). Pengujian Avalanche Effect Pada Kriptografi Teks Menggunakan Autokey Cipher. *Seminar Nasional Teknologi Dan Multidisiplin Ilmu (SEMNASTEKMU)*, *2*(1), 127–134. https://doi.org/10.51903/semnastekmu.v2i1.162

Nisa, L., Indriyani, T., & Ruswiansari, M. (2020). Aplikasi Enkripsi Citra dan Teks Menggunakan Algoritma Diffie-Hellman dan ElGamal. *Jurnal Teknologi Dan Manajemen*, *1*(1), 8–17. https://doi.org/10.31284/j.jtm.2020.v1i1.153

Nugraha, S. N. (2024). Penerapan Algoritma Kriptografi Elgamal Pada Aplikasi Pengamanan Pesan Berbasis Website. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.4794

Permana, A. A., Taufiq, R., & Destriana, R. (2021). Implementasi Aplikasi Pengamanan Pesan Gambar Menggunakan Algoritma One Time Pad. *Proceeding SENDI_U*.

Pinuyut, C. A., Utami, E., & Muhammad, A. H. (2024). Analisis Kinerja Algoritma Advanced Encryption Standard (Aes) Termodifikasi Dalam Enrkipsi Dan Dekripsi Data. *Teknimedia: Teknologi Informasi Dan Multimedia*, *5*(2), 132–137. https://doi.org/10.46764/teknimedia.v5i2.200

Purnama, L., Mulyana, D. L., Aji, A., Sulaiman, E. O. P. (2022). Implementasi Algoritma One Time menggunakan Algoritma Chiper Transposition Sebagai pengaman Rahasisa Pesan Rail Fence Cipher Dan Route Cipher Untuk Keamanan File *03*(01), 2774–7115. https://doi.org/10.55377/j-icom.v3i1.4997

Rihartanto, Utomo, D. S. B., Rizal, A., Diartono, D. A., & Februariyanti, H. (2024). One time pad for enhanced steganographic security using least significant bit with spiral pattern. *International Journal of Informatics and Communication Technology*, *13*(2), 168–177. https://doi.org/10.11591/ijict.v13i2.pp168-177

Siregar, M. Z., Trisna, N. F. I. E., Alya, R., Nasution, Z. Z., Yusuf, M., & Harahap, N. (2024). Penerapan Autentikasi Dua Faktor Untuk Keamanan Data Pribadi Di Instagram: Perspektif Mahasiswa Uinsu Stambuk 21'. *Triwikrama: Jurnal Ilmu Sosial*, *6*(7), 41–50. https://doi.org/10.6578/triwikrama.v6i7.9683

Suseno, A. Y., Sulistiyowati, N., & -, P. (2021). Analisis Peningkatan hybrid Cryptosystem Untuk Enkripsi dan Dekripsi Menggunakan Vigenere Cipher dan RSA Pada Text. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 142. https://doi.org/10.30998/string.v6i2.10309

Syaifuddin, M., Hutagalung, J., & Ganefri, G. (2021). E-Learning Dalam Pengembangan Pembelajaran Kriptografi. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *7*(2), 117–126. https://doi.org/10.33330/jurteksi.v7i2.914

Thu, T., Tun, T., Myint, E. E., & Aung, M. T. (2020). *Message Security Using One Time Pad and Aes Hybrid Cryptography*. *3*(June), 110–114.

Ulfa Br Mtd, R. M., Fauzi, A., & Sembiring, H. (2021). Kombinasi Algoritma Vigenere Cipher Dan One Time Pad Pada Keamanan Citra Digital. *Jurnal Informatika Kaputama (JIK)*, *5*(1), 137–146. https://doi.org/10.59697/jik.v5i1.312