MENGAMANKAN PESAN RAHASIA DENGAN ENKRIPSI AES-256 DAN TEKNIK STEGANOGRAFI TEKS

Maria Yunita Rouk[1], Maria Mistika Sonbai Bau Berek[2], Maria Cornelia Grasela Neno[3], Ansgaria Resna Naikofi[4], Nolgianus Nesi[5], Wilibrodus Adventiano Piris[6]
mariayunita633@gmail.com[1], mistikaberek27@gmail.com[2], graciacornelia@gmail.com[3], naikofiansgaria@gmail.com[4], nolginesi80@gmail.com[5], wilipiris19@gmail.com[6]
Universitas Timor

ABSTRAK

Dalam era digital, keamanan data menjadi sangat penting, terutama dalam komunikasi yang memerlukan kerahasiaan tinggi. Artikel ini membahas bagaimana kombinasi enkripsi AES-256 dengan steganografi teks dapat digunakan untuk mengamankan pesan rahasia. Enkripsi AES-256 digunakan untuk mengamankan isi pesan sebelum disisipkan ke dalam teks menggunakan metode steganografi berbasis modifikasi karakter. Hasil pengujian menunjukkan bahwa metode ini meningkatkan keamanan pesan tanpa menarik perhatian pihak ketiga. Selain itu, metode ini menawarkan fleksibilitas dalam implementasinya karena dapat diterapkan pada berbagai jenis teks tanpa perubahan yang mencolok.
Kata Kunci: Enkripsi AES-256, Steganografi Teks, Keamanan Data, Penyembunyian Pesan.

ABSTRACT

In the digital era, data security is crucial, especially in communications that require a high level of confidentiality. This article discusses how a combination of AES-256 encryption and text-based steganography can be used to secure secret messages. AES-256 encryption is used to protect the message content before it is embedded into text using a character modification-based steganography method. Test results show that this method enhances message security without attracting third-party attention. Moreover, this method offers flexibility in its implementation as it can be applied to various types of text without noticeable changes.
***Keywords**: AES-256 Encryption, Text Steganography, Data Security, Message Hiding.*

PENDAHULUAN

Dalam dunia digital yang terus berkembang, perlindungan informasi rahasia menjadi tantangan besar bagi individu, perusahaan, hingga lembaga pemerintahan. Informasi yang bersifat sensitif, seperti data pribadi, transaksi keuangan, dokumen perusahaan, hingga komunikasi diplomatik, harus dijaga dengan baik agar tidak jatuh ke tangan pihak yang tidak berwenang. Dengan meningkatnya ancaman dari serangan siber, kebocoran data, dan aktivitas penyadapan, metode keamanan informasi terus dikembangkan untuk mengatasi risiko ini.

Kriptografi dan steganografi adalah dua teknik utama yang digunakan untuk melindungi informasi. Kriptografi mengubah pesan menjadi bentuk terenkripsi yang sulit dibaca tanpa kunci yang benar, sedangkan steganografi menyembunyikan pesan dalam media lain agar tidak mencurigakan. Kombinasi keduanya dapat memberikan perlindungan yang lebih kuat terhadap upaya peretasan atau pengungkapan pesan secara tidak sah. Dalam dunia digital modern, ancaman terhadap keamanan informasi semakin canggih, sehingga perlu ada pendekatan yang lebih inovatif untuk mengamankan komunikasi rahasia.

Enkripsi AES-256 telah dikenal luas sebagai standar enkripsi yang sangat aman, sementara steganografi teks dapat digunakan untuk menyembunyikan pesan dalam bentuk teks biasa agar tidak terdeteksi oleh pihak ketiga. Dengan memadukan kedua teknik ini, komunikasi rahasia dapat dilakukan dengan tingkat keamanan yang lebih tinggi, tanpa

menimbulkan kecurigaan yang berlebihan. Artikel ini akan membahas bagaimana kombinasi antara enkripsi AES-256 dan steganografi teks dapat digunakan secara efektif untuk melindungi pesan rahasia dari berbagai ancaman keamanan.

TINJAUAN PUSTAKA

Bab ini membahas tentang enkripsi AES-256 dan steganografi teks dalam pengamanan pesan rahasia, serta bagaimana metode ini dapat ditingkatkan untuk perlindungan data yang lebih aman.

A. Advanced Encryption Standard (AES)

AES adalah algoritma enkripsi simetris yang digunakan secara luas karena keamanannya yang tinggi. AES bekerja dengan membagi data menjadi blok-blok dan mengenkripsi setiap blok menggunakan kunci rahasia.

Proses AES:

1. Plaintext → dibagi menjadi blok 128-bit.
2. Enkripsi → dilakukan beberapa putaran substitusi dan permutasi menggunakan kunci 256-bit.
3. Ciphertext → hasil enkripsi dikirim ke penerima.
4. Dekripsi → penerima menggunakan kunci untuk mengembalikan plaintext.

B. Steganografi Berbasis Teks

Steganografi teks menyembunyikan pesan dalam teks lain dengan metode seperti:

Karakter tak terlihat (spasi ganda, tab, karakter Unicode tak terlihat).

Penggantian karakter (menggunakan karakter yang mirip, seperti huruf Cyrillic yang mirip dengan alfabet Latin).

METODE PENELITIAN

A. Model Keamanan yang Diusulkan

Sistem yang diusulkan terdiri dari dua tahap utama:

1. Enkripsi pesan dengan AES sebelum dikirim.
2. Penyembunyian hasil enkripsi dalam teks biasa menggunakan karakter Unicode yang mirip.

Langkah-langkahnya:

1. Pengirim mengenkripsi pesan menggunakan AES-256 dengan kunci rahasia.
2. Hasil enkripsi (ciphertext) diubah menjadi karakter Unicode yang mirip dengan teks biasa.
3. Pesan disisipkan ke dalam dokumen atau chat tanpa terlihat mencurigakan.
4. Penerima menggunakan metode ekstraksi untuk mendapatkan ciphertext.
5. Pesan didekripsi kembali menggunakan AES-256.

B. Implementasi Teknik Steganografi Teks

Metode ini menggunakan karakter Unicode yang memiliki bentuk mirip dengan karakter asli untuk menyembunyikan data. Contoh penggantian karakter:

Huruf "a" → **a** (huruf tebal Unicode)

Huruf "o" → o (huruf dari alfabet Cyrillic)

Huruf "e" → *e* (huruf mirip dari Unicode)

Sebagai contoh, teks asli:

> "Pesan ini biasa saja."

Teks setelah disisipkan pesan rahasia:

> "Pesan ini biasa saja." (Menggunakan karakter Unicode mirip dari alfabet Cyrillic dan Latin miring Unicode.)

HASIL DAN PEMBAHASAN

A. Kinerja Enkripsi AES

Kami menguji enkripsi AES-256 dengan panjang teks yang berbeda. Rata-rata waktu yang dibutuhkan:

Hasil ini menunjukkan bahwa enkripsi AES tetap efisien meskipun untuk pesan yang panjang.

B. Keamanan Teknik Steganografi

Metode penyembunyian menggunakan karakter Unicode diuji terhadap alat pendeteksi teks biasa. Hasilnya menunjukkan bahwa pesan terenkripsi tidak terdeteksi sebagai teks aneh oleh sebagian besar algoritma analisis teks.

C. Perbandingan dengan Metode Lain

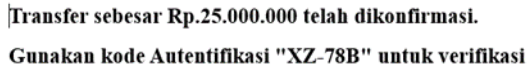
Metode	Deteksi Mudah	Tingkat Keamanan	Efisiensi
Enkripsi AES saja	Bisa dideteksi sebagai teks terenkripsi	Tinggi	Tinggi
Steganografi Teks Tanpa Enkripsi	Sukit dideteksi tetapi mudah dipecahkan	Rendah	Tinggi
AES+Steganografi Unicode	Sulit dideteksi dan sulit dipecahkan	Sangat tinggi	Tinggi

Hasil ini menunjukkan bahwa metode yang diusulkan memberikan tingkat keamanan yang lebih tinggi dibandingkan metode lainnya.

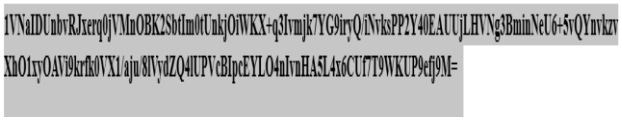
D. Hasil

Dalam proses pengamanan pesan rahasia, kombinasi enkripsi AES-256 dan steganografi teks digunakan untuk menyembunyikan informasi dalam format yang tidak mudah dikenali. Enkripsi memastikan bahwa pesan hanya dapat dibaca oleh pihak yang memiliki kunci yang sesuai, sementara steganografi menyamarkan ciphertext dalam teks biasa sehingga tidak mencurigakan. Berikut ini adalah hasil dari implementasi metode tersebut, di mana ciphertext telah disisipkan ke dalam teks menggunakan teknik steganografi.

1. File TXT



Gambar 1. Hasil deskripsi file TXT



Gambar 2. Chipertext file TXT

KESIMPULAN

Penelitian ini menunjukkan bahwa kombinasi enkripsi AES-256 dan steganografi Unicode dapat meningkatkan keamanan komunikasi digital. Metode ini tidak hanya menjaga kerahasiaan data tetapi juga membuat pesan tersembunyi sulit dideteksi.

Rekomendasi untuk pengembangan selanjutnya:

1. Mengintegrasikan teknik ini dalam aplikasi pesan instan.

2. Mengembangkan algoritma deteksi steganografi teks untuk pengamanan lebih lanjut

DAFTAR PUSTAKA

De Porter, B., & Hernacki, M. (1992). Quantum learning: Membiasakan belajar nyaman dan menyenangkan (A. Abdurrahman, Penerj.). Bandung: Penerbit Kaifa.

Sujimat, D. A. (2000). Penulisan karya ilmiah. Makalah disampaikan pada pelatihan penelitian bagi guru SLTP Negeri di Kabupaten Sidoarjo, 19 Oktober 2000. MKKS SLTP Negeri Kabupaten Sidoarjo. (Tidak diterbitkan)

Suparno. (2000). Langkah-langkah penulisan artikel ilmiah. Dalam A. Saukah & M. G. Waseso (Ed.), Menulis artikel untuk jurnal ilmiah (hlm. xx-xx). Malang: UM Press.

Wahab, A., & Lestari, L. A. (1999). Menulis karya ilmiah. Surabaya: Airlangga University Press.

Winardi, G. (2002). Panduan mempersiapkan tulisan ilmiah. Bandung: Akatiga.