OPTIMALISASI STEGANOGRAFI DENGAN MENGGUNAKAN KUNCI PRIVATE REVERSE ENCRYPTION

Jeki Saputra, Umar Faruq, Yohanes Dwi Cahyono
Jurusan Telekomunikasi, Politeknik Angkatan Darat
Junrejo, Kota Batu, Jawa Timur-Indonesia 65324
umarfaruq0406@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengoptimalkan steganografi dengan menggunakan keamanan kunci privat melalui metode enkripsi Reverse Encryption. Steganografi, sebagai teknik untuk menyembunyikan informasi dalam pesan non-rahasia, menjadi semakin penting dalam konteks komunikasi digital yang berkembang pesat. Penelitian ini mengkaji kombinasi algoritma Vigenère dan Reverse Cipher untuk meningkatkan keamanan data. Metode ini melibatkan proses enkripsi dan dekripsi kunci privat yang telah diamankan menggunakan SHA-1 dan MD5, dengan tujuan untuk mencegah akses tidak sah terhadap informasi sensitif. Hasil penelitian menunjukkan bahwa meskipun metode kombinasi ini mempercepat proses enkripsi dan dekripsi, tantangan tetap ada dalam menjaga integritas data. Penelitian ini memberikan saran untuk pengembangan lebih lanjut dalam metode enkripsi guna meningkatkan keamanan.

Kata kunci : Steganografi, *Reverse*, *encryption*, *SHA-1*, *MD5*.

1. PENDAHULUAN

Steganografi adalah praktik menyembunyikan informasi rahasia dalam pesan non-rahasia. Ini telah digunakan selama berabad-abad untuk melindungi informasi sensitif dari pengintaian. Dengan meningkatnya komunikasi digital, steganografi telah menjadi alat yang semakin penting untuk melindungi informasi digital. Akibatnya, minat terhadap penelitian steganografi meningkat dalam beberapa tahun terakhir. Para peneliti sedang mengeksplorasi teknik-teknik baru untuk menyembunyikan informasi di media digital, serta mengembangkan metode-metode baru untuk mendeteksi pesan-pesan tersembunyi.

Penelitian ini penting karena membantu menjamin keamanan komunikasi digital dan melindungi informasi sensitif dari akses tidak sah. Selain itu, steganografi dapat digunakan untuk berbagai aplikasi, termasuk watermarking digital, perlindungan hak cipta, dan komunikasi rahasia. Metode kriptografi yang dapat digunakan adalah Vigenère Reverse yang merupakan salah satu contoh paling sederhana dari kriptografi transposisi, metode ini juga mudah untuk digunakan dan waktu yang digunakan untuk proses enkripsi maupun dekripsi sangatlah singkat (Sertiani, 2020). Metode ini sederhana dan hanya melibatkan penukaran posisi karakter dalam suatu teks. Sebagai contoh, jika kita memiliki teks "HELLO", enkripsi dengan metode "reverse" akan menghasilkan "OLLEH" dengan menukar urutan karakter dari belakang ke depan. Pada pembahasan kali ini kita menggunkan reverse pada private key yang sudah di encrypt menggunakan SHA 1 dan MD5 agar lebih susah diketahui orang lain makan kita gunakan reverse untuk membalik privat key.

Berdasarkan penelitian terkait maka tujuan dari penelitian ini adalah menerapkan kombinasi enkripsi dekripsi dengan metode kombinasi Reverse Cipher. Penelitian ini bertujuan untuk menganalisis tingkat keamanan kunci private dengan memanfaatkan metode enkripsi "reverse, mengoptimalkan algoritma reverse encryption agar lebih efisien dan aman dan melakukan evaluasi terhadap efektivitas dan keamanan penggunaan reverse encryption pada kunci private serta menganalisis keamanan metode reverse encryption terhadap berbagai serangan kriptografis seperti analisis frekuensi, serangan brute force, atau teknik kriptoanalisis lainnya.

2. TINJAUAN PUSTAKA

Steganografi adalah praktik menyembunyikan informasi rahasia dalam pesan yang tampak tidak mencolok, yang telah digunakan selama berabad-abad untuk melindungi data sensitif. Dalam era digital, teknik ini semakin relevan untuk melindungi informasi dari pengintaian.

2.1. Metode Kriptografi.

Kriptografi merupakan teknik yang digunakan untuk mengamankan informasi melalui pengkodean. Salah satu metode yang dibahas dalam penelitian ini adalah algoritma Vigenère, yang merupakan bentuk kriptografi transposisi sederhana. Metode lain yang digunakan adalah Reverse Cipher, yang bertujuan untuk membalik urutan karakter dalam teks untuk meningkatkan keamanan.

2.2. Keamanan Kunci Private

Keamanan kunci privat sangat penting dalam komunikasi digital. Penelitian sebelumnya menunjukkan bahwa kombinasi beberapa metode kriptografi dapat meningkatkan tingkat keamanan terhadap berbagai serangan kriptografis, seperti analisis frekuensi dan serangan brute force.

2.3. Penelitian Terkait

Beberapa studi sebelumnya telah mengeksplorasi penggunaan kombinasi algoritma dalam kriptografi. Misalnya, penelitian oleh Anggi Rizki et al. (2021) membahas implementasi kombinasi algoritma Reverse Cipher dan Vigenère Cipher untuk keamanan pesan teks pada aplikasi desktop.

3. METODE PENELITIAN

Berikut adalah metodologi penelitian yang dapat diambil untuk mengejar tujuan penelitian "Optimalisasi Steganografy Dengan Menggunakan Keamanan Kunci Private Reverse Encryption" Mulai dengan melakukan tinjauan literatur yang mendalam untuk memahami keamanan kunci private dan berbagai metode enkripsi yang telah ada. Identifikasi kelemahan dan kelebihan dari metode-metode ini, serta gap dalam pengetahuan yang dapat diisi oleh penelitian Anda.

3.1. Tinjauan Literatur

Melakukan studi mendalam tentang keamanan kunci privat dan berbagai metode enkripsi yang ada, serta mengidentifikasi kelemahan dan kelebihan dari masing-masing metode.

3.2. Identifikasi Algoritma

Memilih atau mengembangkan algoritma Reverse Encryption yang sesuai dengan kebutuhan keamanan kunci privat, serta memastikan bahwa algoritma tersebut dapat diterapkan secara efektif.

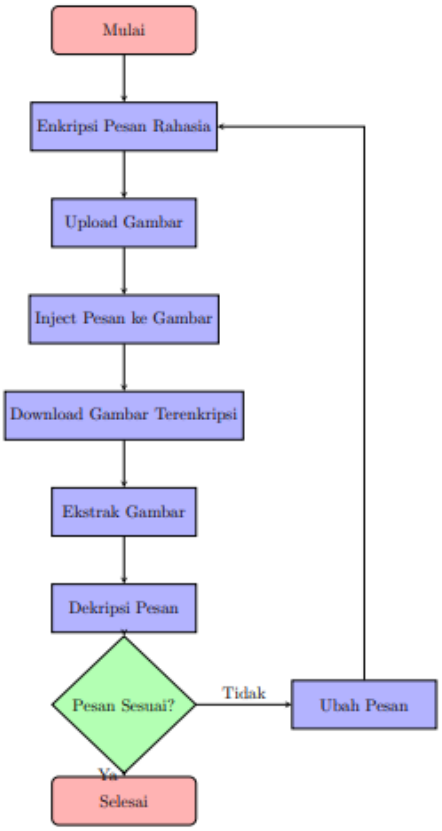
3.3. Desain Eksperimen

Merancang eksperimen untuk menguji keamanan, kecepatan, dan efisiensi dari algoritma yang diusulkan. Parameter eksperimen meliputi ukuran kunci, waktu enkripsi, waktu dekripsi, dan respon terhadap serangan tertentu.

3.4. Implementasi

Dari Bab sebelumnya peneliti sudah menjelaskan langkah demi langkah dari Algoritma dan kelas diagram untuk mengembangkan metode penelitian yang diusulkan, berikut ini adalah Implementasi dari aplikasi Steganografi menggunakan bahasa Pemrograman Javascript. Ada 5 file yang digunakan untuk menjalankan program yang dimaksud diantaranya ada 4 file Javascript dan 1 file HTML dengan flowchart yang menjelaskan program ini berjalan.

Gambar 1 Flowchart ini menggambarkan sebuah langkah proses enkripsi dan dekripsi pesan rahasia dimulai dengan menginisiasi enkripsi pesan rahasia yang akan disembunyikan. kemudian gambar yang akan dipakai sebagai wadah untuk menyimpan pesan diunggah dan diikuti dengan proses inject pesan yang telah dienkripsi ke dalam gambar tersebut. Gambar yang diinject ini kemudian diunduh untuk melakukan ekstraksi. Setelah diekstrak pesan rahasia ini didekripsi untuk menampilkan isi pesan aslinya tahapan ini juga terdapat keputusan untuk mengecek apakah pesan yang didekripsi telah sesuai dengan yang dikirim oleh pengirimnya. Jika pesan tidak sesuai maka proses akan kembali ke langkah enkripsi untuk melakukan penyesuaian. kemudian Ketika pesan yang dikirm telah sesuai maka program telah selesai dikerjakan.



Gambar 1. Flowchart

3.5. Pengujian dan Evaluasi

Melakukan serangkaian pengujian untuk mengevaluasi keamanan algoritma terhadap berbagai serangan, serta mengukur performa algoritma dalam hal waktu enkripsi, waktu dekripsi, dan konsumsi sumber daya.

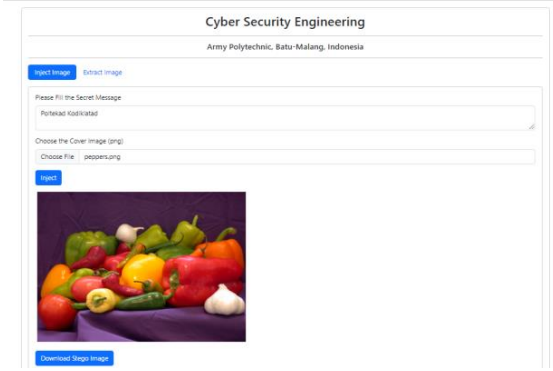
4. HASIL DAN PEMBAHASAN

Aplikasi Enkripsi dan Dekripsi dengan menggunakan metode kombinasi*Vigenere Cipher* dan *Reverse Cipher* ini merupakan aplikasi dekstop yang dibuat guna membantu *user* (terutama mahasiswa poltekad) dalam mengamankan sebuah data ataupun informasi yang sifatnya rahasia. Dalam aplikasi ini terdapat 2 fitur utama yaitu Enkripsi dan Dekripsi. Aplikasi dapat digunakan hanya dengan melakukan instalasi dan menjalakan program tersebut yang terdapat pada folder instalasi akan tetapi terlebih dahulu menginstal XAMPP dan menjalankannya. Berikut beberapa langkah yang harus dilakukan:

Langkah awal mengenkripsi suatu isi pesan rahasia dan mengupload gambar yang akan dienkripsi dengan contoh sebagai berikut.

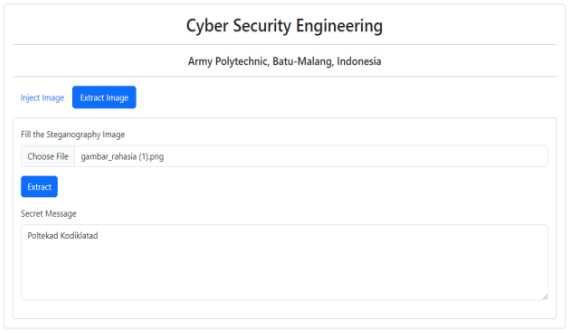
Gambar 2. Upload Gambar

Gambar yang diinject dengan pesan rahasia akan muncul seperti pada gambar dibawah ini kemudian tinggal kita melakukan download untuk diextract gambar.



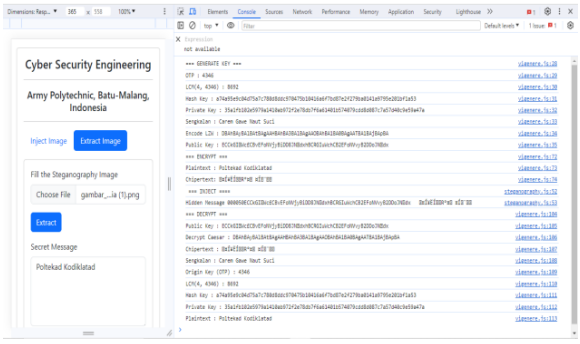
Gambar 3. Inject dengan pesan rahasia

Hasil deskripsi gambar.



Gambar 4. Hasil Deskripsi Gambar

Berikut hasil Enkripsi dari penerapan kombinasi vigenere dan reverse untuk mengamankan pesan pada gambar steganografi



Gambar 5. Hasil Enkripsi

5. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan dengan judul "Optimalisasi Steganografy Dengan Menggunakan Kunci Private Reverse Encryption", penulis berhasil membuat coding dengan nama jurnal. Aplikasi tersebut ditujukan untuk mengamankan pesan, data, maupun informasi user sehingga sulit untuk dibaca dan disalahgunakan oleh user lain ataupun orang yang tidak bertanggung jawab dengan menggubah privat key yang sudah diamankan menggunakan SHA 1 dan MD 5 kemudian dibalik atau dirubah menggunkan reverse chipper. Aplikasi berbasis dekstop ini dibuat dengan menggunakan bahasa pemrograman Javascript yang dilengkapi dengan library Tkinter. Setelah itu aplikasi dikonversi menggunakan CMD (Command Prompt) dengan library PyInstaller dari Python.

Hasil analisa pengujian dan perbandingan yang telah penulis lakukan dihasilkan beberapa urutan waktu proses enkripsi dekripsi tercepat yang diperoleh menggunakan metode Reverse, lalu Vigenere dilanjutkan dengan metode kombinasi SHA 1 dan MD 5 yang dirubah Kembali dengan metode reverse. Namun dengan cepatnya proses enkripsi dekripsi tidak menjamin keamanan tersebut kuat untuk mencegah kebocoran informasi. Dengan begitu, metode kombinasi merupakan pilihan yang tepat untuk aplikasi yang dibuat oleh penulis. Dalam pembuatan aplikasi ini masih jauh dari kata 'sempurna'. Salah contoh kekurangannya yaitu masih terdapat beberapa karakter pada output yang tidak sesuai saat melakukan dekripsi, tentunya dengan hal seperti itu menjadi pekerjaan tambahan bagi user untuk merapikan dan menyamakan output dengan plaintext sebenarnya. Selain itu, penulis juga memberikan saran agar nantinya aplikasi dapat dikembangkan dengan menambahkan berbagai macam metode enkripsi dan dekripsi lainnya.

DAFTAR PUSTAKA

[1] Agus Suryanto dan Anan Nugroho. (2020). Manajemen Proyek Teknologi Informasi. URL:https://books.google.co.id/books?hl=en&lr=&id=430WEAAAQBAJ&oi=fnd&pg=PP1&dq=source:deepublish+manajemen+proyek+teknologi+informasi&ots=zkN2clImfn&sig=nD2BxQDxtDnRmyg_wgT96DiK5Tw&redir_esc=y#v=onepage&q& f=false [Tanggal Akses: 29 – Juni - 2022].

[2] Anggi Rizki, Sayuti Rahman, dan Arnes Sembiring. (2021). 'Implementasi Kriptografi Kombinasi Algoritma Reverse Cipher dan Algoritma Vigenere Cipher untuk Keamanan Pesan Teks Pada Aplikasi Catatan Berbasis Desktop'. SNASTIKOM: Seminar Nasional Teknologi Informasi & Komunikasi.

[3] Anita Septiana Rosana. (2010). 'Kemajuan Teknologi Informasi dan Komunikasi dalam Industri Media di Indonesia'. Gema Eksos. Vol 5(2). pp. 2. URL:

https://media.neliti.com/media/publications/218225-kemajuan-teknologi- informasi-dan-komunik.pdf [TanggalAkses: 23 -Juni - 2022].

[4] Basri. (2016). 'Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi'. Jurnal Ilmiah Ilmu Komputer. Vol. 2(2).

[5] Cornelia Lyman. (2021). 'Apa itu Kriptografi dan Contohnya?'. Pintu Blog. URL: https://pintu.co.id/blog/apa-itu- kriptografi-dan-contohnya [TanggalAkses: 25-Juni-2022]

[6] Dodo Zaenal Abidin. (2017). 'Kejahatan dalam Teknologi Informasi dan Komunikasi'. Jurnal Ilmiah Media Processor. Vol 10(2). pp.1-8. URL: http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107 Tanggal Akses: 23 -Juni - 2022].

[7] Falentino Sembiring. (2021). Buku Ajar Dasar Pemrograman (Python). URL: https://books.google.co.id/books?hl=en&lr=&id=zA08EAAAQBAJ&oi=fnd&pg=PA63&dq=sejarah+bahasa+pemrograman+python&ots=5cSWBr5Quv&sig=9UPW2NIow7ciVT0S51a7E_S1E3M&redir_esc=y#v=onepage&q=sejarah%20bahasa%20pemrograman%20python&f=fals [Tanggal Akses: 28 - Juni 2022].

[8] Harun Mukhtar. (2018). 'Kriptografi' dalam Kriptografi untuk Keamanan Data. Deepublish. Yogyakarta.