Nama : Farhan Nur Aziz Bisri
NPM : 20123071
Kelompok : 15
KRIPTOGRAFI

1. PENDAHULUAN

Kriptografi klasik adalah metode penyandian informasi yang digunakan sebelum era komputer, dengan tujuan melindungi pesan melalui teknik manual seperti substitusi (mengganti huruf) dan transposisi (mengubah urutan huruf). Kriptografi berperan sebagai fondasi dasar bagi kriptografi modern dan untuk memahami konsep awal pengamanan informasi menggunakan sistem simetris. Kriptografi klasik merupakan dasar dari perkembangan sistem keamanan informasi modern. Algoritma-algoritma klasik seperti Caesar, Vigenere, Affine, Playfair, dan Hill Cipher merupakan bentuk awal enkripsi yang digunakan sebelum era komputer modern. *CrypTool 2* adalah aplikasi *open-source* edukatif dari Jerman yang memungkinkan penggunanya melihat secara visual bagaimana proses enkripsi dan dekripsi bekerja, mau cipher klasik ataupun modern.

Tujuan praktikum ini adalah untuk memahami prinsip kerja algoritma kriptografi klasik dengan mengimplementasikannya secara manual menggunakan Pyhton, serta memverifikasi hasilnya menggunakan CrypTool 2 sebagai alat bantu visualisasi.

2. IMPLEMENTASI ALGORITMA

Kelima algoritma diimplementasikan menggunakan Python tanpa *libary* kripto eksternal, program berisi fungsi *encrypt()*. Kode dijalankan dengan plaintext "HELLO" dan hasil dibandingkan dengan *CrypTool* 2.

Hasil Percobaan :

Algoritma	Parameter	Nilai
Caesar Cipher	Plaintext	HELLO
	Key	3
	Ciphertext (Python)	KHOOR
	Ciphertext (CrypTool 2)	KHOOR
Vigenere Cipher	Plaintext	HELLO
	Key	KEY
	Ciphertext (Python)	RUVS
	Ciphertext (CrypTool 2)	RUVS
Affine Cipher	Plaintext	HELLO
	Key	5,8
	Ciphertext (Python)	RCLLA
	Ciphertext (CrypTool 2)	RCLLA
Playfair Cipher	Plaintext	HELLO
	Key	KEYWORD
	Ciphertext (Python)	GYIZSC
	Ciphertext (CrypTool 2)	HELXLO
Hill Cipher	Plaintext	HELLO

	Key	[[3,3],[2,5]
	Ciphertext (Python)	HIOZHN
	Ciphertext (CrypTool 2)	HIOZHN

Dari hasil percbaan, terlihat bahwa cipher klasik berhasil dijalankan dengan hasil identik antara Python dan *CrypTool* 2 (kecuali Playfair Cipher). Namun dari sisi keamanan, algoritma klasik sangat lemah terhadap analisis frekuensi dan brute-force karena ruang kuncinya kecil dan pola statistik plaintext masih tampak pada ciphertext. *CrypTool* 2 membantu memahami proses enkripsi dengan jelas melalui visualisasi langkah-langkahnya dan mempermudah validasi hasil coding manual.

3. ANALISIS KELEMAHAN

Algoritma	Kelebihan	Kelemahan	Jenis Serangan
Caesar	Sederhana dan mudah diimplementasikan	Ruang kunci kecil (25 kemungkinan)	Brute-force, Frequency Analysis
Vigenere	Lebih aman dari Caesar (pakai kunci huruf)	Mudah dipecahkan jika kunci pendek	Kasiski, Friedman Test
Affine	Kombinasi operasi linier	Rentan jika diketahui pasangan plaintext–ciphertext	Known-Plaintext Attack
Playfair	Menggunakan pasangan huruf (lebih kompleks)	Masih bisa diserang statistik (analisis digraph)	Frequency Analysis on Digraphs
Hill	Menggunakan aljabar linear	Kunci tidak selalu invertible mod 26, dan mudah diserang jika banyak data diketahui	Known-Plaintext Attack

Lima Algoritma Klasik (Caesar, Vigenere, Affine, Playfair, Hill) berhasil diimplementasikam menggunakan Python dan diverifikasi menggunakan *CrypTool* 2. Semua hasil enkripsi sesuai antara kedua platform kecuali Playfair Cepher. Meskipun menarik secara historis, cipher klasik tidak aman digunakan pada sistem modern karena mudah dipecahkan.