CIPHER KLASIK: Implementasi Implementasi Kriptografi

Presentasi ini disusun untuk memenuhi Tugas Matakuliah Kriptografi.

Oleh: Wildan Hanif (20123074) & Zulfitrah Akbar (20123084)

PROGRAM STUDI INFORMATIKA S1 - UNIVERSITAS TEKNOLOGI DIGITAL, BANDUNG 2025

Agenda: Lima Algoritma Kunci

Kami akan membahas lima jenis Cipher Klasik, mulai dari yang paling sederhana hingga yang menggunakan aljabar linear.

Caesar Cipher

Cipher substitusi paling dasar, menggeser huruf sesuai n langkah.

Affine Cipher

Pengembangan Caesar dengan fungsi perkalian dan penjumlahan dua kunci.

Vigenere Cipher

Menggunakan kata kunci untuk pergeseran berulang, pola tidak seragam.

Playfair Cipher

Cipher berbasis pasangan huruf (digraph).

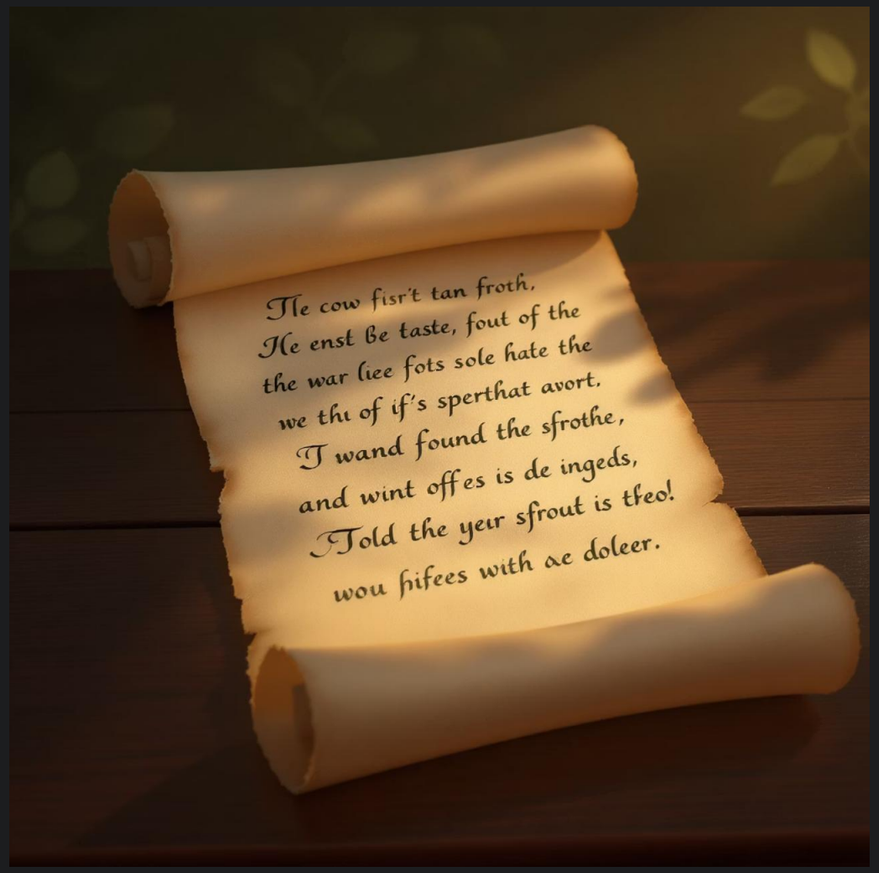
Hill Cipher

Menggunakan aljabar linear dan matriks kunci.

1. Caesar Cipher

Teori Singkat

Caesar Cipher adalah bentuk cipher substitusi paling sederhana, ditemukan oleh Julius Caesar. Algoritma ini menggeser setiap huruf dalam alfabet sejauh n langkah (misalnya, A → D jika pergeseran = 3). Jika mencapai ujung alfabet, pergeseran dilanjutkan dari awal (wrap-around). Hanya bekerja pada huruf, karakter lain seperti angka dan tanda baca diabaikan.



> Sangat lemah terhadap serangan brute force karena hanya ada 25 kemungkinan kunci. Pola frekuensi huruf tetap jelas, memudahkan analisis.

Implementasi Caesar Cipher

Fungsi enkripsi dan dekripsi menggunakan operasi modulo 26 untuk memastikan pergeseran tetap berada dalam batas alfabet.

Enkripsi

```
def caesar_encrypt(text, shift):    return
''.join(chr((ord(c) - s + shift) % 26 + s)         if
c.isalpha() else c         for c, s in [(ch, ord('A') if
ch.isupper()         else ord('a')) for ch in text])
```

Dekripsi

```
def caesar_decrypt(ciphertext, shift): return
caesar_encrypt(ciphertext, -shift)
```

2. Affine Cipher

Pengembangan Caesar

Affine Cipher menambahkan fungsi perkalian dan penjumlahan, menggunakan dua kunci: **a** (harus koprima dengan 26) dan **b** (bilangan bulat).

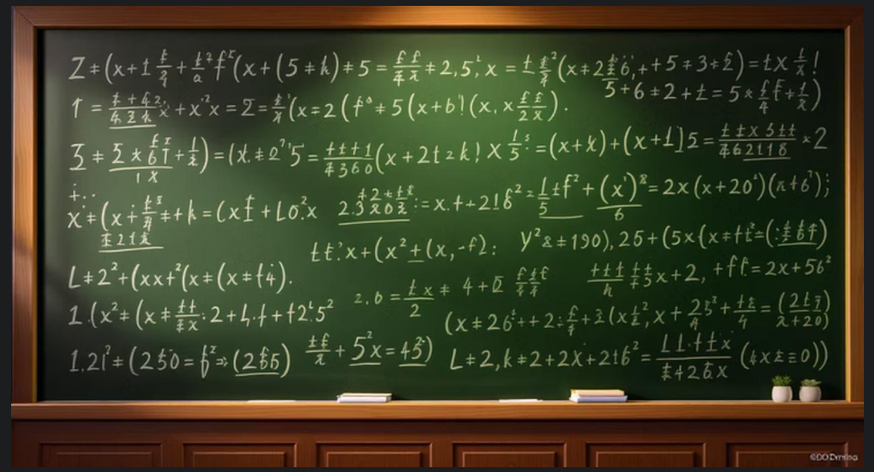
Rumus

Enkripsi: $C = (aP + b) \mod 26$

Dekripsi: $P = a^{-1}(C - b) \mod 26$

Kelemahan

Masih rentan terhadap analisis frekuensi. Kunci terbatas karena nilai **a** harus koprima dengan 26.



3. Vigenere Cipher

Kunci Berulang

Ditemukan oleh Blaise de Vigenère. Cipher ini menggunakan kata kunci untuk menentukan besar pergeseran tiap huruf, membuat pola pergeseran tidak seragam.

Contoh: Plaintext HELLO dengan kunci KEY. Huruf pertama digeser sesuai 'K', kedua sesuai 'E', ketiga sesuai 'Y', lalu diulang.

Lebih kuat dari Caesar, tetapi dapat dipecahkan dengan analisis Kasiski atau Index of Coincidence untuk mencari pola pengulangan kunci.

Implementasi Vigenere Cipher

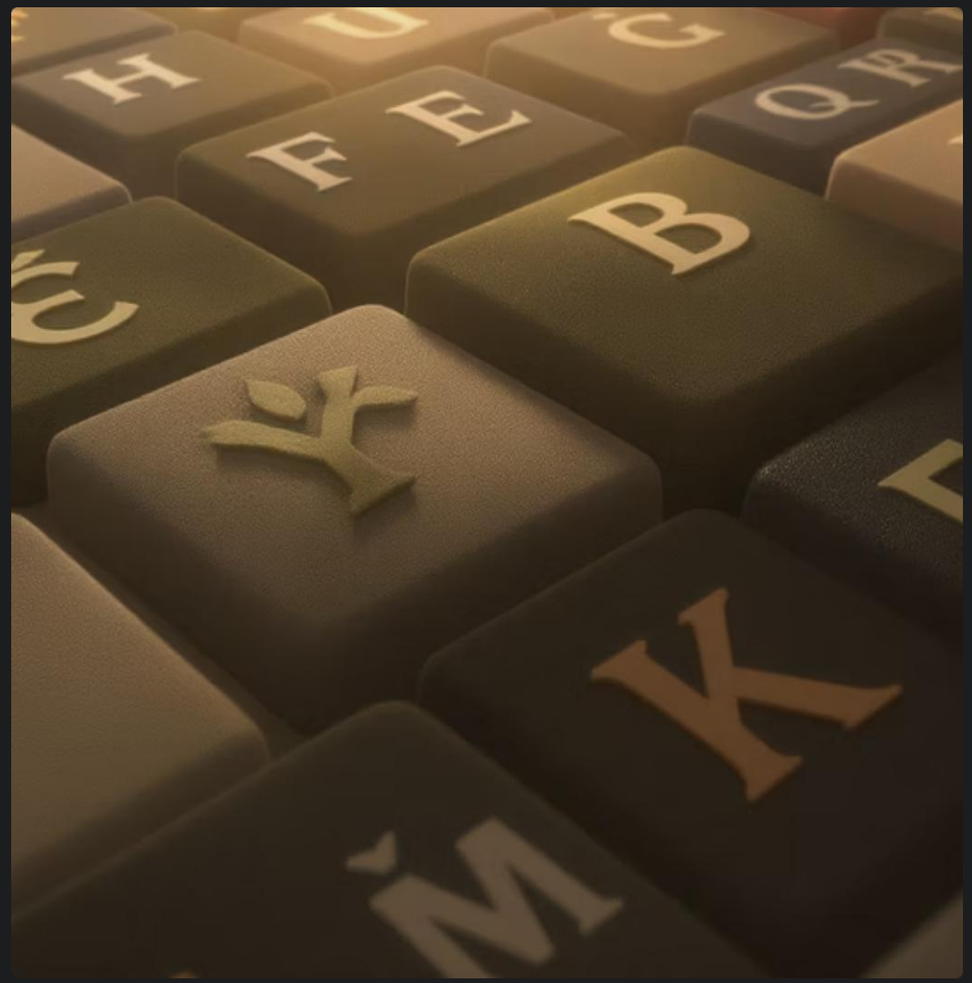
Enkripsi

```
def vigenere_encrypt(text, key):
    res, j = "", 0
    for c in text:
        if c.isalpha():
            s = ord('A') if c.isupper() else ord('a')
            k = ord(key[j % len(key)].lower()) - ord('a')
            res += chr((ord(c) - s + k) % 26 + s); j += 1
        else: res += c
    return res
```

Dekripsi

```
def vigenere_decrypt(cipher, key):
    res, j = "", 0
    for c in cipher:
        if c.isalpha():
            s = ord('A') if c.isupper() else ord('a')
            k = ord(key[j % len(key)].lower()) - ord('a')
            res += chr((ord(c) - s - k) % 26 + s); j += 1
        else: res += c
    return res
```

4. Playfair Cipher



Teori Singkat

Playfair Cipher ditemukan oleh Charles Wheatstone (1854) dan dipopulerkan oleh Lord Playfair. Cipher ini bekerja dengan pasangan huruf (digraph) menggunakan tabel 5×5 huruf (I dan J digabung).

Aturan Rumus

- Satu baris → huruf diganti huruf di kanan.
- Satu kolom → huruf diganti huruf di bawah.
- Beda baris & kolom → tukar silang.

Kelemahan

Lebih kuat dari Vigenere, tetapi masih dapat dianalisis dengan frekuensi pasangan huruf.

5. Hill Cipher

Hill Cipher menggunakan aljabar linear. Plaintext diubah menjadi vektor angka, lalu dikalikan dengan matriks kunci (mod 26). Matriks kunci harus invertible agar dekripsi bisa dilakukan.

Prinsip Aljabar Linear

Plaintext diubah menjadi vektor angka, lalu dikalikan dengan matriks kunci (mod 26).

Rumus

$C = (K \times P) \bmod 26$
$P = (K^{-1} \times C) \bmod 26$

Kelemahan

Jika ada cukup banyak pasangan plaintext–ciphertext, kunci bisa dihitung.

Contoh Implementasi Kode

https://drive.google.com/drive/folders/1ggUYBmjoN8713EXJZOeBda318jBihBLg?usp=drive_link

```python
# ============================================================================
# 1. CAESAR CIPHER
# ============================================================================
def caesar_encrypt(text, shift):
    """
    Mengenkripsi teks menggunakan Caesar Cipher.
    Hanya karakter alfabet yang dienkripsi, karakter lain diabaikan.
    """
    result = ""
    for char in text:
        if char.isalpha(): # Hanya proses huruf
            start = ord('A') if char.isupper() else ord('a')
            # Rumus Enkripsi Caesar: C = (P + K) mod 26
            encrypted_char = chr((ord(char) - start + shift) % 26 + start)
            result += encrypted_char
        else:
            result += char # Karakter non-alfabet tidak diubah
    return result

def caesar_decrypt(ciphertext, shift):
    """
    Mendekripsi teks dari Caesar Cipher.
    Ini sama dengan enkripsi dengan pergeseran negatif.
    """
    # Rumus Dekripsi Caesar: P = (C - K) mod 26
    return caesar_encrypt(ciphertext, -shift)
```

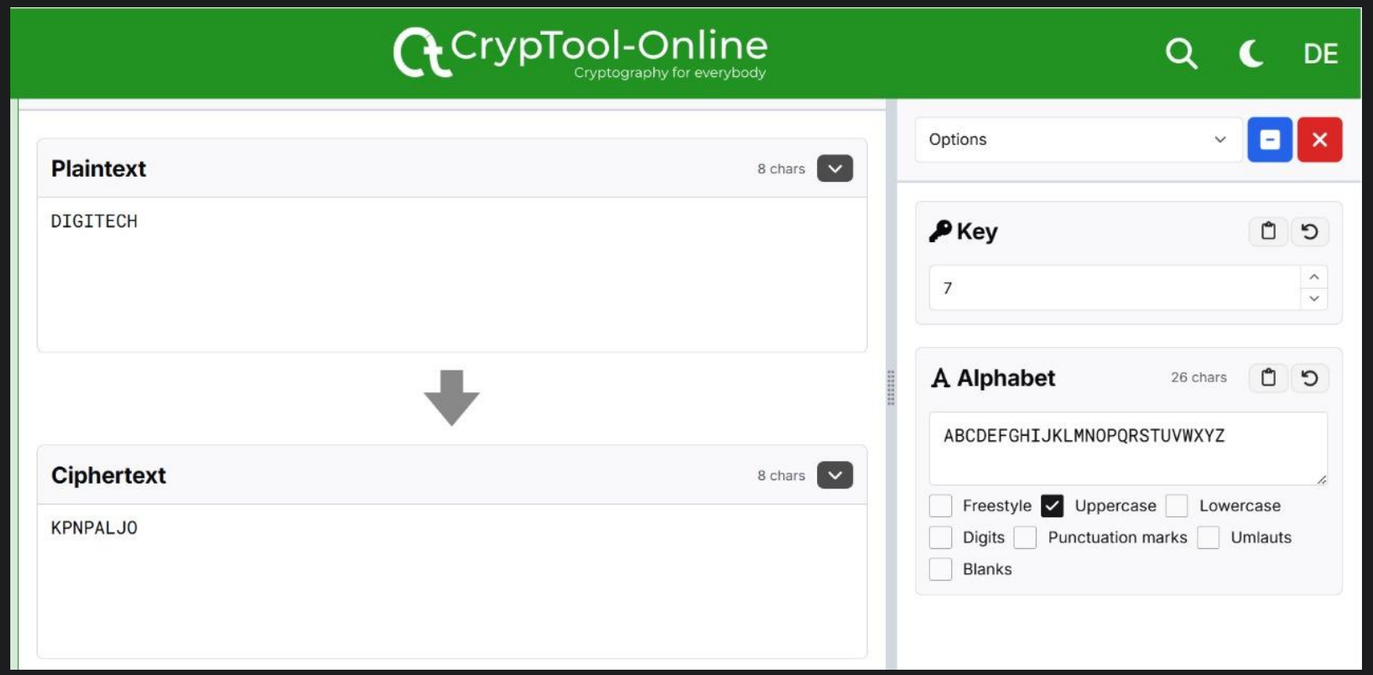
Implementasi dengan Cybertool

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

===== PROGRAM CIPHER KLASIK =====
Pilih Cipher:
1. Caesar Cipher
2. Affine Cipher
3. Vigenere Cipher
4. Playfair Cipher
5. Hill Cipher
0. Keluar
Masukkan pilihan Anda: 1
Pilih mode (1: Enkripsi, 2: Dekripsi): 1
Masukkan teks: DIGITECH
Masukkan kunci pergeseran (angka): 7

Ciphertext: KPNPALJO

Apakah Anda ingin menyimpan hasil ini ke file? (y/n):
```



Kesimpulan dan Takeaway

Cipher Klasik menunjukkan evolusi awal kriptografi, dari substitusi sederhana hingga penggunaan aljabar.

5

Cipher Dibahas

Caesar, Affine, Vigenere, Playfair, Hill.

26

Modulo Alfabet

Dasar operasi untuk semua cipher substitusi berbasis huruf Latin.

2

Kunci Affine

Membutuhkan dua kunci (a dan b) untuk enkripsi.

> Meskipun lemah terhadap komputer modern, pemahaman tentang Cipher Klasik adalah fondasi penting dalam studi Kriptografi.