LAPORAN SINGKAT ANALISIS KEKUATAN DAN KELEMAHAN 5 KRIPTOGRAFI KLASIK

Dosen Pengampu: **Kodrat Mahatma, S.T., M.Kom.**

Disusun Oleh:

Fia Nurfadilla	20123052
Nur Anisa Fitri	20123063

PROGRAM STUDI INFORMATIKA S1

UNIVERSITAS TEKNOLOGI DIGITAL

BANDUNG

2025

1. Pendahuluan

Kriptografi klasik merupakan dasar dari sistem keamanan informasi modern. Walaupun algoritma klasik telah banyak digantikan oleh algoritma kriptografi modern seperti AES dan RSA, pemahaman terhadap algoritma klasik tetap penting untuk memahami prinsip dasar enkripsi (encryption) dan dekripsi (decryption).

Laporan ini membahas lima algoritma kriptografi klasik, yaitu: Caesar Cipher, Vigenère Cipher, Playfair Cipher, Hill Cipher, dan Affine Cipher. Seluruh algoritma tersebut telah diuji menggunakan perangkat lunak CrypTool 2, yang memungkinkan analisis, visualisasi, dan pembandingan berbagai metode kriptografi secara interaktif.

2. Analisis Lima Algoritma Kriptografi Klasik

A. Caesar Cipher

Caesar Cipher mengenkripsi teks dengan menggeser setiap huruf sebanyak *n* posisi dalam alfabet.

- **Kekuatan:**
  - Sederhana dan mudah diimplementasikan.
  - Efektif untuk memperkenalkan konsep dasar substitusi.
- **Kelemahan:**
  - Ruang kunci kecil (hanya 25 kemungkinan).
  - Sangat rentan terhadap serangan brute-force dan analisis frekuensi.

B. Vigenère Cipher

Menggunakan kunci berupa kata untuk menentukan pergeseran huruf yang berbeda pada setiap posisi teks.

- **Kekuatan:**
    - Pola enkripsi lebih kompleks dibanding Caesar Cipher.
    - Tahan terhadap analisis frekuensi sederhana.
- **Kelemahan:**
    - Jika kunci pendek atau berulang, cipher dapat dipecahkan dengan metode Kasiski atau Friedman.
    - Tidak cocok untuk komunikasi modern tanpa penerapan varian yang lebih aman.

C. Playfair Cipher

Cipher substitusi digraf (dua huruf) menggunakan matriks 5x5 yang berisi huruf kunci.

- **Kekuatan:**
    - Menyulitkan analisis frekuensi karena bekerja dengan pasangan huruf.
    - Lebih aman dibanding Caesar dan Vigenère pada konteks klasik.
- **Kelemahan:**
    - Masih dapat dianalisis secara statistik jika ciphertext cukup panjang.
    - Tidak mendukung angka dan simbol tanpa modifikasi tambahan.

D. Hill Cipher

Menggunakan operasi matriks linear pada blok huruf untuk menghasilkan ciphertext.

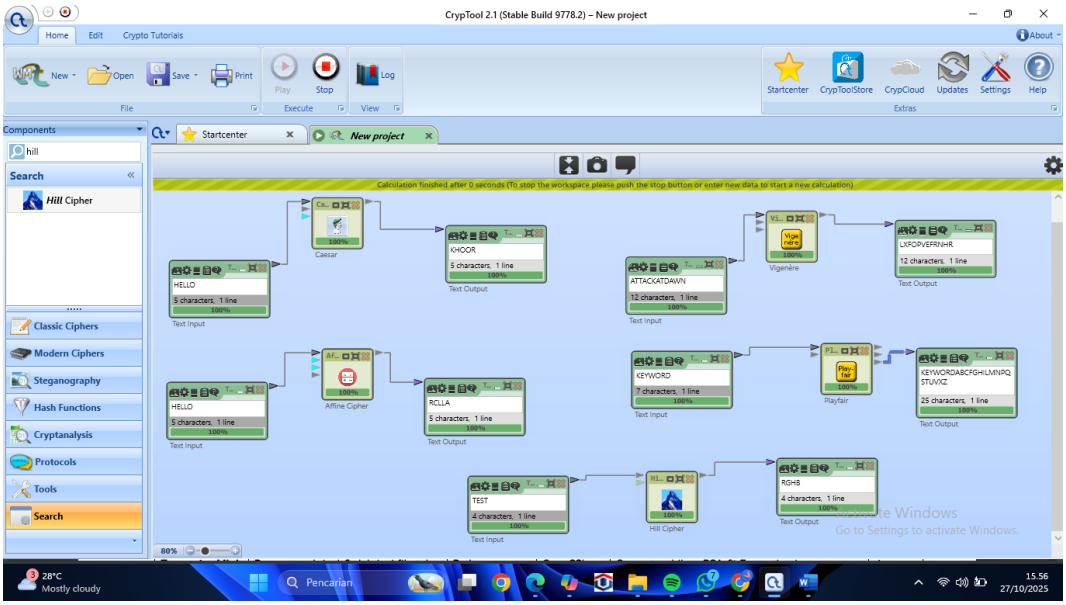
- **Kekuatan:**
    - Menghasilkan pola enkripsi kompleks menggunakan aljabar linear.
    - Efisien untuk pengolahan blok data yang lebih besar.
- **Kelemahan:**
    - Kunci harus berupa matriks invertibel (tidak semua matriks valid).
    - Rentan terhadap serangan *known-plaintext attack* jika terdapat cukup pasangan teks asli dan terenkripsi.

E. Affine Cipher

Merupakan kombinasi antara transformasi linear dan pergeseran sederhana dalam alfabet.

- **Kekuatan:**
  - Lebih kuat dibanding Caesar karena menggunakan dua parameter kunci (a, b).
  - Ruang kunci lebih luas.
- **Kelemahan:**
  - Termasuk cipher substitusi monoalfabetik, masih dapat dianalisis secara frekuensi.
  - Kunci “a” harus coprime dengan 26, sehingga pilihan terbatas.

3. Implementasi dengan CrypTool 2



Seluruh algoritma di atas diimplementasikan dan diuji menggunakan CrypTool 2, aplikasi edukatif berbasis Windows untuk eksplorasi kriptografi klasik dan modern.

Langkah-langkah yang dilakukan dalam CrypTool 2 meliputi:

1. Menentukan algoritma yang akan diuji (Caesar, Vigenère, Playfair, Hill, atau Affine).
2. Mengatur parameter kunci dan memasukkan plaintext.
3. Melihat hasil enkripsi secara visual.
4. Membandingkan tingkat kesulitan pemecahan tiap algoritma.

Hasil implementasi menunjukkan:

- Caesar Cipher paling mudah dipecahkan dengan brute-force.
- Vigenère dan Playfair relatif lebih sulit, namun masih rentan jika diketahui panjang kuncinya.
- Hill Cipher menampilkan enkripsi paling kompleks secara matematis.
- Affine Cipher menunjukkan keseimbangan sederhana namun tetap lebih kuat dari Caesar.

4. Kesimpulan

Lima algoritma kriptografi klasik yang dianalisis memiliki nilai edukatif **tinggi** dalam memahami dasar keamanan informasi. Walaupun tidak layak digunakan dalam sistem keamanan modern, mereka berperan penting dalam pembelajaran konsep fundamental kriptografi seperti substitusi, transposisi, dan operasi matematis pada teks.

Implementasi melalui CrypTool 2 memberikan pengalaman praktis yang membantu mahasiswa memahami:

- Hubungan antara kunci, plaintext, dan ciphertext.
- Kelemahan dasar yang dimanfaatkan dalam kriptanalisis.
- Prinsip evolusi dari kriptografi klasik menuju kriptografi modern.