Kriptografi

02. Implementasi Cipher Klasik

Kodrat Mahatma

Universitas Teknologi Digital

Tujuan Pembelajaran

- Memahami prinsip kerja cipher klasik.
- Mengimplementasikan enkripsi dan dekripsi sederhana.
- Menguji keamanan dasar cipher klasik.

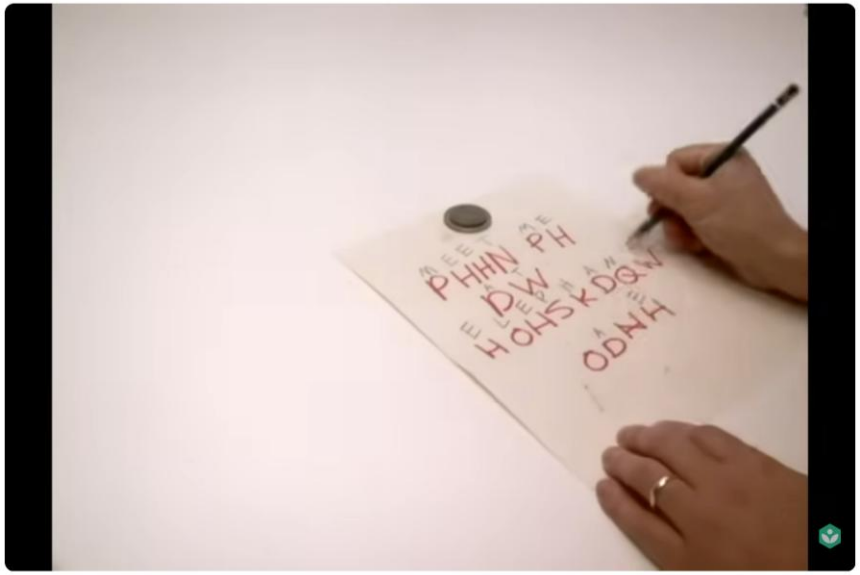
Konsep Dasar Cipher Klasik

Cipher klasik dibagi menjadi dua kategori utama:

1. Substitusi: mengganti simbol dengan simbol lain.
2. Transposisi: mengubah urutan huruf dalam pesan.

Caesar Cipher – Konsep

- Setiap huruf digeser sejauh n posisi.
- Contoh: shift = 3, A→D, B→E.
- Plaintext: HELLO → Ciphertext: KHOOR



The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy

https://youtu.be/sMOZf4GN3oc?si=7P0YRY0PF5WdZF87

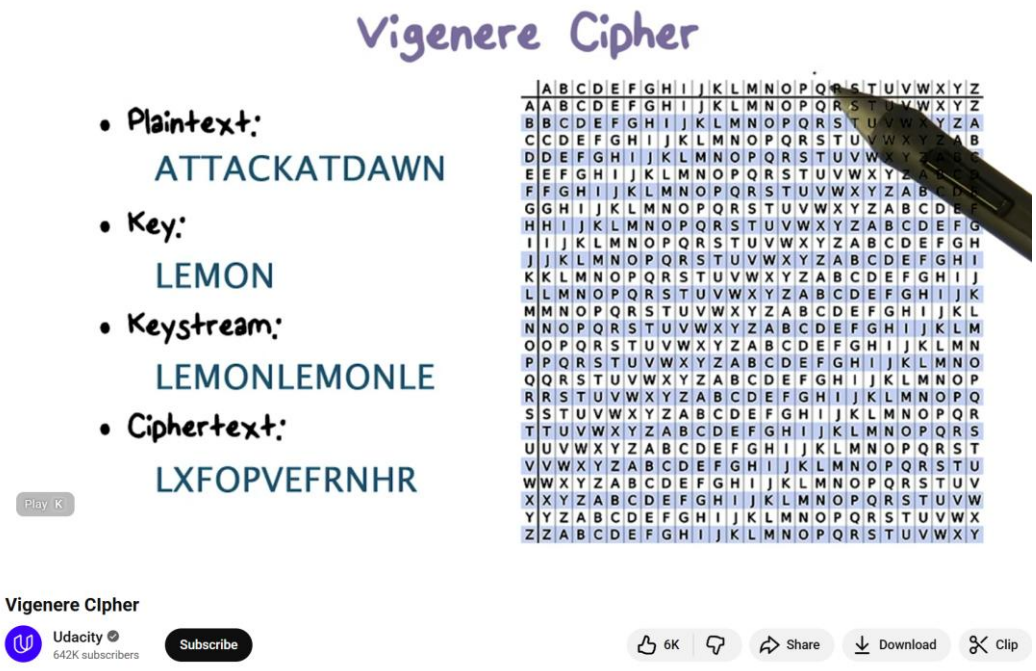
Caesar Cipher – Python Implementation

```
def caesar_encrypt(text, shift):
    result = ''
    for char in text:
        if char.isalpha():
            base = ord('A') if char.isupper() else ord('a')
            result += chr((ord(char) - base + shift) % 26 + base)
        else:
            result += char
    return result

print(caesar_encrypt('HELLO', 3))
```

Vigenère Cipher – Konsep

- Menggunakan kata kunci untuk menentukan pergeseran setiap huruf.
- Contoh: Kunci = LEMON
- Plaintext = ATTACKATDAWN
- Ciphertext = LXFOPVEFRNHR



https://youtu.be/SkJcmCaHqSo?si=A3JfwsoEQJJVhD4Z

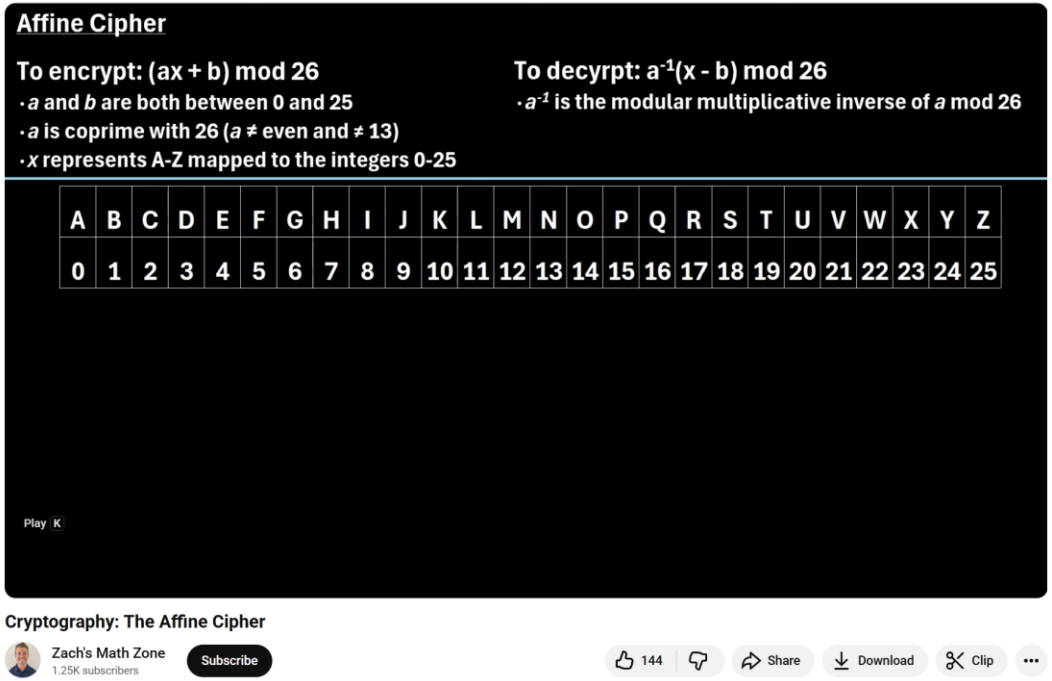
Vigenère Cipher – Python Implementation

```
def vigenere_encrypt(plain, key):
    key = key.upper()
    result = ''
    for i, char in enumerate(plain.upper()):
        if char.isalpha():
            shift = ord(key[i % len(key)]) - 65
            result += chr((ord(char) - 65 + shift) % 26 + 65)
        else:
            result += char
    return result

print(vigenere_encrypt('ATTACKATDAWN', 'LEMON'))
```

Affine Cipher – Konsep

- Rumus: C = (aP + b) mod 26
- Dengan a dan 26 harus relatif prima.
- Contoh: a=5, b=8 → P='A' → C='I'



https://youtu.be/iyESl17IqFQ?si=kAWgmmnaC7soQRvi
https://youtu.be/sroLDJI98sY?si=T5YjehbeQ9H_Q_F3

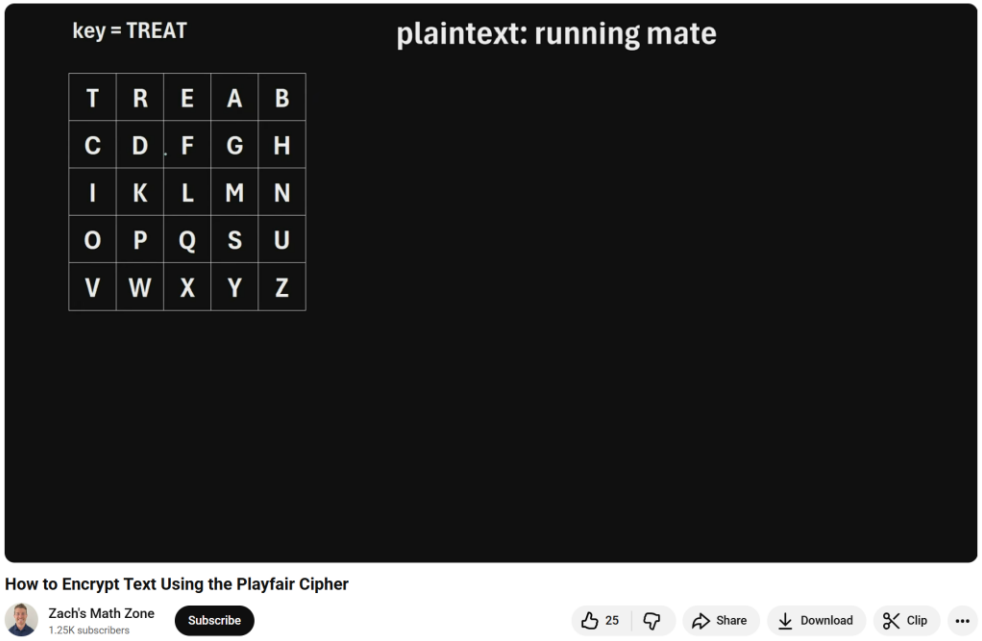
Affine Cipher – Python Implementation

```
def affine_encrypt(text, a, b):
    result = ''
    for char in text.upper():
        if char.isalpha():
            result += chr(((a * (ord(char) - 65) + b) % 26) + 65)
        else:
            result += char
    return result

print(affine_encrypt('HELLO', 5, 8))
```

Playfair Cipher – Konsep

- Menggunakan matriks 5x5 dari kata kunci.
- Langkah: bentuk pasangan huruf, substitusi sesuai posisi di tabel.
- Contoh: KEYWORD → tabel kunci, kemudian enkripsi per pasangan.



https://youtu.be/PrpwPjG3jt4?si=5XpjEvVSSHiNJWhP

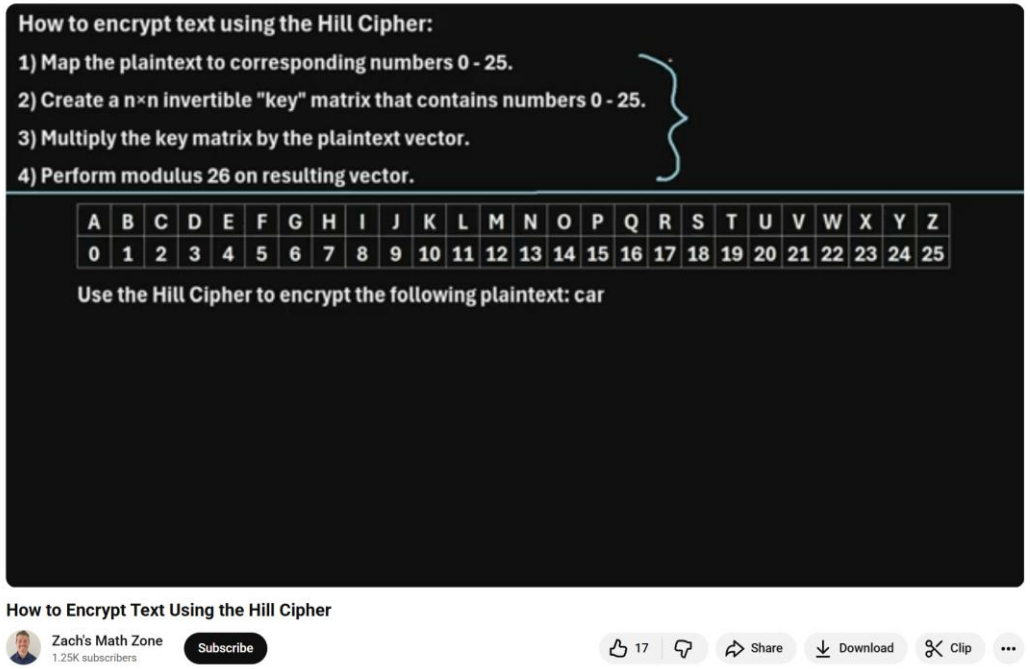
Playfair Cipher – Python (Skema Dasar)

```
def generate_table(key):
    alphabet = 'ABCDEFGHIKLMNOPQRSTUVWXYZ'
    table = ''
    for c in key.upper() + alphabet:
        if c not in table:
            table += c
    return [table[i:i+5] for i in range(0,25,5)]

table = generate_table('KEYWORD')
for row in table: print(row)
```

Hill Cipher – Konsep

- Berdasarkan aljabar linear.
- Gunakan matriks kunci (n×n) dan operasi mod 26.
- C = K × P (mod 26)



https://youtu.be/uRRYf2f7kYA?si=Fpl1gjAbruUXhLVR

Hill Cipher – Python (2x2)

```
import numpy as np

def hill_encrypt(text, key):
    text = text.upper().replace(' ', '')
    n = int(len(key)**0.5)
    key = np.array(key).reshape(n, n)
    result = ''
    for i in range(0, len(text), n):
        block = [ord(c) - 65 for c in text[i:i+n]]
        cipher = np.dot(key, block) % 26
        result += ''.join(chr(c + 65) for c in cipher)
    return result

print(hill_encrypt('TEST', [3,3,2,5]))
```

Perbandingan Cipher Klasik

- Caesar: mudah dipecahkan dengan brute force.
- Vigenère: lebih kuat, tapi rentan terhadap analisis frekuensi.
- Hill: bergantung pada matriks kunci invertibel.
- Affine: kombinasi linear sederhana.

Cipher	Karakteristik	Kelebihan	Kelemahan	Penjelasan Singkat
Caesar Cipher	Pergeseran huruf tetap (misal +3)	Sangat mudah dipahami dan diimplementasikan	Mudah dipecahkan dengan brute force karena hanya 25 kemungkinan kunci	Setiap huruf digeser dengan jumlah tetap. Contoh: A→D, B→E.
Vigenère Cipher	Menggunakan kunci berupa kata, dengan pergeseran berbeda per huruf	Lebih kuat dari Caesar karena pergeseran bergantung pada kunci	Rentan terhadap analisis frekuensi jika kuncinya pendek atau berulang	Polialfabetik cipher; tiap huruf plaintext dikombinasikan dengan huruf kunci.
Hill Cipher	Berdasarkan operasi matriks mod 26	Sulit dipecahkan tanpa mengetahui matriks kunci	Hanya dapat digunakan jika matriks kunci invertibel (memiliki invers)	Mengubah huruf menjadi vektor dan mengenkripsi dengan perkalian matriks.
Affine Cipher	Kombinasi linear dari Caesar Cipher ($E(x) = ax + b \bmod 26$)	Sedikit lebih kuat dari Caesar	Masih mudah dipecahkan karena bersifat linear sederhana	Kombinasi substitusi linier dengan dua parameter a dan b yang memenuhi $\gcd(a,26)=1$.

Aktivitas Praktikum

1. Implementasikan dua cipher klasik menggunakan Python.
2. Buat input/output file teks.
3. Bandingkan hasilnya dengan CrypTool atau CyberChef.

Diskusi

- Apa kelemahan utama cipher klasik di era modern?
- Bagaimana cara menambah keamanan tanpa mengganti algoritma sepenuhnya?

Transisi ke Cipher Modern

- Cipher modern (AES, RSA) menyelesaikan kelemahan klasik dengan matematika modular kompleks, panjang kunci besar, dan operasi bit-level.

Tugas Mini

Buat program sederhana yang:

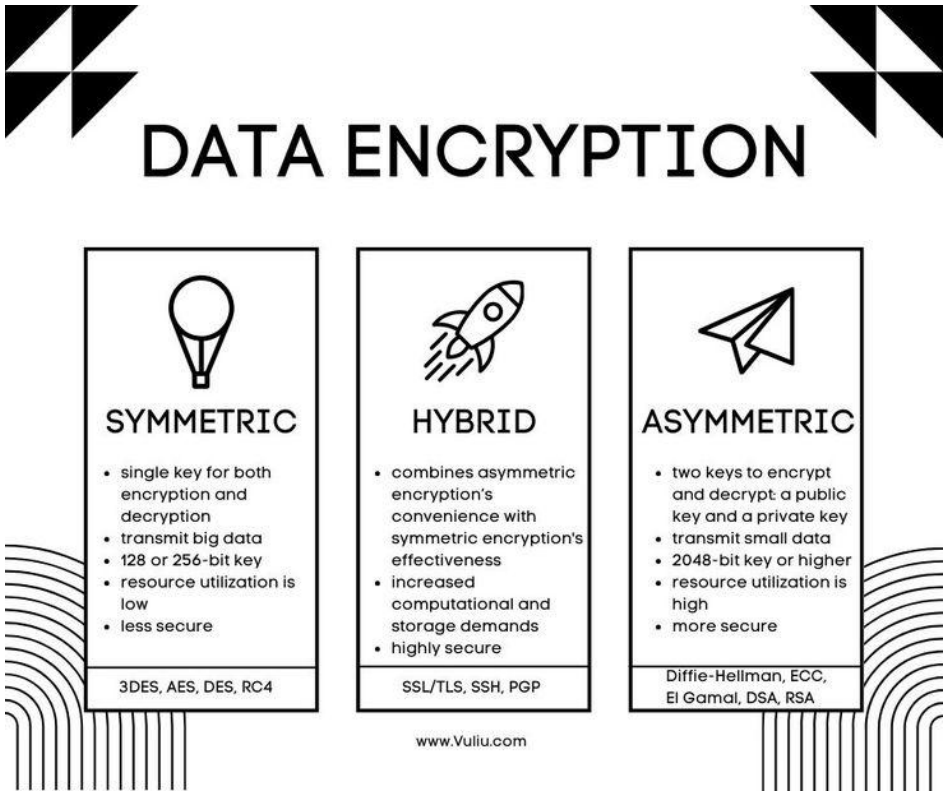
- Menerapkan Caesar & Vigenère Cipher.
- Mampu enkripsi dan dekripsi otomatis.
- Menyimpan hasil ke file .txt.

Sumber Belajar

- **https://www.cryptool.org/en/**
- **Cryptography for Everybody** https://www.youtube.com/c/nilsretrohobbyroom
- AI
- Dan lain-lain

Penutup

- Cipher klasik adalah pondasi untuk memahami kriptografi modern.
- Selanjutnya (minggu depan): Implementasi DES dan AES.



Selamat belajar !

‘Cryptography is the mathematics of trust.’