

Nama : Ikhsan Fadilah
NIM : 20123069
Kelompok : 16

1. Teori

a. Caesar cipher

Caesar cipher menyandikan teks dengan mengganti setiap huruf dengan huruf lain yang bergeser tetap dalam alfabet. Prosesnya sederhana: $c = p + k \pmod{26}$, dengan k sebagai kunci. Kelemahannya jelas karena pola huruf bahasa asli tetap terlihat meskipun hurufnya bergeser, sehingga analisis frekuensi mudah membobolnya.

b. Vigenère cipher

Vigenère memperluas Caesar dengan kunci berulang yang panjangnya lebih dari satu huruf. Setiap huruf plaintext dienkripsi dengan pergeseran sesuai huruf kunci yang bersesuaian. Kelemahannya muncul jika panjang kunci relatif pendek sehingga pola kunci terulang, memudahkan serangan frekuensi berskala lebih luas.

c. Affine cipher

Affine cipher menggunakan pemetaan linier $c = a p + b \pmod{26}$ dengan syarat $\gcd(a, 26) = 1$ agar dekripsi possible. Ini memberi pemetaan huruf yang lebih kompleks daripada pergeseran tunggal, tetapi tetap bersifat linear, sehingga bisa diserang secara matematis jika data cukup banyak.

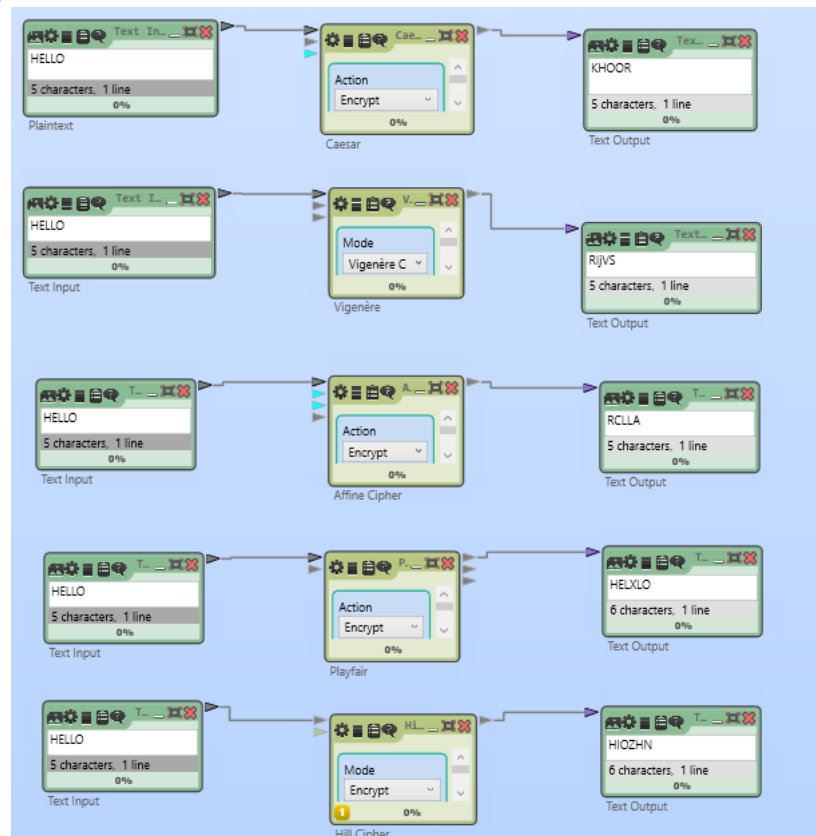
d. Playfair cipher

Playfair menggunakan tabel 5x5 sebagai basis enkripsi pasangan huruf. Enkripsi dilakukan pada pasangan huruf teks dengan aturan berbasis posisi dalam tabel; pola pasangan yang berubah-ubah membuatnya lebih kuat daripada substitusi sederhana, tetapi tetap rentan terhadap analisis pola bila data cukup banyak.

e. Hill cipher

Hill cipher menggunakan aljabar linear: blok huruf dipetakan ke vektor kolom lalu dikalikan dengan matriks kunci $n \times n \pmod{26}$. Dekripsi memerlukan invers matriks kunci modulo 26. Pemilihan kunci yang invertibel sangat penting; jika tidak tepat, keamanan hilang dan serangan matriks bisa berhasil.

2. Output



3. Analisis Kelemahan

a. Caesar Cipher

- Ruang kunci sangat terbatas, hanya 25 kemungkinan, sehingga mudah dipecahkan dengan brute force atau mencoba semua kunci secara manual.
- Cipher ini sangat rentan terhadap analisis frekuensi huruf, karena pola kemunculan huruf dalam ciphertext tetap mencerminkan pola asli bahasa.

b. Vigenère Cipher

- Jika panjang kunci lebih pendek dari pesan, pola kunci akan berulang, sehingga cipher rentan terhadap serangan Kasiski atau analisis indeks koincidensi.
- Cipher ini tetap dapat dipecahkan dengan teknik kriptanalisis lanjutan jika volume data ciphertext cukup besar dan kuncinya tidak cukup acak.

c. Affine Cipher

- Sifat pemetaan linear ($c = ap + b \bmod 26$) menyebabkan pola hubungan huruf tetap ada, sehingga analisis matematis dapat membongkar kunci dari ciphertext yang cukup banyak.
- Jumlah ruang kunci affine cipher tetap relatif terbatas, sehingga cipher ini masih rentan terhadap serangan brute force dan serangan substitusi mono-alfabet.

d. Playfair Cipher

- Cipher tetap mempertahankan sebagian besar pola bahasa, hanya mengacak huruf dalam blok dua, membuatnya masih rentan terhadap analisis pasangan huruf (digrams/ bigrams).
- Jika tabel kunci diketahui atau dapat ditebak, cipher dapat dipecahkan dengan frekuensi atau pola kombinasi pasangan huruf.

e. Hill Cipher

- Jika matriks kunci yang dipilih tidak cukup acak atau memiliki ukuran blok kecil, cipher mudah dipecahkan dengan analisis linear menggunakan persamaan matriks.
- Keamanan sangat bergantung pada keberadaan invers matriks modulo 26; jika matriks tidak invertibel, dekripsi tidak bisa dilakukan dan cipher gagal digunakan dengan benar.