Saturnus : Jurnal Teknologi dan Sistem Informasi
Volume. 2 No. 3 Juli 2024
e-ISSN: 3031-9943; dan p-ISSN: 3031-9935, Hal. 119-128
DOI: https://doi.org/10.61132/saturnus.v2i3.204

Kombinasi Kriptografi Modern Dalam Keamanan Pesan Teks

Dhea Agustina Akmal [1], Dicha Mutia Dhani [2], Febby Syahila [3]
[1,2,3] STMIK Kaputama Binjai

Jl. Veteran No. 4A, Tangsi, Kec. Binjai Kota, Kota Binjai, Sumatera Utara
Korespondensi penulis: agustinadhea91@gmail.com

Abstract. *In the rapidly advancing digital era, information security has become a crucial aspect in maintaining the confidentiality, integrity, and authenticity of data. This article discusses the relationship between information system auditing and the use of modern cryptographic combinations in securing text messages. Information system auditing serves as an evaluation mechanism to ensure that security policies, procedures, and standards are correctly and consistently applied. On the other hand, modern cryptography provides advanced encryption technology that protects text messages from unauthorized access and manipulation. By combining these two approaches, we can create a robust framework for securing text messages, ensuring that data remains safe and protected during transmission and storage. Research results indicate that integrating information system auditing with modern cryptographic techniques significantly enhances the security and reliability of information systems.*

Keywords: *Elgamal; XOR; Text*

Abstrak. Dalam era digital yang semakin berkembang, keamanan informasi menjadi aspek yang krusial dalam menjaga kerahasiaan, integritas, dan keaslian data. Artikel ini membahas hubungan antara audit sistem informasi dan penggunaan kombinasi kriptografi modern dalam pengamanan pesan teks. Audit sistem informasi berfungsi sebagai mekanisme evaluasi untuk memastikan bahwa kebijakan, prosedur, dan standar keamanan diterapkan dengan benar dan konsisten. Di sisi lain, kriptografi modern menyediakan teknologi enkripsi canggih yang melindungi pesan teks dari akses dan manipulasi oleh pihak yang tidak berwenang. Dengan menggabungkan kedua pendekatan ini, kita dapat menciptakan kerangka kerja yang kuat untuk pengamanan pesan teks, memastikan bahwa data tetap aman dan terjamin selama proses pengiriman dan penyimpanan. Hasil penelitian menunjukkan bahwa integrasi audit sistem informasi dengan teknik kriptografi modern secara signifikan meningkatkan tingkat keamanan dan keandalan sistem informasi.

Kata kunci: Elgamal; XOR; Teks

LATAR BELAKANG

Perkembangan zaman membuat teknologi informasi dan komunikasi semakin maju. Proses bertukar pesan atau informasi menjadi semakin mudah dilakukan. Dalam proses bertukar pesan sangat penting menjaga keamanan pesan atau informasi agar pesan tersebut tidak dapat dimengerti oleh pihak lain maupun pihak yang tidak berwenang.

Audit sistem informasi dan kriptografi modern merupakan dua komponen penting dalam menjaga keamanan informasi di era digital. Audit sistem informasi adalah proses evaluasi terhadap infrastruktur TI untuk memastikan kepatuhan terhadap kebijakan, prosedur, dan standar keamanan yang berlaku. Sementara itu, kriptografi modern adalah teknologi yang digunakan untuk melindungi integritas, kerahasiaan, dan keaslian data melalui teknik enkripsi yang canggih.

Received : 15 Juni 2024, Accepted : 02 Juli 2024, Published : 31 Juli 2024
* Dhea Agustina Akmal, agustinadhea91@gmail.com

Kombinasi kedua aspek ini, audit sistem informasi dan kriptografi modern, memberikan kerangka kerja yang kokoh untuk pengamanan pesan teks. Audit sistem informasi memastikan bahwa mekanisme enkripsi diterapkan dengan benar dan dipatuhi secara konsisten, sedangkan kriptografi modern menyediakan alat untuk melindungi data dari akses yang tidak sah dan manipulasi. Dengan demikian, kolaborasi antara audit sistem informasi dan kriptografi modern sangat esensial untuk menciptakan lingkungan yang aman dan terjamin dalam pertukaran informasi teks.

KAJIAN TEORITIS

Kriptografi adalah seni atau ilmu untuk menghasilkan pesan rahasia. Pesan asli, disebut plaintext, disandikan menjadi pesan terenkripsi yang disebut dengan ciphertext melalui proses enkripsi, dan ciphertext diubah kembali menjadi plaintext melalui proses dekripsi. Kriptografi memiliki beberapa algoritma yang banyak digunakan untuk mengamankan informasi. Salah satu algoritma kriptografi yang umum digunakan dalam keamanan adalah algoritma XOR. Algoritma XOR adalah algoritma yang sering digunakan dalam sandi yang menggunakan operasi bit demi bit dan termasuk dalam kriptografi klasik. Algoritma XOR juga merupakan algoritma sederhana yang menggunakan prinsip logika XOR. Untuk proses dimana proses enkripsi dilakukan dengan kunci XOR pada plaintext unntuk mendapatkan cipherteks. Pada proses dekripsi, ciphertext dikodekan dengan XOR dengan kunci untuk mendapatkan teks aslinya (plaintext). Proses enkripsi dan dekripsi tidak sulit dan mudah untuk diimplementasikan.

Algoritma enkripsi OR atau XOR eksklusif adalah sebuah algoritma Kriptografi yang melakukan logika XOR pada setiap biner dalam teks. Algoritma ElGamal adalah sepasang kunci yang dihasilkan dengan memilih bilangan prima p dan dua bilangan acak g dan x, dengan syarat nilai g dan x kurang dari p, yang memenuhi persamaan. Algoritma ElGamal ini memiliki tingkat keamanan dalam pemecahan masalah logaritma diskret pada group pergandaan bilangan prima yang besar, maka upaya untuk memecahkan pesan yang telah dienkripsi menjadi sangat sulit. Selain tingkat keamanan pada pemecahan logaritma diskret, algoritma ElGamal memiliki kelebihan dalam menghasilkan ciphertext (pesan yang telah tersamarkan) yang berbeda untuk plaintext (pesan belum disamarkan, masih dapat dibaca dengan jelas) yang sama pada proses enkripsi, tetapi ketika ciphertext di dekripsi akan menghasilkan plaintext (pesan belum disamarkan, masih dapat dibaca

dengan jelas) yang sama pada proses enkripsi, tetapi ketika ciphertext di dekripsi akan menghasilkan plaintext yang sama.

Proses algoritma ElGamal terdiri atas 3 proses yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Setiap proses dalam algoritma ini menggunakan teori bilangan terutama bilangan prima dan modulo bilangan.Namun di sisi lain, algoritma ElGamal juga mempunyai kekurangan yaitu membutuhkan resource yang besar dan processor yang mampu melakukan perhitungan besar. Meskipun memiliki kelemahan tersebut, namun algoritma ElGamal memiliki kelebihan yang jauh lebih banyak, sehingga dalam paper ini menggunakan algoritma ElGamal dalam meningkatkan keamanan data.

METODE PENELITIAN

a. Kriptografi

Kriptografi adalah studi tentang metode komunikasi yang aman antara dua belah pihak. Biasanya ada dua pihak yang saling mengirim pesan, tetapi mereka ingin menghindari kemungkinan pihak ketiga memahami isi dari pesan mereka jatuh kepada pihak yang salah.

Kriptografi adalah sebuah seni yang berfokus pada menyembunyikan dan mengirimkan pesan secara diam-diam. Banyak sandi yang digunakan sepanjang sejarah, banyak diantaranya sekarang dianggap tidak aman menurut standar modern. Nyatanya, baru pada pertengahan abad ke-20 kriptografi berubah dari seni menjadi sebuah sains .

Kriptografi telah digunakan selama ribuan tahun untuk membantu menyediakan rahasia komunikasi antara pihakpihak yang saling percaya. Dalam bentuknya yang paling dasar, dua orang, sering dilambangkan sebagai Alice dan Bob, telah menyepakati kunci rahasia tertentu. Di lain waktu, Alice mungkin ingin mengirim pesan rahasia ke Bob (atau Bob mungkin ingin mengirim pesan ke Alice). Kunci digunakan untuk mengubah pesan asli (yang biasanya kita sebut dengan plaintext) menjadi bentuk acak yang tidak dapat dipahami kepada siapa saja yang tidak memiliki kunci. Proses ini disebut enkripsi, dan pesan yang diacak disebut ciphertext. Ketika Bob menerima ciphertext, dia dapat menggunakan kunci untuk mengubah ciphertext kembali menjadi plaintext atau teks asli, ini disebut dengan proses dekripsi.

b. Elgamal

El-Gamal adalah sistem enkripsi kunci asimetris yang ditemukan Taher El-Gamal pada tahun 1985. Algoritma ini merepresentasikan metode alternatif untuk cipher kunci publik RSA. Perbedaan utama antara algoritma El Gamal dan RSA adalah bahwa keamanan RSA bergantung pada kesulitan faktorisasi bilangan prima besar, sementara El-Gamal bergantung pada kesulitan dalam menghitung modulus logaritmik diskrit dari bilangan prima besar. Masalah logaritma diskrit adalah masalah sulit dalam matematika karena itu penting terutama pada konjungtur untuk mendapatkan semua solusi yang mungkin. Jadi sistem crypto ini hampir rusak tidak tersedia atau membutuhkan waktu lama. Terutama Keunggulan teknologi El Gamal adalah pesan teks yang sama menghasilkan pesan teks rahasia yang berbeda setiap saat jika dienkripsi.

Algoritma ElGamal adalah sepasang kunci yang dihasilkan dengan memilih bilangan prima p dan dua bilangan acak g dan x, dengan syarat nilai g dan x kurang dari p, yang memenuhi persamaan. ElGamal dapat digunakan untuk tanda tangan digital dan enkripsi, keamanannya bergantung pada kesulitan menghitung logaritma diskrit dalam bidang yang terbatas. Untuk menghasilkan pasangan kunci, pertama pilih bilangan prima, p, dan dua bilangan acak, g dan x, sehingga g dan x keduanya lebih kecil dari p, lalu hitung = $gX\ mod$. Kunci publiknya adalah y, g dan p. Baik g dan p dapat dibagikan oleh sekelompok pengguna. Kunci pribadinya adalah X.

Proses Pembentukan Kunci El-Gamal pembentukan kunci merupakan proses penentuan suatu bilangan yang kemudian akan digunakan sebagai kunci pada proses enkripsi dan dekripsi pesan. Kunci untuk enkripsi dibangkitkan dari nilai p, g, y sedangkan kunci untuk dekripsi terdiri dari nilai x, p. Masing-masing nilai mempunyai persyaratan yang harus dipenuhi. Langkah-langkah dalam pembuatan kunci adalah sebagai berikut:

1. Pilih sembarang bilangan prima p, dengan syarat $p > 255$.
2. Pilih bilangan acak g dengan syarat $g < p$.
3. Pilih bilangan acak x dengan syarat $1 = x = p - 2$.
4. Hitung $y = gpmod\ p$.

Kunci public adalah y, g, p sedangkan kunci private adalah x. Nilai y, g, dan p tidak dirahasiakan sedangkan nilai x harus dirahasiakan karena merupakan kunci private untuk mendekripsi plaintext

c. Algoritma XOR

Teknik XOR melakukan enkripsi dan dekripsi terhadap sebuah informasi dengan menggunakan kunci tunggal dan operasi bit XOR.[11] Tabel logika dari operasi XOR adalah sebagai berikut:

Tabel 1. Tabel Logika Operasi XOR

A	B	A ⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Proses Enkripsi XOR atau dekripsi di awali dengan merubah setiap nilai plaintext ke biner Formula untuk melakukan proses enkripsi dan dekripsi adalah :

Enkripsi : $\boldsymbol{Ci} = \boldsymbol{Pi\ XOR\ Ki}$

Deskripsi : $\boldsymbol{Pi} = \boldsymbol{Ci\ XOR\ k}$

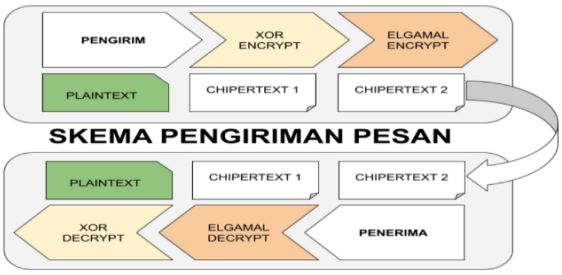
HASIL DAN PEMBAHASAN

1. Pengertian Perancangan

Perancangan adalah Proses untuk mendefinisikan sesuatu yang akan dikerjakan dengan menggunakan teknik yang bervariasi serta didalamnya melibatkan deskripsi mengenai arsitektur serta detail komponen dan juga keterbatasan yang akan dialami dalam proses pengerjaannya. Perancangan adalah suatu proses untuk membuat dan mendesain sistem yang baru.

Berdasarkan pengertian diatas dapat disimpulkan bahwa perancangan sistem adalah sebuah proses setelah analisis dari siklus pengembangan sistem untuk merancang suatu sistem.

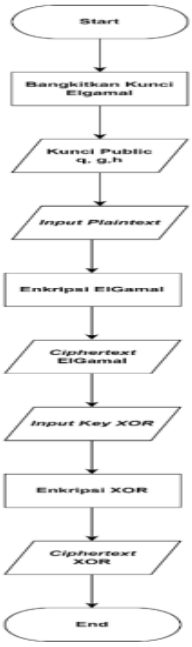
2. Rancangan Penelitian



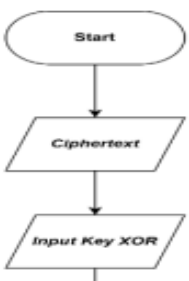
Pada gamba grafi hybrid yang mengimplementasikan penggabungan dua teknik kriptografi yang berbeda, yaitu ElGamal dan algoritma XOR, untuk pengiriman pesan. Pada tahap pertama, pesan asli dienkripsi menggunakan algoritma XOR dengan menggunakan kunci XOR yang diinputkan oleh pengguna. Proses ini bertujuan untuk memastikan kerahasiaan dan

integritas pesan saat pengiriman. Setelah itu, pesan terenkripsi pertama (chipertext 1) yang dihasilkan dari tahap XOR akan dienkripsi kembali menggunakan skema ElGamal yang akan menghasilkan pesan terenkripsi kedua (chipertext 2) yang selanjutnya akan dikirimkan pada penerima. Pada bagian penerima dilakukan proses dekripsi dengan cara melakukan dekripsi elgamal pada pesan terenkripsi (chipertext 2) yang diterima sehingga menghasilkan pesan terdekripsi pertama (chipertext 1). Kemudian pesan terdekripsi pertama akan didekripsi kembali menggunakan proses dekripsi xor yang kemudian menghasilkan pesan aslinya.

Untuk lebih mengetahui bagaimana kedua metode tersebut dapat mengamankan pesan dengan baik dapat dilihat melalui gambar dibawah ini.

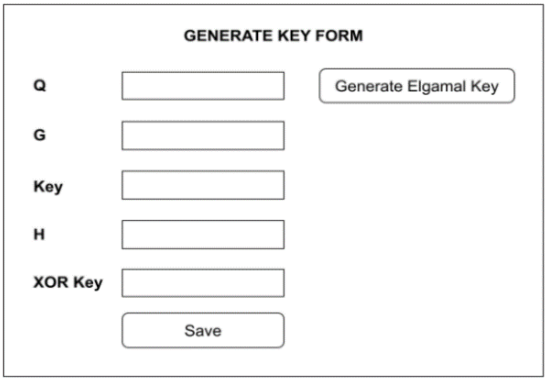


Pada gambar 2 dapat kita lihat flowchart enkripsi ElGamal dan XOR, dimana flowchart dimulai dari start kemudian bangkitkan (Generate) kunci elgamal yang nantinya akan menghasilkan nilai q, g, h. Kemudian setelah membangkitkan kunci, maka kita masukkan plaintext yang akan kita enkripsi. Kemudian enkrip plaintext dengan menggunakan algoritma ElGamal. Kemudian hasil enkripsi akan menghasilkan ciphertext dari algoritma ElGamal. Kemudian ciphertext ElGamal ini kita enkripsi kembali dengan menggunakan algoritma XOR dengan menggunakan kunci XOR. Kemudian ciphertext ElGamal tersebut sudah berhasil kita rubah menjadi ciphertext algoritm XOR. Kemudian untuk mendekripsi pesan yang telah di enkripsi dapat kita lihat pada gambar 3. berikut ini.

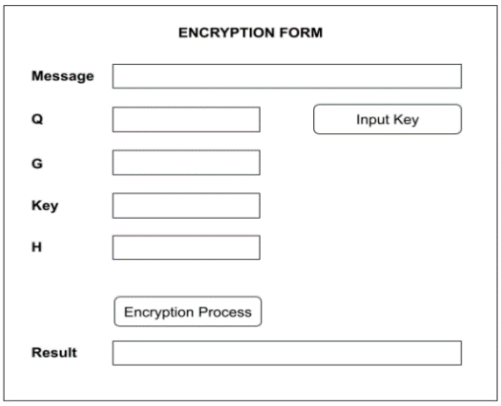


Pada gambar 3 dapat kita lihat flowchart dekripsi algoritma ElGamal dan XOR dimana flowchart dimulai dari Start. Kemudian masukkan ciphertext yang akan didekripsi. Kemudian kita masukkan kunci XOR, kemudian proses dekripsi XOR dilakukan. Kemudian setelah proses XOR berhasil dilakukan, maka ciphertext akan berubah menjadi ciphertext algoritma ElGamal. Ciphertext dari algoritma ElGamal ini akan kita dekripsi Kembali dengan menggunakan kunci private algoritma ElGamal. Kemudian proses dekripsi algoritma ElGamal dilakukan yang nantinya ciphertext algoritma ElGamal akan menghasilkan plaintext seutuhnya atau menjadi pesan yang sempurna.

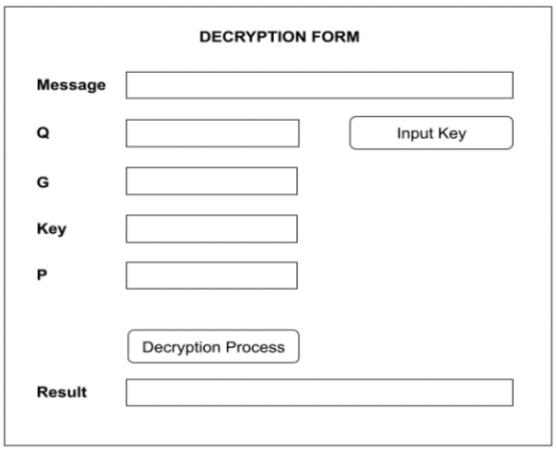
3. Rancangan Antarmuka



Pada gambar perancangan diatas dapat dilihat bahwa terdapat beberapa variabel yang akan dibangkitkan yaitu variabel Q, G, H, Key yang dapat dimasukkan secara manual atau atau otomatis melalui tombol generate dan XOR Key yang hanya dapat dimasukkan secara langsung oleh pengguna. Kemudian setelah pengguna menetapkan variabel-variabel yang dibutuhkan maka selanjutnya seluruh variabel tersebut akan secara otomatis disimpan kedalam sebuah file teks dengan nama kunci_enkrip.txt.



Dari gambar diatas dapat kita lihat bahwa dalam antarmuka enkripsi memuat beberapa fungsi seperti fungsi untuk memasukkan pesan di kotak teks “Message” dan terdapat juga tempat untuk menampung kunci-kunci variabel elgamal seperti Q, G, Key, H yang bagian-bagian tersebut dapat diunggah dari sebuah file yang diperoleh dari proses pembangkitan kunci sebelumnya. Untuk melakukan proses enkripsi pengguna dapat menekan tombol “Encryption Process” untuk menghasilkan ciphertext yang bersamaan dengan itu juga menghasilkan file teks dengan nama kunci_dekrip.txt untuk proses dekrip nantinya.



Pada gambar diatas dapat dilihat bahwa rancangan antarmuka dekripsi memiliki kemiripan dengan enkripsi namun memiliki perbedaan pada variabel P dimana pada proses dekripsi menggunakan parameter P sebagai private key untuk melakukan dekripsi pada chipertext yang telah dimasukkan pada kotak teks pesan "Message".

KESIMPULAN DAN SARAN

Studi ini mengungkapkan bahwa penggunaan kombinasi kriptografi modern memiliki potensi besar untuk meningkatkan keamanan pesan teks. Dengan menggabungkan teknik-teknik kriptografi seperti enkripsi simetris dan asimetris, serta penggunaan tanda tangan digital dan algoritma hash, dapat diperkuat keamanan data dalam komunikasi digital. Kriptografi modern tidak hanya menyediakan mekanisme untuk menjaga kerahasiaan dan integritas pesan, tetapi juga mampu mengatasi tantangan baru seperti serangan komputasi kuantum. Penelitian ini juga menyoroti perlunya keseimbangan antara keamanan yang kuat dan efisiensi operasional dalam penerapan kombinasi kriptografi ini.

Dengan mempertimbangkan kesimpulan yang mencakup potensi keamanan yang ditingkatkan oleh kriptografi modern dan saran untuk memperluas penelitian lebih lanjut, jurnal ini dapat memberikan kontribusi yang berharga terhadap peningkatan praktik keamanan informasi di masa depan.

DAFTAR REFERENSI

Alfiah, F., Sudarji, R., & Taqiyyuddin Al Fatah, D. (2020). Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake, 12260.

Iqbal, H., & Krawec, W. O. (2020). Semi-quantum cryptography. In *Quantum Information Processing*, *19*(3). Springer US. https://doi.org/10.1007/s11128-020-259

Makhomah, R., Santoso, K. A., & Kamsyakawuni, A. (2021). Pengkodean Teks Menggunakan Kombinasi Hill Cipher dan Operasi XOR. *PRISMA, Prosiding Seminar Nasional Matematika*, *4*, 548–552.

Rubinstein_Salzedo, S. (2018). *Cryptography*. Springer Cham. https://doi.org/10.1007/978-3-319-94818-8.

Saputro, Pujo, H. (2023). Implementasi Algoritma Exclusive OR (XOR) Dalam Pengembangan Aplikasi Chat Berbasis Android. *Informatika Fakultas Sains & Teknologi Universitas Labuhan Batu, 11*(1), 71–76.

Sulaiman, O. K., Nasution, K., & Siambaton, M. Z. (2020). Three Pass Protocol untuk Keamanan Kunci Berbasis Base64 pada XOR Cipher. *Jurnal Sains Komputer & Informatika (J-SAKTI), 4*(September), 721–727.

Yusfrizal. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Cipher Dan RSA Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK), 3*(2), 29–3.