# IMPLEMENTASI ALGORITMA KRIPTOGRAFI KLASIK (CAESAR, VIGENERE, AFFINE, PLAYFAIR, HILL)

Disusun Oleh:

Adkia (20123047)

Ihsan Tafaquh fiddin (20123013)

## 1. Tujuan

Mempelajari dan mengimplementasikan lima algoritma kriptografi klasik untuk memahami cara kerja enkripsi dan dekripsi pesan serta melakukan analisis kelemahannya.

## 2. Dasar Teori

Kriptografi klasik merupakan metode pengamanan pesan yang digunakan sebelum era komputer modern. Prinsip utamanya adalah mengubah pesan asli (plaintext) menjadi bentuk tidak bermakna (ciphertext) dengan menggunakan kunci tertentu.

Algoritma yang digunakan dalam praktikum ini meliputi:

- Caesar Cipher – Menggeser huruf berdasarkan jumlah tertentu dalam alfabet.
- Vigenere Cipher – Menggunakan tabel substitusi berdasarkan kata kunci berulang.
- Affine Cipher – Menggunakan operasi linear dalam bentuk (a*x + b) mod 26.
- Playfair Cipher – Menggunakan matriks 5x5 untuk mengenkripsi pasangan huruf
- Hill Cipher – Menggunakan operasi matriks dalam aritmetika modulo 26.

## 3. Alat dan Bahan

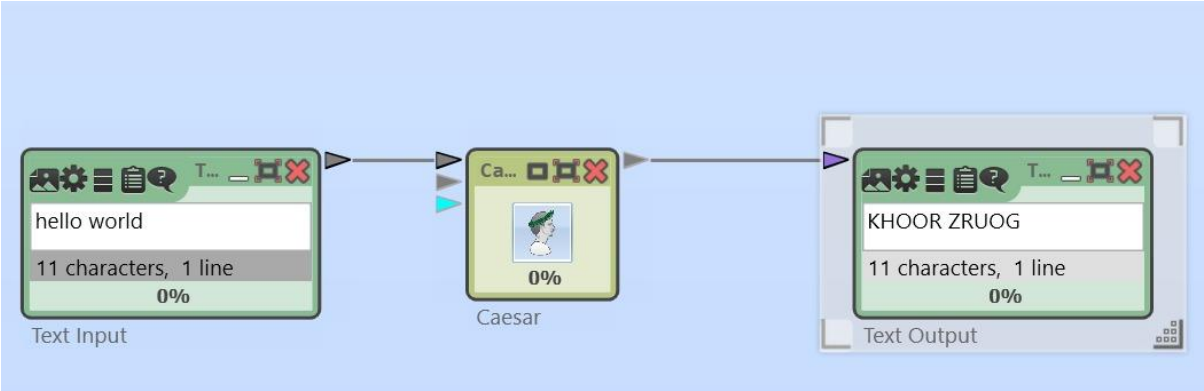
- Platform: Google Colab
- Perangkat Lunak Pendukung: CrypTool
- Bahasa Pemrograman: Python
- Library: NumPy (untuk operasi matriks pada Hill Cipher)
- Sumber kode: GitHub – Praktikum Cipher oleh Adkia Ihsan

## 4. Langkah Kerja

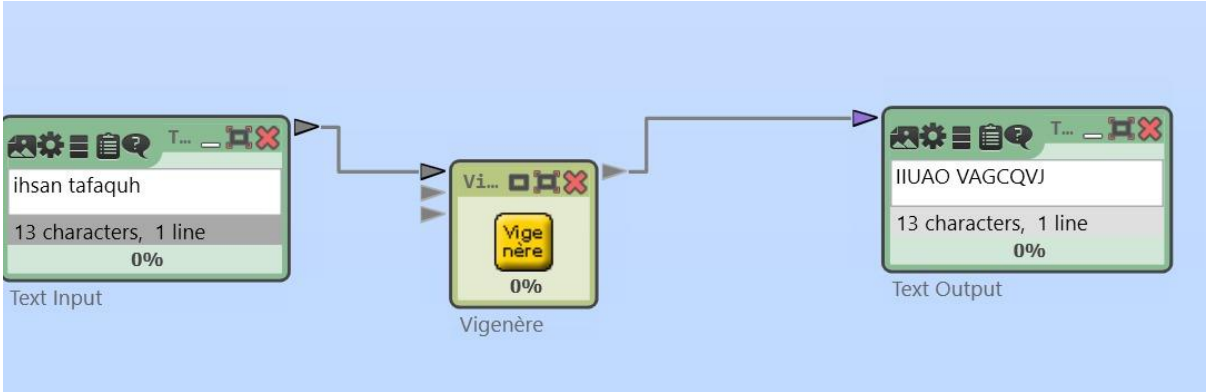
- Membuat fungsi enkripsi dan dekripsi untuk masing-masing algoritma.
- Menguji hasil enkripsi dengan beberapa contoh plaintext.
- Melakukan dekripsi untuk memastikan hasil sesuai dengan pesan asli.
- Melakukan analisis kelemahan tiap algoritma.
- Menyimpulkan hasil implementasi dalam laporan singkat.

## 5. Hasil Implementasi

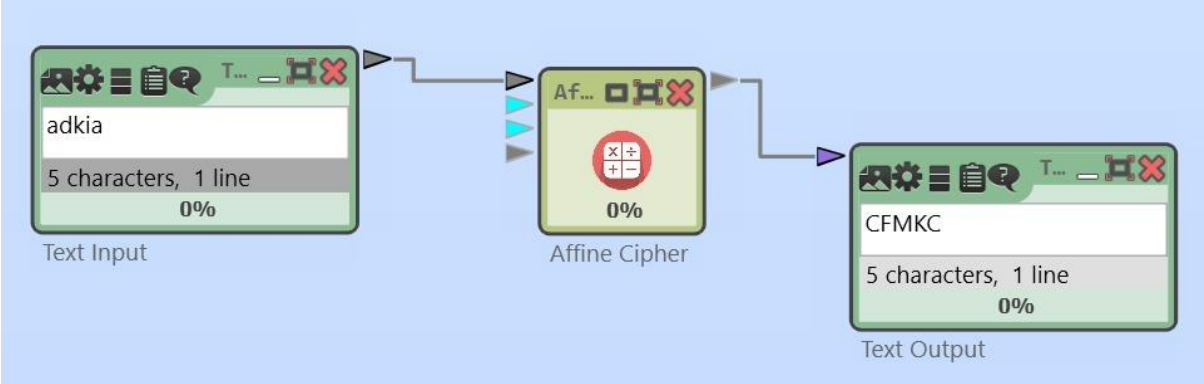
- Caesar



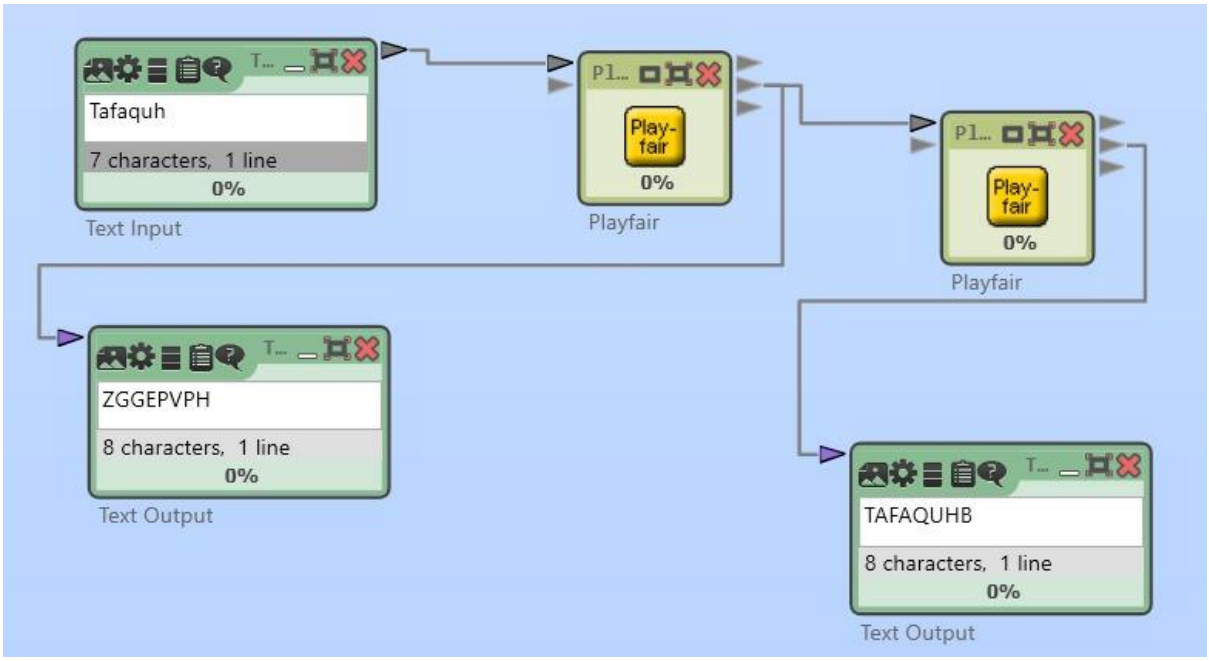

- Vigenere



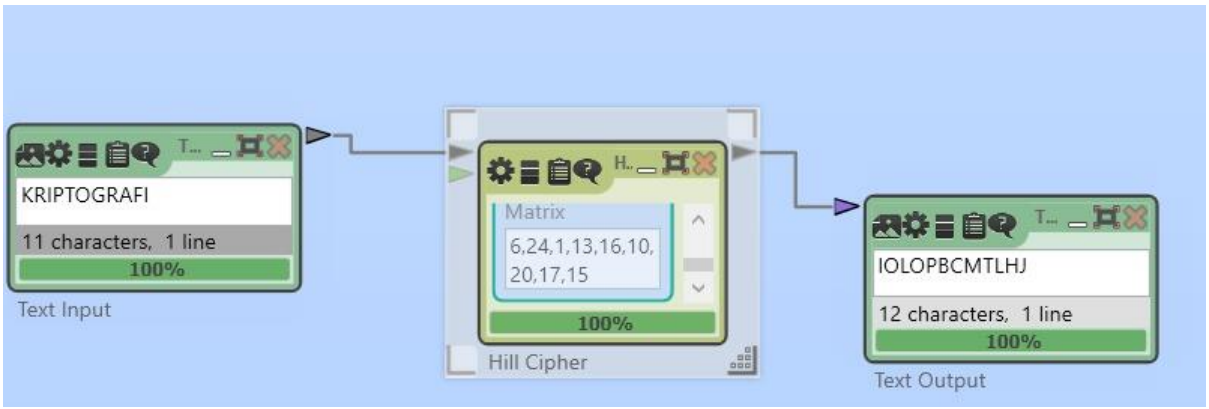

- Affine




- Playfair




- Hill




## 6. Analisis Kelemahan

Setiap algoritma kriptografi klasik memiliki kelemahannya masing-masing yang membuatnya tidak lagi aman digunakan di era modern. Caesar Cipher tergolong paling sederhana dan mudah dipecahkan, karena hanya memiliki 25 kemungkinan kunci sehingga dapat dibobol dengan teknik brute-force atau analisis frekuensi huruf. Vigenere Cipher memang lebih kuat dibanding Caesar karena menggunakan kata kunci berulang, namun tetap lemah terhadap serangan Kasiski examination dan frequency analysis terutama jika panjang kunci relatif pendek. Affine Cipher juga mudah diserang karena sifatnya yang linear; apabila penyerang mengetahui dua pasangan plaintext dan ciphertext, maka nilai kunci dapat dihitung dengan mudah.

Selanjutnya, Playfair Cipher memiliki pola pengacakan huruf yang kurang kuat karena mengenkripsi pasangan huruf (digram) tanpa benar-benar menyembunyikan frekuensi kemunculan pasangan tersebut, sehingga masih rentan terhadap analisis statistik. Terakhir, Hill Cipher memberikan konsep enkripsi berbasis matriks yang menarik, namun algoritma ini

sangat bergantung pada kunci yang invertible (memiliki invers modulo 26). Jika matriks kunci tidak memenuhi syarat tersebut, proses dekripsi akan gagal sepenuhnya.

Secara keseluruhan, kelima algoritma ini berfungsi baik untuk memahami dasar-dasar kriptografi, tetapi memiliki kelemahan mendasar terhadap serangan kriptanalisis modern yang membuatnya tidak cocok digunakan untuk sistem keamanan digital masa kini.

## 7. Kesimpulan

Implementasi lima algoritma kriptografi klasik menunjukkan bahwa meskipun metode ini efektif untuk memahami dasar kriptografi, semuanya memiliki kelemahan signifikan terhadap serangan modern. Namun, prinsip-prinsip yang digunakan menjadi dasar penting bagi algoritma kriptografi modern yang lebih kompleks.

## 8. Link GitHub

- **https://github.com/sailullah/Praktikum-Cipher/blob/main/Praktikum_Cipher_-_Adkia_Ihsan.ipynb**
- **https://github.com/IhsanTafaquh-coder-dev/Praktikum-Cipher/blob/08aefd47bba851e71287c2cc777814503cfa8e55/Praktikum_Cipher.ipynb**