Journal of Information Technology and Computer Science (INTECOMS)
Volume 7 Nomor 3, Tahun 2024
e-ISSN : 2614-1574
p-ISSN : 2621-3249

PENERAPAN KRIPTOGRAFI AES PADA FRES-CAESAS: PERLINDUNGAN PESAN TEKS DAN FAIL DOKUMEN

APPLICATION OF AES CRYPTOGRAPHY IN FRES-CAESAS: PROTECTION OF TEXT MESSAGES AND DOCUMENT FAILS

Dadang Mulyana Iskandar[1], Muhamad Zaeni Nadip[2], Nandy Dinilhaq[3], Anggit Purnama[4]
[1,2,3,4]Sekolah Tinggi Ilmu Komputer, Cipta Karya Informatika, DKI Jakarta, Indonesia.
mahvin2021@gmail.com[1], zaeni167@gmail.com[2], nandydinilhaq@gmail.com[3], sehanap06@gmail.com[4]

ABSTRACT

Data security solutions have led technical progress. Cryptography and steganography are two of several fields of science that have developed these techniques to protect sensitive data. Data security requires a suite of tools, not a single solution. The main objective of this research is to use the Advanced Encryption Standard (AES) algorithm and cryptography to secure text conversations, document files and their contents. AES is an effective cryptographic method. Data can be encrypted and decrypted using symmetric ciphertext blocks. Users can encrypt SMS, store it in an encrypted document, encrypt the document content, and compress it, according to data analysis. To ensure data protection through security and encryption, the results of document file encryption are hidden in an image.

Keywords: *Cryptography, Advanced Encryption Standard (AES), Text Messages, Document File Contents, Steganography.*

ABSTRAK

Solusi keamanan data telah memimpin kemajuan teknis. Kriptografi dan steganografi adalah dua dari beberapa bidang ilmu yang telah mengembangkan teknik ini untuk melindungi data sensitif. Keamanan data memerlukan seperangkat alat, bukan solusi tunggal. Tujuan utama penelitian ini adalah menggunakan algoritma Advanced Encryption Standard (AES) dan kriptografi untuk mengamankan percakapan teks, fail dokumen, beserta isinya. AES adalah metode kriptografi yang efektif. Data dapat dienkripsi dan didekripsi menggunakan blok ciphertext simetris. Pengguna dapat mengenkripsi SMS, menyimpannya dalam dokumen terenkripsi, mengenkripsi konten dokumen, dan mengompresnya, sesuai dengan analisis data. Untuk menjamin perlindungan data melalui keamanan dan enkripsi, hasil enkripsi fail dokumen disembunyikan dalam sebuah gambar.

Kata Kunci: Kriptografi, Advanced Encryption Standard (AES), Pesan Teks, Isi Fail Dokumen, Steganografi.

PENDAHULUAN

Saat ini, individu menggunakan komputer di rumah dan bisnis, dimanapun dan kapanpun. Keamanan data menjadi prioritas utama dalam komputerisasi untuk melindungi informasi dan data. Dalam pengamanan data, metode kriptografi dan steganografi menjadi solusi efektif.

Kriptografi melibatkan enkripsi dan dekripsi data menggunakan algoritma seperti Advanced Encryption Standard (AES) untuk menjaga kerahasiaan pesan. AES terkenal karena keamanannya dan efisiensinya dalam berbagai platform.

Steganografi, seni menyembunyikan pesan dalam media pesan, memberikan lapisan keamanan tambahan. Pada media citra digital, pesan rahasia disematkan tanpa indikasi jelas kepada pihak tidak berwenang.

Penelitian ini menggabungkan kriptografi AES dan steganografi dalam implementasi yang holistik. Tujuannya adalah menciptakan sistem keamanan data yang solid dan efisien, menjaga kerahasiaan pesan dan fail dokumen. Penelitian ini diharapkan memberikan kontribusi pada pengembangan metode keamanan data yang canggih dan bisa diandalkan.

TINJAUAN PUSTAKA

Dokumen Digital

Dokumen digital adalah bentuk informasi elektronik yang melibatkan berbagai tahapan, mulai dari pembuatan hingga distribusi. Dapat berupa tulisan,

suara, gambar, dan format lainnya, diakses melalui komputer atau sistem elektronik. Huruf, angka, dan simbol dapat dipahami oleh orang dengan kapasitas kognitif yang tepat.

Citra

Gambar analog diambil sampelnya dan diubah menjadi gambar diskrit untuk menghasilkan gambar dua dimensi. Piksel membentuk gambar. Teknologi dasar warna pada citra digital menggunakan konsep RGB (Red, Green, Blue), di mana kombinasi intensitas ketiga warna ini menghasilkan beragam spektrum warna. RGB menjadi dasar untuk pengelolaan warna dalam citra digital, memungkinkan reproduksi warna yang akurat di layar atau perangkat elektronik.

Kompresi Fail (Fail Compress)

Kompresi fail mengurangi ukuran data dengan menyandikan informasi dengan bit yang lebih sedikit. Hal ini bertujuan untuk menghemat ruang penyimpanan dan mempercepat proses transfer data. Dengan mengurangi jumlah bit yang digunakan, kompresi fail dapat menghasilkan versi data yang lebih efisien secara ruang dan memungkinkan pengguna untuk menyimpan atau mentransfer informasi dengan kecepatan yang lebih baik.

Fail

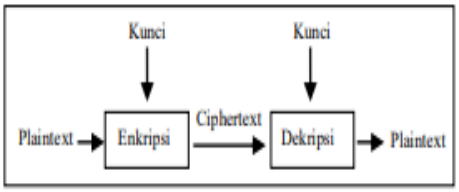
Fail adalah objek data yang bisa diakses dan dimanipulasi pengguna dalam sistem fail. Setiap fail dalam direktori memiliki nama unik dan jalur atau alamat direktori. Fail ini memiliki aliran data dari titik data tertaut. Karakteristik fail memberikan informasi lebih lanjut tentang status atau sifatnya. Fitur-fitur tersebut antara lain waktu pembuatan dan lain-lain

METODE

Metode keamanan data mencakup steganografi Command/DOS sertakriptografi AES

Kriptografi

Kriptografi mengamankan komunikasi dengan mengenkripsi dan mendekripsi. Plaintext diubah menjadi ciphertext menggunakan algoritma dan kunci. Istilah penting meliputi plaintext, ciphertext, pengirim, penerima, enkripsi, dekripsi, dan cipher dengan kunci. Kriptografi fokus pada keamanan kunci, bukan algoritma. Keamanan data tergantung pada kerahasiaan dan kekuatan kunci, dengan enkripsi dan dekripsi diilustrasikan melalui Gambar 1.



Gambar 1. Skema Enkripsi Dan Dekripsi Dengan Menggunakan Kunci.

Sejarah kriptografi

Enkripsi awal menggunakan kertas, pensil, dan perangkat mekanis sederhana. Metode kriptografi klasik utama adalah transposisi dan substitusi. Algoritme transposisi mengatur ulang huruf pesan, sedangkan metode penggantian menggantikannya.

Tujuan kriptografi

Pendahuluannya menyatakan bahwa tujuan utama kriptografi adalah untuk memberikan layanan keamanan di bidang berikut:

- Kerahasiaan: Melindungi komunikasi dari akses yang tidak sah
- Integritas data memastikan keaslian pesan dan transmisi tidak terpengaruh.
- Untuk memverifikasi identitas, otentikasi digunakan. Identitas dikaitkan dengan ini.
- Non-penyangkalan: komunikator tidak dapat menyangkal pengiriman pesan atau tindakan.

Advanced Encryption Standard (AES)

Sebuah kompetisi tahun 1997 memilih algoritma dekripsi baru untuk menggantikan DES. Dari dua puluh satu kontestan dari berbagai negara, hanya lima yang berhasil mencapai babak final pada

tahun 1999: Serpent (Ross Anderson dari Cambridge, Eli Biham dari Technion, Lars Knudsen dari UC San Diego), MARS dari IBM America, Twofish dari Bruce Schneier, John Kelsey, Niels Ferguson dari Counterpane Internet Security Inc., Doug Whiting dari Hi/fn Inc., David Wagner dari Berkeley, Chris Hall dari Princeton, Rijnd Pada tahun 2000, Rijndael, standar AES yang aman dan efisien, diadopsi. Nama penemunya digabungkan menjadi "Rijndael".

Deskripsi Advanced Encryption Standard (AES)

AES adalah algoritma kriptografi simetrik untuk mengamankan data melalui enkripsi dan dekripsi. AES berfungsi untuk blok data 128-bit dengan kunci 128, 192, atau 256-bit. Teks diubah menjadi ciphertext selama enkripsi dan kembali lagi selama dekripsi. Tabel 1 menunjukkan bahwa ukuran blok serta kunci mempengaruhi total prosesnya.

Tabel 1. Jumlah proses berdasarkan bit blok dan kunci.

Panjang Kunci Dalam bit	Panjang Kunci (*Nk*) Dalam *words*	Ukuran Blok Data (*Nb*) Dalam *words*	Jumlah Proses (*Nr*)
128	4	4	10
192	6	4	12
256	8	4	14

Status—blok data masukan serta kunci—ditangani dengan cara seperti array sebelum membuat teks tersandi. Teknik ini memiliki empat langkah penting: AddRoundKey, SubBytes, ShiftRows, dan MixColumns. Kecuali MixColumns, semua tahapan proses diulang. Tahap terakhir ini spesial. Dekripsi membalikkan enkripsi.

Enkripsi memerlukan lebih banyak kunci karena permintaan subkunci mungkin mencapai ribuan bit dan panjang kunci normal adalah 128-256 bit. Setiap level membutuhkan subkunci. Jumlah subkuncinya adalah Nb(Nr+1) yang berarti Nb ialah ukuran kata blok datanya dan Nr adalah jumlah tahapan kata. Ketika blok data 128-bit dan kunci 4 kata digunakan, 10 proses akan berjalan. Rumus ini menghasilkan 1408 bit kunci, atau 44 kata. Jadwal kunci menentukan berapa banyak kunci sekunder yang dihasilkan dari kunci primer.

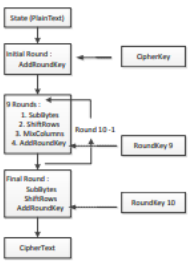
Ekspansi Kunci AES

AES memperluas kunci sandi, K, untuk membuat jadwal kunci. Ekspansi kunci menciptakan kata Nb(Nr+1). Strategi ini memerlukan Nb kata kunci di awal dan Nb kata kunci di setiap putaran.

Jadwal kunci menghasilkan array linier gaya [wi] yang terdiri dari kata-kata 4-byte. Fungsi SubWord menerapkan S-Box ke masing-masing empat byte masukan untuk membuat kata keluaran. Setelah permutasi siklik, RotWord menghasilkan [a1, a2, a3, a0] dari [a0, a1, a2, a3]. Rcon[i] terdiri dari nilai [xi-1, {00}, {00}, {00}], dengan x direpresentasikan sebagai {02} pada kolom GF(28).

Kata-kata Nk pertama dari perluasan kunci mencakup kunci sandi. Setiap kata, w[i], merupakan XOR dari kata sebelumnya (w[i-1]) dan kata sebelumnya (w[i-Nk]), dengan Nk adalah banyaknya kata. Sebelum XOR, w[i-1] ditransformasikan pada kelipatan Nk. XOR diikuti oleh konstanta putaran Rcon[i].

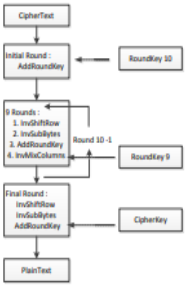
Transformasi empat byte enkripsi AES adalah SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Input yang disalin pertama-tama dikonversi dengan menambahkan kunci bulat ke byte-nya. SubBytes, ShiftRows, MixColumns, dan AddRoundKey lalu mengubah status sebanyak n kali. Fungsi putaran tidak mengubah status menggunakan MixColumns di putaran terakhir. Lihat Gambar 2 untuk diagram alur enkripsi AES.



Gambar 2. Diagram Alur Proses Enkripsi AES.

Dekripsi AES

Cipher invers AES dapat dihasilkan dengan membalikkan dan membalikkan transformasi cipher. Cipher invers mengubah byte menggunakan InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Gambar 3 menggambarkan diagram alur dekripsi algoritma Advanced Encryption Standard.



Gambar 3. Diagram Alur Proses Dekripsi AES.

Steganografi

Steganografi, dari bahasa Yunani yang berarti “tulisan tersembunyi”, menyembunyikan pesan dari manusia. Melindungi data sensitif secara digital melibatkan penyimpanan wadah—gambar, suara, teks, dan video—bersama dengan datanya.

Perbedaan mendasar antara steganografi dan kriptografi terletak pada hasil keluarannya. Kriptografi menghasilkan data yang tidak sama seperti wujud asli, Kelihatannya campur aduk, tapi mudah dibentuk kembali. Steganografi terlihat seperti manusia namun tidak terdeteksi *computer* dan *device* pemrosesan digital lain.

Sejarah Steganografi

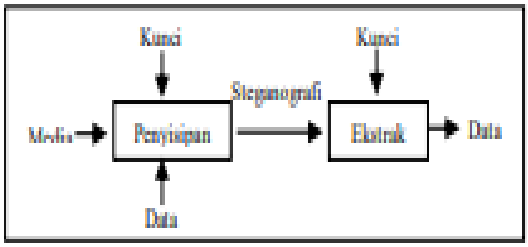
Ibu kota Mesir, Menet Khufu, menggunakan steganografi empat milenium lalu. Hieroglif—tulisan visual—pertama kali digunakan. Juru tulis tersebut mempergunakan huruf Mesir kuno guna menggambarkan hidup tuannya. Berbagai tulisan Mesir kuno ini menginspirasi komunikasi rahasia modern. Orang Mesir kuno tidak diragukan lagi menulis menggunakan steganografi pertama [1].

Proses Steganografi

Steganografi melibatkan penyisipan dan ekstraksi pesan. Plaintext, ciphertext, gambar, dan lainnya mungkin disertakan dalam bit-stream.

Memasukkan pesan ke dalam sampul media yang tidak dimodifikasi adalah penyisipan. Media stego meliputi media sampul dan sisipan. Langkah pertama dalam menginterpretasikan media stego adalah ekstraksi. Kunci stego dapat digunakan secara diam-diam untuk mengekstrak pesan.

Steganografi melibatkan enkripsi pesan dan melapisinya di atas objek lain untuk membuat "objek stego". Steganografi mencakup penyematan, ekstraktor, dan stegoanalyzer. Strategi ekstraksi dan penyisipan ditunjukkan melalui Gambar 4.



Gambar 4. Skema penyisipan dan ekstraksi dalam steganografi.

Disk Operating System (DOS)

DOS, OS baris perintah, populer pada tahun 1980an. Media yang dapat dipindahkan telah menjadikan "DOS" sebagai sistem operasi yang diinstal komputer saat dihidupkan. Manajemen perangkat keras dan perangkat lunak komputer adalah salah satu dari banyak aplikasinya. DOS berguna sebagai alat tambahan saat Windows tidak berfungsi dengan baik, memungkinkan akses ke hard drive tanpa antarmuka grafis (GUI), serta untuk menjalankan proses diagnostik serta penuntasan permasalahan sistemnya.

HASIL DAN PEMBAHASAN

DESKRIPSI SISTEM

Peneliti akan mengembangkan sistem keamanan data yang mengenkripsi teks, dokumen, serta fail mempergunakan AES dalam penelitian ini. Bukan hanya itu! Teknologi ini mendukung steganografi, yaitu menyembunyikan data atau pesan dalam gambar. Sistem Keamanan Data Aplikasi "Crypto AES And Stegano" (Fres-CAESAS) penelitian ini menggabungkan kedua pendekatan ini.

Application Data Security System - Crypto AES And Stegano (Fres-CAESAS)

Penulis menggunakan "Sistem Keamanan Data Aplikasi - Crypto AES dan Stegano" untuk "Fres-CAESAS." Setelah nama penulis, "Fres" dan "CAESAS" masing-masing adalah Crypto AES dan Stegano. Aplikasi ini mengamankan data menggunakan kriptografi, steganografi, dan algoritma AES. Data mungkin disembunyikan menggunakan gambar.

Fres-CAESAS menyediakan tiga macam teknik keamanan data. Teknik pertama menggunakan kriptografi, teknik kedua menggunakan steganografi, dan teknik ketiga merupakan kombinasi antara kriptografi dan steganografi pada suatu data. Pengguna dapat memilih teknik keamanan yang sesuai dengan kebutuhan mereka, baik menggunakan kriptografi, steganografi, atau kombinasi dari keduanya, untuk menjaga keamanan data mereka.

Alur Sistem Application Fres-CAESAS

Peneliti melindungi data aliran sistem Aplikasi Fres-CAESAS menggunakan kriptografi berbasis AES dalam pekerjaan ini. Mengikuti langkah-langkah ini:

1. Enkripsi Pesan Teks (Plaintext):
   - Pesan teks dienkripsi menggunakan metode AES dengan *key* yang dikenali hanya dari penggunanya
   - Hasil enkripsi, yang disebut ciphertext, disimpan sebagai fail dokumen dalam format *.txt.
2. Enkripsi Isi Fail Dokumen:
   - Isi teks dari failnya itu dienkripsi kembali oleh pengguna menggunakan key yang tidak sama.
   - Hasilnya adalah fail dokumen yang telah dienkripsi.
3. Kompresi Fail Dokumen:
   - Fail dokumen yang telah dienkripsi kemudian dikompresi menjadi fail kompresi.
4. Penerapan Steganografi:
   - Pada tahap ini, proses steganografi dilibatkan.
   - Penyisipan ataupun penyembunyian fail kompresi di suatu fail gambar
5. Hasil Akhir:
   - Hasil akhir dari proses tersebut adalah sebuah fail gambar.
   - Di dalam fail gambar tersebut ada suatu pesan rahasia ataupun fail yang telah dienkripsi dan dikompresi.

Seluruh perancangan sistem, yang melibatkan proses enkripsi serta sisipan pesan rahasia, bisa diuraikan lebih lanjut dalam Gambar 5. Maka demikian, aplikasi Fres-CAESAS menyatukan teknik kriptografi dan steganografi untuk menciptakan lapisan keamanan ganda pada data yang sensitif.

Gambar 5. Diagram Alur Sistem – Encryption and Hidden

Langkah-langkah dekripsi fail gambar yang berisi pesan rahasia melalui steganografi:

1. Penerapan Steganografi:
   - Ekstraksi fail atau pesan rahasia dari fail gambar.
2. Ekstraksi Fail Kompresi:
   - Fail kompresi diekstraksi dari hasil steganografi.
3. Dekripsi Fail Dokumen:
   - Fail dokumen yang terenkripsikan didekripsi menggunakan kunci enkripsi fail dokumen.
4. Dekripsi Isi Fail Dokumen:

- Isi fail dokumen didekripsi mempergunakan kunci enkripsi isi fail dokumen.

5. Dekripsi Pesan Teks:
   - Pesan teks (chipertext) didekripsi dengan kunci enkripsi pesan teks.
6. Hasil Akhir:
   - Menghasilkan pesan rahasia pada plaintext.

Ilustrasi sistem dekripsi dan tampilan pesan rahasia dapat dilihat pada Gambar 6, menunjukkan cara Fres-CAESAS mengembalikan pesan rahasia dari fail gambar yang telah melalui steganografi dan enkripsi.

Gambar 6. Diagram Alur Sistem - UnHidden and Decryption.

IMPLEMENTASI SISTEM

Log In Fres-CAESAS

Tahapan pertamanya menggunakan Application Fres-CAESAS:

1. Buka Aplikasi Fres-CAESAS:
   - Jalankan aplikasi Fres-CAESAS di perangkat.
2. Tampilan Awal (Main Display):
   - Setelah dibuka, Anda akan melihat Main Display seperti di Gambar 7.
   - Ini termasuk form Log In.
3. Form Log In:
   - Pengguna diminta memasukkan username dan password pada form LogIn.
   - Input harus sesuai dengan informasi pengguna.
4. Log In:
   - Setelah memasukkan username dan password, tekan tombol Log In untuk masuk ke aplikasi.

Perhatikan bahwa username dan password diperlukan untuk memastikan akses terbatas hanya pada pengguna yang berwenang. Gambar 7 memberikan visualisasi tampilan awal dengan form Log-In.

Gambar 7. Main Display & Log In Menu Application Fres-CAESAS

Menu aplikasi Fres-CAESAS terdiri dari beberapa form sebagai tombol aplikasi untuk menyelesaikan proses registrasi. Form aplikasi meliputi Form AES Crypto – Enkripsi dan Dekripsi, Form Stegano – Cache dan Formulir Tak Tersembunyi, Form Crypto AES dan Stegano – 1 formulir Fail Pesan, dan Form Pesan Rahasia Fres. Gambar 8 menampilkan menu yang tersedia pada aplikasi ini.

Gambar 8. Display Menu Application

"One Message Fails" adalah proses khusus untuk membuat pesan rahasia yang diubah menjadi satu fail dokumen tunggal. Proses ini melibatkan beberapa tahap untuk mempertahankan keamanan fail ataupun pesan rahasianya. Jika pengguna berkeinginan mengamankan data dengan menggabungkan teknik kriptografi AES dan steganografi, langkah-langkahnya sebagai berikut:

1. Klik Tombol "Crypto AES And Stegano – 1 Message Fails":
   - Pengguna mengklik tombol ini pada menu aplikasi.
2. Muncul Form Display of Crypto AES And Stegano – 1 Message Fails:
   - Setelah mengklik tombol, timbul form "Display of Crypto AES And Stegano – 1 Message Fails."
   - Tampilan awal form ini adalah "Display of Encryption and Hidden – One Message Fails," terlihat pada Gambar 9.
3. SubMenu di Form Display of Crypto AES And Stegano – 1 Message Fails:
   - Form berikut memiliki dua submenu dalam satu form:

- Submenu awal: "Encryption and Hidden – One Message Fails."
- Submenu selanjutnya: "Decryption and UnHidden – One Message Fails."Pada submenu pertama, pengguna dapat melakukan proses enkripsi dan sembunyian pesan ataupun fail rahasia dalam satu fail dokumen. Sementara pada submenu kedua, pengguna dapat melakukan proses dekripsi dan pengungkapan pesan ataupun fail rahasia yang disimpan.

Dengan adanya dua submenu ini, pengguna memiliki fleksibilitas untuk melakukan proses enkripsi dan dekripsi pada satu fail dokumen yang berisi pesan rahasia dengan menggunakan kombinasi teknik kriptografi dan steganografi. Gambar 9 memberikan gambaran visual kepada tampilan awal dari form "Display of Crypto AES And Stegano – 1 Message Fails."

Gambar 9. Display of Crypto AES And Stegano – 1 Message Fails (Display of Encryption and Hidden – One Message Fails)

PENGUJIAN SISTEM

Pengujian Aplikasi Fres-CAESAS berfokus pada bagian “Enkripsi dan Tersembunyi” dan “Dekripsi dan Tidak Tersembunyi”, yang menggunakan enkripsi AES dan merupakan “1 Fail Pesan.” Dokumen, pesan teks, dan data lainnya termasuk dalam kategori ini.

Tujuannya adalah mengukur keberhasilan perangkat lunak dalam enkripsi dan dekripsi dengan kunci yang benar, memastikan pemulihan data dengan kunci yang tepat, dan ketidakbacaan data dengan kunci yang tidak sesuai.

Tampilan pesan teks untuk pengujian bisa diamati di Gambar 10. Pengujian melibatkan enkripsi dan dekripsi pesan teks, isi fail dokumen, dan fail dokumen untuk memastikan keamanan dan integritas data.

Gambar 10. Display of Original Text Message (Plaintext).

Pengetesan kepada Pesan Teks (Plaintext) Terenkripsi

Pengujian enkripsi pada Application Fres-CAESAS memastikan pesan teks terlindungi dengan aman. Hasil enkripsi mengubah pesan teks menjadi ciphertext, tidak dapat dimengerti oleh pihak tidak berwenang. Berikut hasilnya:

1. Hasil Enkripsi Pesan Teks:
   - Tampilan pesan teks terenkripsi bisa diamati di Gambar 11, menghasilkan ciphertext.
2. Hasil Enkripsi Pesan Teks dalam Fail Dokumen:
   - Tampilan pesan teks terenkripsikan yang dilaksanakan penyimpanan di fail dokumen (*.txt) terlihat di Gambar 12.
   - Fail tersebut berisi informasi terenkripsi yang tidak dapat dimengerti tanpa dekripsi yang sesuai.

Proses enkripsi ini melindungi pesan teks, menjadikannya sulit dimengerti tanpa kunci yang benar. Gambar 11 dan Gambar 12 menunjukkan hasil enkripsi pesan teks dan penyimpanannya dalam fail dokumen, langkah krusial dalam menjaga keamanan dan kerahasiaan data.

Gambar 11. Display of Text Message (PlainText) Encrypted Output.

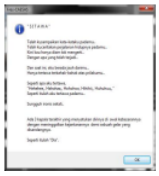
Gambar 12. Display of Text Message (PlainText) Encrypted Extention *.txt Output.

Pengetesan kepada Pesan Teks Terdekripsi

Pengujian dekripsi pada Application Fres-CAESAS menjamin bahwa pesan teks dapat dipulihkan ke bentuk aslinya dengan menggunakan kunci yang tepat. Berikut hasilnya:

1. Hasil Dekripsi Pesan Teks:
   - Tampilan pesan teks terdekripsikan dengan *key* yang sesuai bisa diamati melalui Gambar 13.
   - Proses dekripsi mengembalikan pesan teks ke bentuk aslinya sehingga informasi dapat dimengerti.
2. Hasil Dekripsi Pesan Teks dari Fail Dokumen:
   - Tampilan pesan teks yang terdekripsikan, tersimpan di fail dokumen (*.txt), terlihat pada Gambar 15.
   - Fail dokumen berisi pesan teks yang berhasil dikembalikan ke bentuk aslinya melalui proses dekripsi.

Dengan adanya proses dekripsi, pesan teks yang terenkripsi dapat dikembalikan oleh pemilik kunci yang sesuai. Gambar 13, Gambar 14 dan Gambar 15 menunjukkan hasil dekripsi pada pesan teks dan pengembalian informasi ke bentuk semula. Proses ini memastikan data yang diamankan dengan kriptografi AES dapat dikembalikan ke bentuk aslinya menggunakan kunci yang benar.



Gambar 13. Display of Information Text Message (PlainText) Decrypted Output With a Key Match.

Gambar 14. Display of Text Message (Plaintext) Decrypted Output With a Key Match.

Gambar 15. Display of Text Message (Plaintext) Decrypted Extention *.txt Output With a Key Match.

Gambar 16 menunjukkan layar yang menampilkan informasi kata sandi yang salah alih-alih dekripsi saat pengujian dengan *key* yang tidak sesuai dengan pesan teks

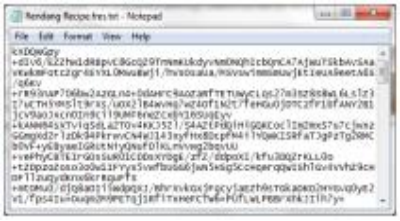
Gambar 16. Display of Information Invalid Password.

Pengetesan kepada Isi Fail Dokumen Terenkripsi

Menguji enkripsi pada isi fail dokumen dalam Application Fres-CAESAS dilakukan untuk memastikan keamanan. Hasilnya sebagai berikut:

- Hasil Enkripsi Isi Fail Dokumen (Ciphertext):
  - Tampilan isi fail dokumen yang terenkripsi dapat dilihat pada Gambar 17.
  - Proses enkripsi menghasilkan ciphertext sebagai representasi terenkripsi dari isi fail dokumen.

Dengan adanya proses enkripsi, isi fail dokumen yang awalnya dapat dibuka secara terang-terangan menjadi terlindungi dan sulit dimengerti tanpa kunci yang benar. Gambar 17 menunjukkan hasil enkripsi pada isi fail dokumen, menjadikan informasi dalam fail tersebut teracak dan tersamarkan untuk menjaga keamanan data.

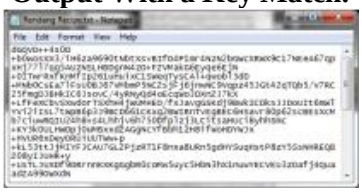


Gambar 17. Display of the Contents of the Documents Encrypted Output.

Pengetesan kepada Isi Fail Dokumen Terdekripsi

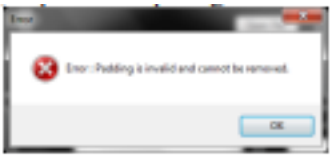
Dengan menggunakan kunci kanan, eksperimen mengubah dokumen menjadi teks biasa untuk memahaminya. Ini membantu memahami isinya. Dekripsi fail menggunakan kunci kanan dan tampilan isi dokumen ditunjukkan melalui Gambar 18 dan 19.

Gambar 18. Display of Information the Contents of The Documents Decrypted Output With a Key Match.

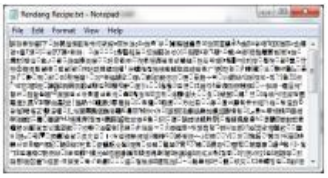


Gambar 19. Display of the Contents of The Documents Decrypted Output With a Key Match.

Menguji dekripsi menggunakan *key* yang tidak sesuai dengan pesan teks (plain text) dapat memberikan informasi yang tidak akurat pada Gambar 20. Gambar 21 menampilkan hasil dekripsi untuk teks yang tidak terbaca.



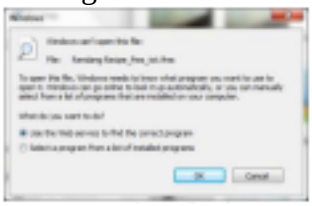
Gambar 20. Display of Information Error



Gambar 21. Display of the Contents of The Documents Decrypted Output With an UnMatch Key.

Pengetesan kepada Fail Dokumen Terenkripsi

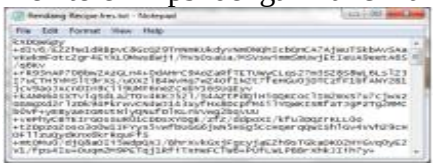
Periksa enkripsi fail dokumen untuk mengakses fail terenkripsikan. Menampilkan informasi fail dokumen terenkripsi menghasilkan Gambar 22.



Gambar 22. Display of Information Fail Documents Decrypted Output.

Pengetesan kepada Fail Dokumen Terdekripsi

Tes enkripsi dan dekripsi fail dokumen menggunakan kunci yang dapat dipulihkan. Gambar 23 menampilkan fail dokumen terenkripsi dengan kunci kanan.



Gambar 23. Display of Fail Documents Decrypted Output With a Key Match

Gambar 16 menunjukkan bahwa menggunakan kunci yang tidak cocok dengan format fail untuk memecahkan kode dokumen akan menghasilkan data kata sandi yang salah.

Pengetesan kepada Fail Tersembunyi

Menguji penyembunyian fail pada Application Fres-CAESAS dilakukan untuk memastikan kerahasiaan informasi. Hasilnya:

- Tampilan Hasil Fail Tersembunyi di Fail Citra:
  - Hasil fail yang tersembunyikan di fail citra terlihat pada Gambar 24.

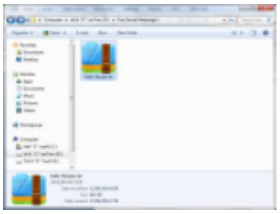
- Proses penyembunyian menghasilkan citra yang tampak normal namun menyimpan informasi tersembunyi di dalamnya.

Mekanisme ini memastikan bahwa fail tersembunyi tidak dapat diketahui tanpa proses ekstraksi yang sesuai. Gambar 24 menunjukkan efektivitas teknik steganografi dalam aplikasi ini.

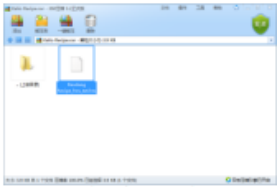
Gambar 24. Display of Hiddened Fail Output in an Image Fail.

Pengetesan kepada Fail Terurai

Verifikasi konversi fail tersembunyi ke fail gambar. Setelah mendekonstruksi, Anda dapat memulihkan dan mengakses fail. Gambar 25 dan 26 menunjukkan hasil dekonstruksi fail.



Gambar 25. Display of Extracted Fail Output is a Fail Compression.



Gambar 26. Display of Secret Fail Output in a Fail Compression

PERCOBAAN DAN ANALISIS HASIL PERCOBAAN SISTEM

Di tahpaan berikut, percobaan akan diterapkan, dan hasil percobaan sistem dari aplikasi Fres-CAESAS akan dianalisis. Aplikasi ini melibatkan proses-proses seperti enkripsi, dekripsi, penyembunyian, dan pengembalian isi dari fail dokumen, fail dokumen terenkripsi, fail kompresi, serta fail citra yang merupakan penutup penyembunyian.

Percobaan Sistem Kepada Process Encrypt Output – *the Contents of The Document*

Tabel 2. Percobaan Sistem Kepada Process Encrypt Output – the Contents of The Document.

File Name	*File Size Before Contents Encrypted*	*File Size After Contents Encrypted*
Brownies *Recipe*.txt	15 *bytes*	44 *bytes*
Rendang *Recipe*.txt	581 *bytes*	1.560 *bytes*

Percobaan Sistem Kepada Process Decrypt Output – *the Contents of The Document*

Tabel 3. Percobaan Sistem Kepada Process Decrypt Output – the Contents of The Document.

File Name	*File Size Contents Encrypted*	*File Size After Contents Decrypted*
Brownies *Recipe*.txt	44 *bytes*	15 *bytes*
Rendang *Recipe*.txt	1.560 *bytes*	581 *bytes*

Percobaan Sistem Kepada Process Encrypt Output – Fail Documents

Tabel 4. Percobaan Sistem Kepada Process Encrypt Output – Fail Documents.

File Name	*File Size Before File Encrypted*	*File Size After File Encrypted*
Healthy Tips.docx	16.376 *bytes*	16.384 *bytes*
Safety Tips.pdf	16.926 *bytes*	16.928 *bytes*

Percobaan Sistem Kepada Process Decrypt Output – Fail Documents

Tabel 5. Percobaan Sistem Kepada Process Decrypt Output – Fail Documents.

File Name	*File Size File Encrypted*	*File Size After File Decrypted*
Healthy Tips.docx	16.384 *bytes*	16.376 *bytes*
Safety Tips.pdf	16.928 *bytes*	16.926 *bytes*

Proses enkripsi meningkatkan ukuran pesan atau fail rahasia karena menambahkan header informasi, termasuk 8 karakter identifikasi dan karakter terakhir yang mencatat jenis AES yang digunakan (misalnya, AES-128). Header ini juga menambahkan 16 karakter ke kunci AES yang telah diacak, tergantung pada jenis AES yang digunakan. Fail hasil enkripsi terdiri dari elemen informasi header dan elemen data yang dikodekan. Informasi header berperan sebagai pengidentifikasi untuk fail terenkripsi dan digunakan dalam proses dekripsi untuk mendeteksi kunci yang benar. Meskipun

ukuran fail terenkripsi lebih besar, setelah didekripsi, ukuran fail kembali ke nilai asli sebelum proses enkripsi dilakukan.

Percobaan Sistem Kepada Process Hidden Output – Fail Compress

Tabel 6. Percobaan Sistem Kepada Process Hidden Output – Fail Compress.

Original Image File & Size	Secret File Name & Size	Hidden Image File & Size
	Corps of Tip.rar	
596.489 bytes	11.785 bytes	608.274 bytes
	Corps of Recipe.zip	
655.511 bytes	27.853 bytes	683.364 bytes

Percobaan Sistem Kepada Process UnHidden Output – Fail Compress

Tabel 7. Percobaan Sistem Kepada Process UnHidden Output – Fail Compress.

Hidden Image File & Size	UnHidden Secret File Name Saved & Size
	Corps of Article.rar
608.274 bytes	608.274 bytes
	Corps of Menu.rar
655.511 bytes	683.364 bytes

Proses penyembunyian pesan dalam citra menyebabkan peningkatan ukuran fail gambar karena inklusi ukuran pesan tersembunyi. Saat diekstraksi, ukuran fail tetap sama dengan fail gambar wadah. Meskipun citra yang diekstraksi masih menampakkan pesan tersembunyi, fail rahasia bisa diakses tanpa kerusakan dari fail kompresi tanpa perubahan ukuran.

SIMPULAN

Solusi keamanan data yang diimplementasikan melibatkan penggunaan algoritma (AES) dan steganografi untuk melindungi percakapan teks, fail dokumen, dan isinya. Aplikasi Fres-CAESAS menyediakan platform yang memungkinkan pengguna untuk mengamankan informasi melalui teknik enkripsi dan steganografi, atau kombinasi keduanya sesuai dengan kebutuhan mereka.

Sistem keamanan berlapis-lapis dalam aplikasi ini dirancang untuk memberikan tingkat keamanan yang tinggi terhadap data rahasia. Dengan menggunakan AES, data dapat dienkripsi dan didekripsi dengan blok ciphertext simetris, meningkatkan efektivitas kriptografi dalam melindungi informasi sensitif.

Ketika terdeteksi fail rahasia dalam gambar, isi fail tetap terenkripsi dan dikirim sebagai pesan teks, menjaga kerahasiaan informasi tersebut. Proses penyisipan pesan rahasia pada gambar dilakukan dengan mempertahankan penampilan visual yang mirip dengan aslinya, dengan perbedaan hanya pada ukuran fail. Ini menunjukkan bahwa solusi ini tidak hanya efektif dalam melindungi data, tetapi juga menjaga integritas visual dari media penyimpanan.

Dengan demikian, implementasi keamanan data menggunakan AES dan steganografi dengan Aplikasi Fres-CAESAS memberikan lapisan perlindungan yang kokoh terhadap data sensitif, menjadikannya solusi yang dapat diandalkan dalam melibatkan teknologi keamanan data.

DAFTAR PUSTAKA

1. Dadang Iskandar Mulyana. (2022). “Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)”. Jurnal Pendidikan Sains dan Komputer.
2. Dadang Iskandar Mulyana. (2022). “Pengamanan Transkrip Mahasiswa Menggunakan Kriptografi Playfair Cipher”. Jurnal Teknik Elektro dan Komputasi (ELKOM).
3. Federal Information Processing Standards Publication 197.
4. Lusiana, V. (2011). "Implementasi Kriptografi Pada Fail Dokumen Menggunakan Algoritma AES-128." Jurnal Dinamika Informatika.
5. Dadang Iskandar Mulyana. (2022). “Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text”
6. Maulid Hidayat, Muhlis Tahir, Achmad Sukriyadi, Amir Sulton,

Cindi Ajeng S. A, dan Sofyan Abduh F. (2019).”Implementasi Kriptografi RSA Untuk Keamanan Fail Dokumen”

7. Armaja Basuki (2016) “Implementasi Kriptografi Berlapis Menggunakan Algoritma Tansposisi, Vigenere dan Blok Cipher Berbasis Mobile”
8. Dahlia Br Ginting (2010) “Peran Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman)”
9. Dr. Ir. Mochammad Irfan, M.Eng., dan Dr. Ir. Asep Iwan Gunawan, M.Eng (2023) “Kriptografi: Tantangan dan Peluang di Era Digital”
10. Dr. Ir. Mochammad Irfan, M.Eng., Dr. Ir. Asep Iwan Gunawan, M.Eng., dan Dr. Ir. Rini Nurhayati, M.T. (2023) “Pengembangan Metode Kriptografi Baru Menggunakan Algoritma Quantum”
11. Ilham Saputra, Arief Nugroho, dan Muhammad Ilham (2023). “Implementasi Kriptografi Pada Fail Dokumen Menggunakan Algoritma AES-128”
12. Dr. Ir. Mochammad Irfan, M.Eng., Dr. Ir. Asep Iwan Gunawan, M.Eng., dan Dr. Ir. Rini Nurhayati, M.T. (2022). “Penerapan Kriptografi Caesar Cipher Dan Hill Cipher dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realist”
13. Dadang Iskandar Mulyana. (2022). “Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen Dengan Algoritma Triple DES Berbasis Web”
14. Dadang Iskandar Mulyana. (2022) “Implementasi Algoritma One Time menggunakan Algoritma Chiper Transposition Sebagai pengaman Rahasisa Pesan Rail Fence Cipher Dan Route Cipher Untuk Keamanan Fail”
15. Dadang Iskandar Mulyana. (2023) “Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks”