LAPORAN ANALISIS KELEMAHAN CIPHER KLASIK

Universitas Teknologi Digital

Disusun Oleh :

1. Mochammad Rival Sopyan - 20123006
2. Fernanda Syah Putra - 20123019
3. Muhamad Rifky Raihan - 20123021

PROGRAM STUDI S1 INFORMATIKA

UNIVERSITAS TEKNOLOGI DIGITAL

TAHUN AJARAN 2024/2025

CAESAR CHIPHER

Teori Singkat

Caesar Cipher adalah algoritma kriptografi klasik yang menyandikan teks dengan cara **menggeser huruf alfabet** sejauh nilai tertentu (*shift*). Misalnya, jika shift = 3, maka A → D, B → E, dan seterusnya. Proses dekripsi dilakukan dengan menggeser huruf ke arah sebaliknya. Termasuk jenis **kriptografi simetris**, karena kunci enkripsi dan dekripsi sama.

Input dan Output

Input:

- Teks (plaintext)
- Nilai shift (0–25)
- Mode (E untuk enkripsi, D untuk dekripsi)

Output:

- Hasil enkripsi atau dekripsi teks.
  Contoh:
  Input: HALO DUNIA, Shift: 3 → Output: KDOR GXQLD

Kelemahan

- Ruang kunci kecil (hanya 25 kemungkinan).
- Mudah dipecahkan dengan *brute force* atau *frequency analysis*.
- Tidak mengenkripsi karakter selain huruf.
- Tidak aman untuk penggunaan modern.

VIGENERE CHIPHE

Teori Singkat

Vigenère Cipher adalah algoritma kriptografi klasik yang mengenkripsi teks menggunakan **kata kunci (key)**.
Setiap huruf pada teks digeser berdasarkan nilai huruf pada kunci. Jika kunci habis, maka diulang. Termasuk jenis **kriptografi simetris** karena kunci yang digunakan sama untuk enkripsi dan dekripsi.

Input dan Output

Input:

- Teks (plaintext)
- Kunci (key)
- Mode (E = enkripsi, D = dekripsi)

Output:

- Hasil enkripsi atau dekripsi.
  Contoh:
  Input: HALODUNIA, Key: KEY → Output: RIJVSUYVJ

Kelemahan

- Rentan terhadap *frequency analysis* jika kunci pendek.
- Dapat dipecahkan dengan *Kasiski test*.
- Tidak aman untuk penggunaan modern

AFFINE CHIPHER

Teori Singkat

Affine Cipher adalah algoritma kriptografi klasik yang mengenkripsi teks dengan mengubah setiap huruf menjadi angka, kemudian dihitung menggunakan dua kunci, yaitu **a** dan **b**. Proses enkripsi dilakukan dengan rumus $C = (aP + b) \bmod 26$, sedangkan dekripsinya menggunakan rumus $P = a^{-1}(C - b) \bmod 26$. Nilai **a** harus koprima terhadap 26 agar bisa memiliki invers. Algoritma ini termasuk jenis **kriptografi simetris** karena menggunakan kunci yang sama untuk enkripsi dan dekripsi.

Input dan Output

Input:

- Teks (plaintext)
- Nilai kunci a dan b
- Mode (E = enkripsi, D = dekripsi)

Output:

- Hasil enkripsi atau dekripsi.
  Contoh:
  Input: HALO, a=5, b=8 → Output: RIFS

Kelemahan

- Mudah dipecahkan dengan *brute force* karena ruang kunci kecil.
- Pola frekuensi huruf tetap terlihat.
- Tidak cocok untuk keamanan modern.

PLAYFAIR CHIPHER

Teori Singkat

Playfair Cipher adalah algoritma kriptografi klasik yang mengenkripsi pasangan huruf (digraph) menggunakan **matriks 5x5** yang dibentuk dari kata kunci (key). Huruf "J" biasanya digabung dengan "I". Enkripsi dilakukan dengan mengganti posisi huruf dalam tabel sesuai aturan baris dan kolom. Algoritma ini termasuk jenis **kriptografi simetris** karena kunci yang digunakan sama untuk enkripsi dan dekripsi.

Input dan Output

Input:

- Teks (plaintext)
- Kata kunci (key)
- Mode (E = enkripsi, D = dekripsi)

Output:

- Hasil enkripsi atau dekripsi.
  Contoh:
  Input: HALO, Key: KEY → Output: ICMT

Kelemahan

- Rentan terhadap analisis frekuensi digraph.
- Tidak aman untuk penggunaan modern.
- Panjang teks bisa berubah karena penambahan huruf "X".

HILL CHIPHER

Teori Singkat

Hill Cipher adalah algoritma **kriptografi klasik berbasis aljabar linear**, yang menggunakan **matriks kunci** untuk mengenkripsi dan mendekripsi pesan.

Setiap huruf diubah menjadi angka (A=0, B=1, …, Z=25), lalu dihitung menggunakan **perkalian matriks mod 26**.

Jenis cipher ini termasuk **kriptografi simetris**, karena kunci enkripsi dan dekripsi sama (namun dekripsi menggunakan invers matriks dari kunci tersebut).

Input dan Output

Input:

- Teks (plaintext)
- Matriks kunci (misalnya 2x2)
- Mode (E = Enkripsi, D = Dekripsi)

Output:

- Hasil enkripsi atau dekripsi berupa teks huruf kapital.
  Contoh:
  Plaintext: “HELP”
  Key: [[3, 3], [2, 5]]
  → Ciphertext: “HIAT”

Kelemahan

- Kunci hanya bisa digunakan jika **matriks memiliki invers modulo 26**.
- Tidak tahan terhadap **serangan analisis linear**.
- Kurang aman untuk komunikasi modern.