# LAPORAN ANALISIS CIPHER KLASIK

Universitas Teknologi Digital


Disusun Oleh :

1. Nabilla Maesaroh (20123027)
2. Sayyidah Muthi Nur Aisyah (20123003)


**PROGRAM STUDI S1 INFORMATIKA**
**UNIVERSITAS TEKNOLOGI DIGITAL**
**TAHUN AJARAN 2024/2025**

1. CAESAR CIPHER

Teori Singkat Caesar Cipher merupakan salah satu bentuk sandi substitusi paling sederhana. Setiap huruf dalam teks digeser sejauh nilai tertentu (disebut shift). Misalnya jika pergeseran 2, maka huruf A akan menjadi C, B menjadi D, dan seterusnya. Cipher ini termasuk dalam kriptografi simetris karena proses enkripsi dan dekripsinya menggunakan kunci yang sama.

Input dan Output

- Input :
  a. Teks biasa (plaintext)
  b. Nilai pergeseran (shift) antara 0–25
  c. Mode: E (enkripsi) atau D (dekripsi)
- Output :

  Hasil teks yang sudah dienkripsi atau didekripsi

  Contoh :

  a. Plaintext: SIFAT
  b. Shift: 4 → Ciphertext: WMJEY
- Kelemahan :
  a. Ruang kunci yang sangat kecil, hanya 25 kemungkinan
  b. Dapat dipecahkan dengan metode brute force atau analisis frekuensi
  c. Tidak mengenkripsi karakter non-alfabet
  d. Tidak aman untuk komunikasi modern karena terlalu sederhana

2. VIGENÈRE CIPHER

Teori Singkat Vigenère Cipher adalah metode enkripsi dengan menggunakan kata kunci (key) untuk menentukan besar pergeseran setiap huruf. Jika kunci lebih pendek dari teks, maka kunci akan diulang hingga panjangnya sama. Cipher ini termasuk dalam kategori kriptografi simetris karena kunci yang digunakan sama untuk proses enkripsi dan dekripsi.

Input dan Output

- Input :
  a. Teks (plaintext) Kunci (key)
  b. Mode: E (enkripsi) atau D (dekripsi)
- Output :
  Hasil enkripsi atau dekripsi teks
  Contoh :
  a. Plaintext: INFORMATIKA
  b. Key: CODE → Ciphertext: KRPJQVCXMSO
- Kelemahan :
  a. Rentan terhadap frequency analysis bila kuncinya terlalu pendek
  b. Dapat dipecahkan menggunakan metode Kasiski atau Friedman Test
  c. Tidak cocok untuk penggunaan keamanan tingkat tinggi

3. AFFINE CIPHER

Teori Singkat Affine Cipher bekerja dengan cara mengubah setiap huruf menjadi angka (A=0, B=1, …, Z=25) lalu dihitung menggunakan dua parameter kunci, yaitu a dan b.
Rumus enkripsi : $C = (aP + b) \bmod 26$,
sedangkan dekripsi: $P = a^{-1}(C - b) \bmod 26$,
dengan syarat nilai a harus relatif prima terhadap 26 agar memiliki invers. Cipher ini juga bersifat simetris.
Input dan Output

- Input :
  a. Teks (plaintext)
  b. Nilai kunci a dan b
  c. Mode: E (enkripsi) atau D (dekripsi)
- Output :
  Teks hasil enkripsi atau dekripsi
  Contoh :
  a. Plaintext: DATA
  b. a = 7, b = 3 → Ciphertext: GLWL
- Kelemahan :
  a. Ruang kunci relatif kecil dan mudah dipecahkan dengan brute force
  b. Pola huruf masih bisa dikenali dengan analisis frekuensi
  c. Tidak direkomendasikan untuk sistem keamanan modern.

4. PLAYFAIR CIPHER

Teori Singkat Playfair Cipher mengenkripsi pasangan huruf (disebut digraph) menggunakan tabel 5x5 yang dibuat berdasarkan kata kunci. Huruf "J" biasanya digabungkan dengan "I". Enkripsi dilakukan dengan mencari posisi kedua huruf di tabel dan menggantinya sesuai aturan baris dan kolom. Cipher ini tergolong simetris.
Input dan Output

- Input :
  a. Teks (plaintext)
  b. Kata kunci (key)
  c. Mode: E (enkripsi) atau D (dekripsi)
- Output :
  Hasil enkripsi atau dekripsi teks
  Contoh :
  a. Plaintext: KRIPTOGRAFI
  b. Key: TEKNIK → Ciphertext: LTMUYNKQTCVK
- Kelemahan:
  a. Rentan terhadap frequency analysis pada pasangan huruf
  b. Kadang menambahkan huruf ekstra (misalnya "X") agar jumlah huruf genap
  c. Tidak efektif untuk keamanan modern

5. HILL CIPHER

Teori Singkat Hill Cipher merupakan metode kriptografi klasik berbasis aljabar linear. Setiap huruf diubah menjadi angka, kemudian dihitung menggunakan perkalian matriks kunci (key matrix) dan dioperasikan dengan mod 26. Proses dekripsi dilakukan dengan menggunakan invers dari matriks kunci tersebut. Karena menggunakan perhitungan matriks, cipher ini bisa mengenkripsi lebih dari satu huruf sekaligus.
Input dan Output

- Input :
  a. Teks (plaintext)
  b. Matriks kunci (misalnya 2×2 atau 3×3)
  c. Mode: E (enkripsi) atau D (dekripsi)
- Output :
  Teks hasil enkripsi atau dekripsi huruf kapital
  Contoh :
  a. Plaintext: DATA
  b. Key: [[3, 2], [5, 7]] → Ciphertext: ZEBU
- Kelemahan :
  a. Matriks kunci harus memiliki invers modulo 26 agar bisa didekripsi
  b. Tidak tahan terhadap linear analysis attack
  c. Proses enkripsi memerlukan perhitungan matriks yang kompleks