PENGEMBANGAN KUNCI ENKRIPSI ASIMETRIS PADA VIGENERE CHIPER

Desyderius Minggu, Ricki Septian Nurptratama*, Riyant Budi Setiawan
Jurusan Telekomunikasi, Politeknik Angkatan Darat
Junrejo, Kota Batu, Jawa Timur-Indonesia 65324
ricki.firewall@gmail.com

ABSTRAK

Keamanan data merupakan aspek krusial dalam sistem informasi. Berbagai metode enkripsi terus dikembangkan untuk melindungi kerahasiaan data. Salah satu metode enkripsi yang sering digunakan adalah Vigenere Cipher, sebuah metode substitusi teks. Kelemahan utama Vigenere Cipher terletak pada penggunaan kunci simetris, yang rentan terhadap serangan kriptoanalisis, terutama jika panjang kunci tidak sebanding dengan panjang teks. Beberapa penelitian sebelumnya telah mencoba meningkatkan keamanan Vigenere Cipher melalui penggabungan teknik enkripsi lain seperti fungsi acak, algoritma Blum Blum Shub, serta pendekatan berbasis waktu. Meski demikian, metode-metode ini masih memiliki keterbatasan dalam hal distribusi kunci yang tetap bersifat simetris. Penelitian ini bertujuan untuk mengatasi kelemahan tersebut dengan mengembangkan kunci enkripsi asimetris yang dapat diterapkan pada Vigenere Cipher. Dengan mengadopsi mekanisme kunci publik dan kunci privat, diharapkan keamanan distribusi kunci dapat ditingkatkan, sehingga dapat meminimalisir risiko serangan kriptoanalisis. Metode penelitian ini mencakup desain dan implementasi skema kunci asimetris pada enkripsi Vigenere serta evaluasi keamanan dan efisiensi skema yang dihasilkan. Hasil penelitian ini diharapkan dapat berkontribusi pada pengembangan metode enkripsi yang lebih aman dan efisien, yang dapat diterapkan dalam berbagai aplikasi keamanan data.

Kata kunci : *Vigenere, Chiper, enkripsi*

1. PENDAHULUAN

Keamanan data menjadi salah satu kebutuhan mendesak di era digital saat ini, di mana informasi sering kali dipertukarkan melalui jaringan yang rentan terhadap penyadapan dan serangan pihak ketiga. Untuk melindungi data, salah satu metode klasik yang digunakan adalah enkripsi, yang mengonversi informasi asli menjadi bentuk terenkripsi yang sulit dipahami tanpa kunci yang sesuai. Vigenere Cipher adalah salah satu algoritma enkripsi klasik yang banyak diterapkan karena kesederhanaannya. Algoritma ini bekerja dengan cara substitusi teks menggunakan kunci, di mana setiap karakter dalam teks asli dienkripsi menggunakan karakter dalam kunci secara berulang [1]. Namun, kelemahan utama Vigenere Cipher terletak pada penggunaan kunci simetris, yang rentan terhadap serangan kriptoanalisis, terutama jika panjang kunci lebih pendek atau sama dengan teks sehingga kunci perlu diulang. Hal ini mempermudah deteksi pola dan memudahkan serangan berbasis statistik [2].

Untuk mengatasi kelemahan ini, beberapa penelitian telah menggabungkan Vigenere Cipher dengan teknik keamanan lainnya. Salah satu upaya awal adalah dengan mengombinasikan steganografi berbasis Least Significant Bit (LSB) pada enkripsi Vigenere untuk menyembunyikan pesan dalam citra digital, sehingga meningkatkan tingkat keamanan [1]. Namun, kelemahan distribusi kunci simetris tetap menjadi tantangan utama. Penelitian lainnya telah mencoba menggunakan modifikasi Autokey untuk memperpanjang kunci secara dinamis, meskipun pendekatan ini masih terbatas dalam keamanan distribusi kunci [2].

Selain itu, beberapa pendekatan telah memperkenalkan lapisan kunci tambahan, seperti kombinasi fungsi acak, angka Euler, dan algoritma Blum Blum Shub. Pendekatan berlapis ini bertujuan untuk meningkatkan keamanan dengan menghasilkan kunci yang lebih acak dan sulit diprediksi [3]. Namun, sifat simetris dari kunci yang digunakan masih menimbulkan masalah keamanan dalam proses distribusi.

Pendekatan lain mencoba menggabungkan kunci berbasis string dan waktu penyisipan dengan metode One Time Pad (OTP) dan Message Digest 5 (MD5) untuk menghasilkan kunci yang lebih aman. Metode ini bertujuan untuk meningkatkan variasi kunci sehingga lebih sulit untuk dipecahkan [4][5]. Meskipun pendekatan ini memberikan peningkatan keamanan, kelemahan distribusi kunci simetris tetap ada, sehingga metode ini masih kurang efektif untuk menghadapi serangan pada proses distribusi kunci.

Beberapa penelitian telah menunjukkan bahwa pendekatan berbasis budaya, seperti penggunaan simbol budaya Jawa yang disebut sengkalan, dapat diterapkan dalam kriptografi untuk memberikan elemen unik pada pengamanan data [6]. Namun, aplikasi metode ini masih terbatas pada konteks tertentu. Pada sisi lain, algoritma hashing seperti SHA-1 telah lama digunakan untuk menjaga integritas data, meskipun penerapannya lebih umum pada pengamanan hash dibanding enkripsi kunci [7].

Pendekatan hybrid yang menggabungkan Vigenere Cipher dengan algoritma hashing atau enkripsi berbasis waktu telah menunjukkan potensi untuk meningkatkan keamanan data dalam berbagai aplikasi [8][9]. Penggunaan algoritma kriptografi

modern juga telah dilakukan untuk memperkuat enkripsi klasik pada data besar, yang memberikan hasil yang lebih baik terhadap serangan kriptoanalisis [10].

Penelitian ini bertujuan untuk mengatasi kelemahan utama pada Vigenere Cipher dengan mengembangkan metode enkripsi kunci asimetris. Dengan menerapkan kunci publik dan kunci privat, kelemahan distribusi kunci pada skema kunci simetris dapat diminimalkan. Diharapkan penerapan kunci asimetris pada Vigenere Cipher ini dapat memperkuat keamanan keseluruhan, khususnya dalam distribusi kunci, sehingga meningkatkan efektivitas metode ini dalam pengamanan data.

2. TINJAUAN PUSTAKA

Keamanan data telah menjadi perhatian utama dalam teknologi informasi, terutama dengan berkembangnya kebutuhan perlindungan data di berbagai aplikasi. Enkripsi Vigenere, yang merupakan teknik substitusi teks, telah lama digunakan sebagai salah satu metode untuk mengamankan data melalui penerapan kunci pada teks asli. Meskipun demikian, kelemahan utama dari Vigenere Cipher adalah pada penggunaan kunci simetris yang berisiko terhadap serangan kriptoanalisis. Ketika panjang kunci lebih pendek dari teks, kunci harus diulang, yang menyebabkan pola dapat dikenali dan memudahkan serangan [1].

Upaya awal untuk meningkatkan keamanan Vigenere Cipher adalah dengan menggabungkannya dengan teknik steganografi berbasis Least Significant Bit (LSB). Teknik ini menyembunyikan pesan dalam gambar digital sehingga dapat memberikan lapisan keamanan tambahan [1]. Namun, kelemahan utama tetap terletak pada penggunaan kunci simetris yang membutuhkan distribusi kunci secara langsung.

Berbagai penelitian telah dilakukan untuk mengatasi kelemahan ini. Salah satu pendekatan yang signifikan adalah penggunaan modifikasi Autokey pada Vigenere Cipher. Metode ini bertujuan untuk meningkatkan keamanan dengan menciptakan kunci yang lebih bervariasi, namun masih memiliki keterbatasan dalam hal distribusi kunci yang bersifat simetris [2]. Metode lain yang menggunakan kunci tiga lapis dengan memanfaatkan fungsi acak, angka Euler, dan algoritma Blum Blum Shub telah berhasil meningkatkan keamanan kunci pada Vigenere Cipher, namun tetap mempertahankan kunci simetris [3].

Lebih lanjut, penelitian yang menggabungkan dua kunci, yaitu kunci berbentuk string normal dan kunci berbasis waktu, telah dikembangkan. Teknik ini bertujuan untuk memperluas variasi kunci yang digunakan, sehingga lebih sulit bagi pihak tidak sah untuk mendekripsi pesan [4]. Selain itu, penelitian lain menggabungkan One Time Pad (OTP) dan Message Digest 5 (MD5) pada enkripsi Vigenere untuk menghasilkan kunci yang lebih acak dan kuat, meskipun masalah mendasar terkait simetri kunci tetap belum terselesaikan [5].

Alternatif lain untuk meningkatkan keamanan data dalam enkripsi adalah melalui pendekatan budaya, seperti pengenalan simbol budaya Jawa (sengkalan) sebagai komponen tambahan dalam pengamanan data. Pendekatan ini mencoba menggabungkan budaya lokal dengan teknik enkripsi untuk memperkuat kerahasiaan [6]. Namun, meskipun inovatif, penerapannya terbatas dalam skala tertentu dan belum memiliki standar keamanan yang memadai.

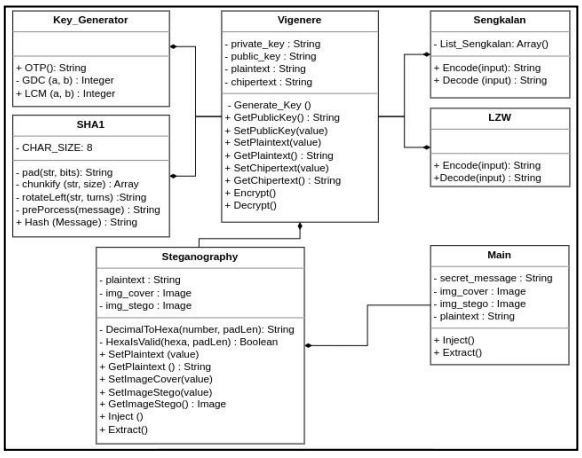
Secara umum, hashing telah digunakan dalam berbagai penelitian untuk memperkuat enkripsi data. Algoritma hashing seperti SHA-1 sering kali diimplementasikan untuk menjaga integritas data selama proses transmisi dan penyimpanan [7]. Hashing juga menjadi bagian penting dalam pendekatan hybrid, yang menggabungkan metode enkripsi Vigenere dengan algoritma hashing untuk mengamankan kunci distribusi [8].

Pendekatan lain menggunakan enkripsi berbasis waktu untuk meningkatkan keamanan data. Dengan memanfaatkan perubahan waktu sebagai elemen dalam proses enkripsi, penelitian ini bertujuan untuk menghasilkan kunci yang lebih dinamis [9]. Selain itu, penggunaan algoritma kriptografi modern pada Vigenere Cipher juga telah dilakukan untuk meningkatkan ketahanan enkripsi pada data yang lebih kompleks dan besar [10].

Melihat kelemahan dari metode-metode yang telah dibahas, penelitian ini mengusulkan pengembangan enkripsi kunci asimetris yang diterapkan pada Vigenere Cipher. Dengan menerapkan kunci publik dan privat, kelemahan distribusi kunci pada skema simetris diharapkan dapat diatasi, sehingga meningkatkan keamanan keseluruhan.

3. METODE PENELITIAN

Kontribusi penelitian pertama adalah mengimplementasikan enkripsi Vigenere yang dilengkapi dengan kunci asimetris (kunci publik dan kunci privat). Para peneliti mengimplementasikannya ke dalam 5 kelas, yaitu (1) Pembangkit Kunci, (2) Enkoding Sengkalan,



Gambar 1. *Class Diagram*

Penjelasan rinci tentang setiap langkah dalam kontribusi penelitian pertama dapat dilihat dalam diskusi berikut.

3.1. Tahap 1: Menghasilkan One Time Password (OTP)

Pada tahap 1, sistem secara otomatis menghasilkan angka acak sebanyak 4 digit. Tujuan dari implementasi metode ini adalah agar kunci enkripsi selalu berubah setiap kali proses enkripsi dilakukan. Persamaan matematis pada tahap 1 terlihat seperti rumus untuk persamaan 1 di bawah ini.

$$OTP = password + \sum_{i=1}^{4} IntToStr([\lfloor Math.Random() \times 10 \rfloor])$$

Tahap 1. Menghasilkan *One Time Password (OTP)*

Dimana OTP adalah data dalam bentuk string yang terdiri dari 4 karakter. OTP ini merupakan kunci asli, yang nantinya akan dimodifikasi untuk menjadi kunci privat dan kunci publik.

3.2. Tahap 2: Menghitung Least Common Multiple (LCM) dari OTP

Tujuan dari tahap 2 adalah untuk memodifikasi OTP guna menghasilkan angka yang tidak sama dengan hasil OTP. Selanjutnya, hasil dari tahap 2 akan digunakan untuk membentuk kunci privat, yang akan diimplementasikan dalam enkripsi substitusi. Persamaan matematis pada tahap 2 terlihat seperti rumus untuk persamaan 2 di bawah ini.

$$GCD(a,b) = \begin{cases} a & if\ b = 0 \\ GCD(a,b) & if\ b \neq 0 \end{cases} \quad (2)$$

$$LCM(a,b) = \frac{(a \times b)}{GCD(a,b)}$$

Dimana:
a = Panjang String Nomor OTP = 4
b = Nomor OTP
gcd = faktor persekutuan terbesar (greatest common divisor)

Tahap 2. Menghitung *Least Common Multiple (LCM)* dari *OTP*

3.3. Tahap 3 : Menghasilkan hash dari Hasil Least Common Multiple (LCM)

Pada tahap 3, ini adalah tahap untuk membentuk kunci privat sebenarnya, di mana kunci privat ini nantinya akan digunakan dalam tahap enkripsi. Untuk lebih mengamankan kunci privat ini, mekanisme yang diterapkan adalah mengacak (hash) hasil dari proses pada langkah 2. Untuk mengacak (hash) dalam penelitian ini, digunakan metode Secure Hash Algorithm versi 1 (SHA-1). Peneliti tidak membahas alur proses SHA-1 secara rinci, karena peneliti memanfaatkan fungsi SHA-1 yang tersedia dalam Request For Comments (RFC) 3174 (Eastlake, 2001). Persamaan matematis pada tahap 3 terlihat seperti rumus untuk persamaan 3 di bawah ini.

1. Initialization (3)
   a) $H_0, H_1, H_2, H_3, H_4 =$ *are the initial values used to init*
2. Pesan padding
   a) Pesan masukan dipad ke dalam bentuk yang dapat diproses, biasanya dengan menambahkan padding dan informasi tentang panjang pesan.Message Block Splitting:
   b) Pesan yang telah dipadding dibagi menjadi blok-blok lebih kecil, biasanya masing-masing berukuran 512 bit.
3. Pesan Block Expansion:
   a) Setiap blok pesan diperluas menjadi 80 kata dengan panjang 32 bit.
4. Inisialisasi Variabel:
   a) Variabel internal seperti A, B, C, D, E diinisialisasi dengan nilai H_0, H_1, H_2, H_3, H_4.
5. Pemrosesan Blok Pesan:
   a) I Melibatkan serangkaian operasi logika bitwise, rotasi bit, dan fungsi non-linear.
6. Updating Hash Values:
   a) After processing each message block, the values of H_0,H_1,H_2,H_3,H_4 are updated with the results of the processing.
7. Iterasi:
   a) Pemrosesan blok pesan diulang hingga seluruh pesan selesai diproses.
8. Kunci Privat (PvK): Nilai hash akhir H_0, H_1, H_2, H_3, H_4 diambil sebagai output hash SHA-1.

Tahap 3. Menghasilkan hash dari Hasil *Least Common Multiple (LCM)*

3.4. Tahap 4 : Mengenkripsi dan Mendekripsi OTP menjadi Kalimat Sengkalan

Sengkalan adalah budaya yang berasal dari masyarakat Pulau Jawa, Indonesia. Ungkapan - ungkapan sengkalan adalah bentuk ekspresi masyarakat Jawa. Definisi sengkalan adalah kalimat dan kata-kata yang memiliki karakter angka. Dari kalimat atau kata-kata ini, angka tahun dibentuk seperti yang tertulis di gerbang rumah atau pemakaman (Adi, 2014). Contoh pengkarakteran angka menjadi kata sengkalan ditunjukkan dalam Tabel 1 di bawah ini.

Symbol	List of Sengkalan Sentences
0	Akasa, Awang-Awang, Barakan, Ilang, Sirna, etc.
1	Badan,Budha,Budi, Bumi,Candra,Karta, etc.
2	Apasang, Asta, Athi-athi, Buja, Bujana, etc.
3	Agni, Api, Apyu, Bahni, Benter, etc.
4	Bun, Catur, Dadya, Gawe, Karta, etc.
5	Angin, Astra, Bajra, Bana, Bayu, etc.
6	Amla, Anggana, Anggang-Anggang, Amnggas, Artati, etc.
7	Acala, Ajar, Angsa, Ardi, Arga, etc.
8	Anggusti, Astha, Bajul, Basu, Basuki, etc.
9	Ambuka, Anggangsir, Angleng, Angrong, Arum, etc.

Tabel 1. Simbol Kalimat Sengkalan

Sebagai contoh, kalimat sengkalan "Sirna Ilang Kartaning Bumi", jika diterjemahkan secara harfiah, artinya "Kemakmuran bumi telah hilang." Namun, makna sebenarnya tidak seperti itu. Makna menurut ilmu sengkalan adalah bahwa "Sirna" adalah simbol untuk angka 0, "ilang" adalah simbol untuk angka 0, "kartaning" atau "karta" adalah simbol untuk angka 4, dan "bumi" adalah simbol untuk angka 1. Ketika diatur, angka-angka tersebut menjadi 0041. Jika dibaca dari belakang ke depan, ini menjadi angka 1.400. Angka ini menunjukkan tahun 1.400 Saka atau 1.478 M (Adi, 2014).

Dalam penelitian ini, aturan sengkalan digunakan untuk menunjukkan karakter On Time Password. Dengan menambahkan kontribusi penggabungan Sengkalan dengan On Time Password, dapat dihasilkan kunci publik yang berbeda dari kunci privat. Berdasarkan ini, untuk mengkodekan metode Sengkalan ke dalam sistem keamanan enkripsi kunci publik, dapat dijelaskan dalam persamaan matematis seperti persamaan 4 di bawah ini. Untuk keperluan proses dekripsi, kalimat "sengkalan" ini harus dikembalikan (didekode) menjadi OTP. Persamaan matematis untuk proses dekripsi kalimat Sengkalan ini terlihat seperti persamaan 4 di bawah ini.

$$L = \begin{bmatrix} a01\ a02 \dots a0n \\ a11\ a12 \dots a1n \\ \dots \\ a91\ a92 \dots a9n \end{bmatrix} \quad (4)$$

Encode :

$$Encode(input) = Sengkalan + \sum_{k=0}^{n-1} L[ordinal(input,k)][M \times n]$$

Dimana :
Input = the OTP, example 1400.
L = Daftar Kalimat Sengkalan. Contoh: a01 = Sirna, a02 = Ilang, a11 = Bumi, etc
n = Jumlah kata untuk setiap karakter angka dalam kalimat “sengkalan”.
Sengkalan = Kalimat Sengkalan. Contoh input= 1400 maka kalimat Sengkalan = Bumi Karta Sirna Ilang.

Decode :

$$Decode(input) = \sum_{i=0}^{n-1} \left(\sum_{rows=0}^{9} \sum_{cols=0}^{100} cols \cdot \delta(L[rows][cols], input[i]) \cdot \delta(found, false) \cdot \delta(rows, 9) \right) \cdot 10^{n-1-i}$$

Dimana:
input = Kalimat Sengkalan. Contoh: "Sirna Ilang Karta Bumi"
n = jumlah kata untuk setiap angka karakter "sengkalan".
baris = jumlah baris simbol kalimat sengkalan (0..9)
kolom = jumlah kolom kalimat sengkalan untuk setiap simbol
L = Daftar Kalimat Sengkalan. Contoh: a01 = Sirna, a02 = Ilang, a11 = Bumi, dll.

Tahap 4. Mengenkripsi dan Mendekripsi *OTP* menjadi Kalimat Sengkalan

Sebelumnya peneliti sudah menjelaskan langkah demi langkah dari Algoritma dan kelas diagram untuk mengembangkan metode penelitian yang diusulkan.

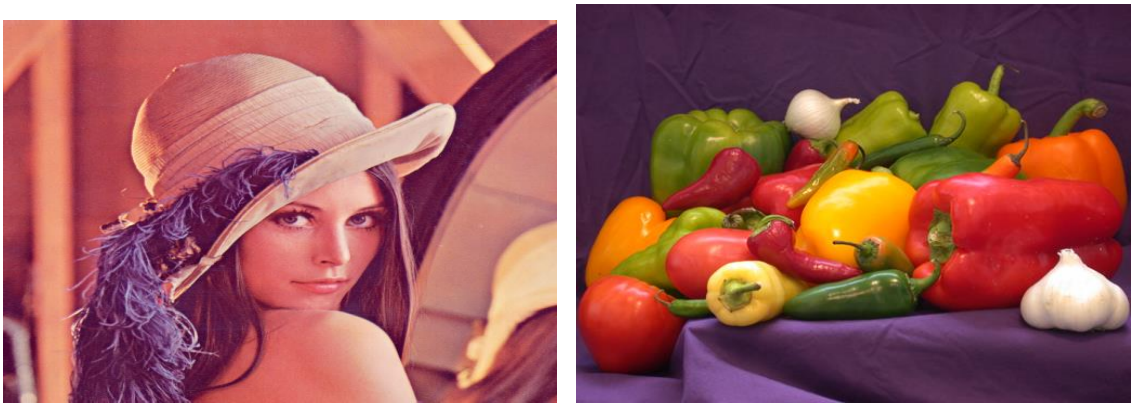
4. HASIL DAN PEMBAHASAN

Program dalam penelitian ini mendukung Antarmuka Pengguna Grafis (GUI). Studi eksperimental dilakukan dalam empat tahap menggunakan GUI. Tahap-tahap ini dijelaskan sebagai berikut:

a. Gambar Cover: Pada tahap ini, gambar penutup diunggah dari kamera atau file menggunakan GUI.
b. Pesan Rahasia: Pengguna mengunggah pesan yang ingin disembunyikan dalam gambar penutup secara manual.

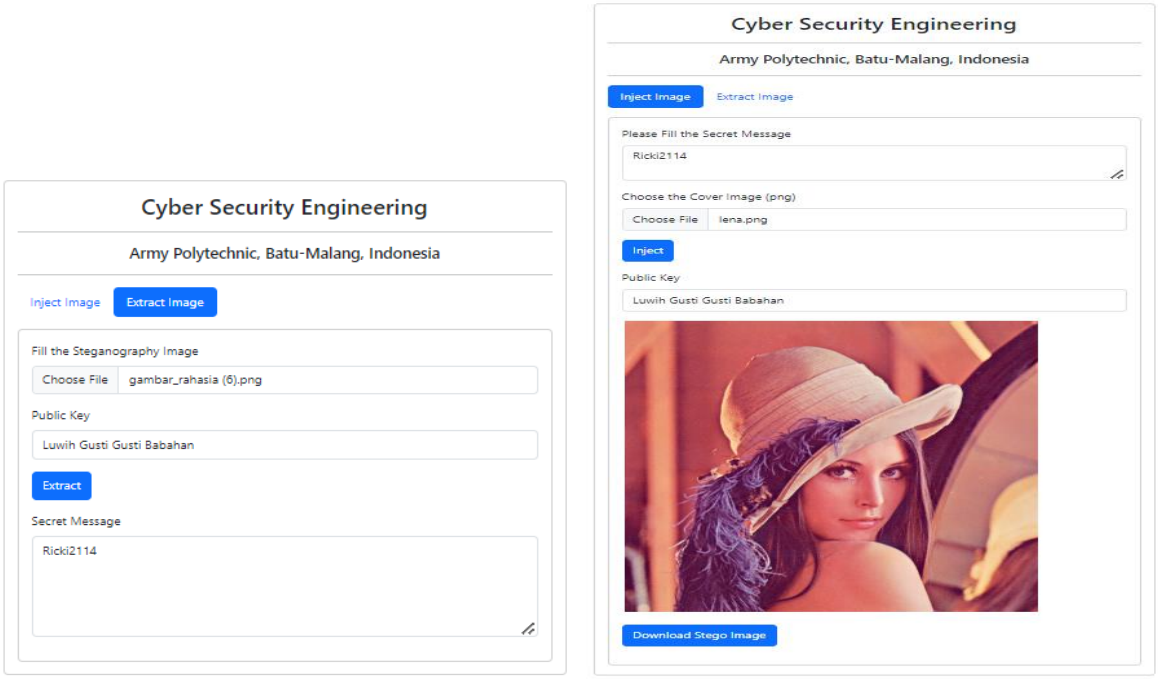
Menyembunyikan Data Dengan Menggeser Bit Sengkalan: Pada fase ini, pesan rahasia yang telah dienkripsi disisipkan ke dalam gambar penutup. Proses ini melibatkan pergeseran Bit Paling Tidak Signifikan (LSB) dari nilai piksel dalam gambar penutup.

Pada Gambar 2 menampilkan gambar-gambar yang digunakan dalam studi eksperimental ini. Pada Gambar 3, ditampilkan contoh gambar antarmuka pengguna (GUI) Steganografi.



(a) (b)

Gambar 2. Gambar Cover (a) Lena dan (b) Pepers



(a) (b)

Gambar 3. Antarmuka Pengguna (GUI) untuk Steganografi (a) *Inject* dan (b) *Extract*

```
=== GENERATE KEY ===
OTP : 9111
LCM(4, 9111) : 36444
Private Key : 36444
Public Key : Luwih Gusti Gusti Babahan
=== ENCRYPT ===
Plaintext : Ricki2114
Chipertext: □□□□□egeh
 === INJECT ====
Hidden Message 000009□□□□□egeh
=== DECRYPT ===
Public Key : Luwih Gusti Gusti Babahan
Chipertext : □□□□□egeh
Origin Key (OTP) : 9111
LCM(4, 9111) : 36444
Private Key : 36444
Plaintext : Ricki2114
```

Gambar 4. Hasil Analisa

Gambar 4 menunjukkan skema steganografi gambar yang menggunakan metode Least Significant Bit (LSB) untuk menyisipkan pesan rahasia ke dalam gambar. Metode LSB adalah salah satu metode steganografi yang paling sederhana dan umum digunakan. Metode ini bekerja dengan mengubah nilai bit paling kanan (LSB) dari beberapa pixel dalam gambar untuk mewakili bit dari pesan rahasia.

Pada gambar tersebut, proses steganografi dilakukan dalam beberapa langkah berikut:

a. Generate Key

Proses pertama adalah menghasilkan kunci untuk digunakan dalam proses enkripsi dan steganografi. Kunci ini terdiri dari dua bagian, yaitu OTP (One Time Pad) dan LCM (Least Common Multiple). OTP adalah kunci acak yang hanya digunakan satu kali. LCM adalah kelipatan persekutuan terkecil dari OTP dan lebar gambar.

b. Enkripsi Pesan
   Pesan rahasia yang akan disisipkan ke dalam gambar terlebih dahulu harus dienkripsi menggunakan kunci OTP. Enkripsi OTP adalah metode enkripsi yang sangat kuat karena menggunakan kunci acak yang tidak dapat diprediksi.
c. Penyisipan Pesan
   Setelah pesan dienkripsi, pesan tersebut kemudian disisipkan ke dalam gambar menggunakan metode LSB. Proses ini dilakukan dengan mengubah nilai LSB dari beberapa pixel dalam gambar untuk mewakili bit dari pesan rahasia.
d. Deskripsi Pesan
   Untuk mendekripsi pesan yang disisipkan ke dalam gambar, proses yang sama dilakukan secara terbalik. Pertama, nilai LSB dari beberapa pixel dalam gambar dikembalikan ke nilai aslinya. Kemudian, pesan rahasia didekripsi menggunakan kunci OTP.

Pada gambar pesan rahasia yang disisipkan adalah "Ricki2114". Pesan ini disisipkan ke dalam gambar "2222Degeh". Pesan rahasia tersebut dapat dilihat dengan menggunakan alat dekompresi gambar.

Secara keseluruhan, skema steganografi yang ditunjukkan pada gambar tersebut memiliki beberapa kelebihan, yaitu:

- Mudah untuk diterapkan
- Tingkat keamanan yang tinggi
- Tidak mengubah kualitas gambar secara signifikan

Namun, skema steganografi ini juga memiliki beberapa kekurangan, yaitu:

- Dapat dideteksi menggunakan teknik steganalysis.
- Kapasitas penyimpanan pesan yang terbatas.

Untuk meningkatkan keamanan skema steganografi ini, dapat dilakukan beberapa hal, yaitu:

- Menggunakan algoritma enkripsi yang lebih kuat
- Menggunakan teknik steganografi yang lebih kompleks.

Selain itu, untuk meningkatkan kapasitas penyimpanan pesan, dapat dilakukan kompresi pesan sebelum disisipkan ke dalam gambar.

Penelitian ini bertujuan untuk meningkatkan keamanan enkripsi Vigenere dengan mengimplementasikan kunci asimetris (kunci publik dan kunci privat). Metode yang diusulkan melibatkan pembangkitan kunci, perhitungan Least Common Multiple (LCM) dari One Time Password (OTP), penghasilan hash dari hasil LCM, dan penggunaan kalimat sengkalan sebagai kunci publik. Implementasi dilakukan dalam aplikasi steganografi dengan GUI, di mana pesan rahasia dienkripsi dan disisipkan ke dalam gambar menggunakan metode Least Significant Bit (LSB).

Hasil penelitian menunjukkan bahwa metode yang diusulkan dapat meningkatkan keamanan enkripsi Vigenere dengan menggabungkan kunci asimetris. Antarmuka pengguna grafis memungkinkan pengguna untuk mengunggah gambar penutup, pesan rahasia, serta menjalankan proses penyisipan dan ekstraksi pesan. Skema steganografi dengan metode LSB digunakan untuk menyisipkan pesan rahasia ke dalam gambar.

5. KESIMPULAN DAN SARAN

Kesimpulannya, penelitian ini berhasil mengembangkan kunci enkripsi asimetris untuk Vigenere Cipher yang dapat meningkatkan keamanan distribusi kunci. Metode ini menggabungkan OTP, LCM, SHA-1, dan kalimat sengkalan untuk menciptakan kunci publik dan privat yang unik. Implementasi dalam aplikasi steganografi dengan GUI menunjukkan bahwa metode ini efektif dalam menyembunyikan pesan rahasia dengan metode LSB.
Saran untuk penelitian selanjutnya adalah mengeksplorasi metode enkripsi yang lebih kuat dan teknik steganografi yang lebih kompleks untuk meningkatkan keamanan dan kapasitas penyimpanan pesan.

DAFTAR PUSTAKA

[1] Purba, A. M. (2021). Steganography Based on LSB and Vigenere Cipher for Securing Text Information.
[2] Subandi. (2017). Analysis of Vigenere Cipher Encryption Algorithm with Modified Autokey to Increase Security.
[3] Wibowo, A. (2022). Enhancement of Vigenere Cipher Encryption Method using Triple Layer Key.
[4] Wijaya, B. (2023). Dual Key Encryption using One Time Pad and MD5 for Vigenere Cipher Security Improvement.
[5] Putra, C. R. (2023). Improving Vigenere Cipher Security through One Time Pad and Message Digest 5 (MD5) Combination.
[6] Adi, S. K. (2014). Sengkalan: Simbol Budaya Jawa yang Dapat Dikonversi ke Angka.
[7] Eastlake, D. (2001). RFC 3174 - US Secure Hash Algorithm 1 (SHA-1).
[8] H. Nugroho, "Implementasi hybrid enkripsi dan algoritma hashing untuk keamanan kunci pada Vigenere Cipher," Jurnal Teknologi Informasi dan Kriptografi, vol. 11, pp. 33-40, 2022.
[9] I. Fauzan, "Penggunaan enkripsi berbasis waktu untuk meningkatkan keamanan data pada Vigenere Cipher," Jurnal Sistem Informasi, vol. 9, pp. 76-83, 2022.
[10] J. Sutrisno, "Penerapan algoritma kriptografi modern pada Vigenere Cipher untuk keamanan data besar," Jurnal Keamanan Informasi, vol. 6, pp. 91-100, 2023.