NARASI RECORDING KOMBINASI + BREAKDOWN CODING

Halo semuanya. Pada kesempatan kali ini saya akan mempresentasikan sebuah aplikasi keamanan data berbasis web yang menggabungkan dua teknik sekaligus, yaitu kriptografi dan steganografi. Aplikasi ini mampu mengacak pesan rahasia, dan kemudian menyembunyikannya ke dalam gambar digital tanpa merusak tampilan visualnya.

Konsep Dasar:

Ada dua konsep utama yang digunakan:

1. Kriptografi

Bagian ini bertugas mengacak pesan sehingga tidak dapat dibaca secara langsung.

Pada projek ini digunakan Caesar Cipher dan Vigenère Cipher.

2. Steganografi

Teknik ini bukan mengacak pesan, tetapi menyembunyikan pesan tersebut ke dalam media digital, contohnya gambar.

Kalau kriptografi = membuat pesan sulit dipahami

Steganografi = membuat pesan tidak terlihat

Alur Kerja Aplikasi:

1. Masukkan teks

2. Pilih metode enkripsi

3. Pesan diubah menjadi bentuk acak

4. Pesan terenkripsi diubah ke biner

5. Biner disisipkan ke pixel gambar menggunakan LSB

6. Gambar bisa diunduh (Stego Image)

7. Saat ekstraksi, gambar dibaca ulang pixel-nya

8. Sistem menyusun kembali pesan

Demo Flow:

Masukkan teks rahasia, pilih Caesar Cipher, tampilkan hasil scramble,

pilih Vigenère Cipher, embed ke gambar, extract pesan kembali.

Penjelasan Backend (Python) — Breakdown Fungsi / Algoritma:

1. caesar_encrypt(text, shift)

Tujuan: Menggeser setiap karakter alfabet sebanyak nilai shift.

Algoritma: Cek huruf, ubah ke ASCII, tambahkan shift, modulo 26, kembalikan huruf.

Contoh Efek: HALO shift 5 $\rightarrow$ MFQT

2. vigenere_encrypt(text, key)

Tujuan: Men-shift karakter berdasarkan key.

Algoritma: Loop karakter, hitung offset ASCII key, tambahkan ke karakter.

Keunggulan: Pola shift dinamis.

3. embed_message_lsb(image, message, output_path)

Tujuan: Menyisipkan pesan biner ke pixel gambar.

Algoritma detail: Pesan → ASCII → Biner → Sisipkan ke LSB pixel → Tambahkan NULL byte.

4. extract_message_lsb(image)

Tujuan: Mengambil kembali pesan yang disembunyikan.

Algoritma: Baca LSB pixel, kumpulkan 8 bit, convert ke karakter, berhenti pada NULL byte.

5. Pembuatan gambar template

Menggunakan Image.new() dan draw.text().

6. Penyimpanan file PNG

Dipilih karena tidak merusak data.

Penjelasan Frontend (HTML + JavaScript):

Frontend menyediakan input, preview, embed/extract, dan download gambar.

Struktur Utama HTML:

Input teks, input shift, upload gambar, canvas.

Tailwind CSS:

Digunakan untuk utilitas styling cepat dan konsisten.

JavaScript Functions:

encryptCaesar()

encryptVigenere()

embedMessage()

extractMessage()

downloadStego()

Canvas API:

Digunakan untuk manipulasi pixel per pixel.

Struktur Bit dalam Steganografi:

Perubahan 1 bit pada LSB tidak terlihat oleh mata manusia.

Kelebihan Aplikasi:

Security berlapis, tidak membutuhkan server, UI mudah digunakan.

Kekurangan:

LSB dapat dideteksi analisis forensik, Caesar cipher lemah brute force.

Kesimpulan:

Aplikasi ini berhasil menyembunyikan pesan terenkripsi ke dalam media gambar tanpa merusak tampilan visualnya. Pesan dapat diekstraksi kembali melalui antarmuka web secara intuitif.

Penutup:

Demikian penjelasan mengenai implementasi kriptografi dan steganografi berbasis web. Terima kasih telah menyimak.