TUGAS SESI 13
NAMA : INDAH PUSPITASARI
KELAS : TI 22 H
NIM : 20220040095
MATKUL : Algoritma dan Struktur data

Sebutkan 3 buah Enkripsi klasik dan 1 buah enkripsi modern berikut implementasinya

JAWABAN

- **Enkripsi klasik**

1. Caesar chiper

Caesar chiper adalah metode enkripsi substitusi yang menggunakan pergeseran karakter dalam abjad. Setiap huruf dalam teks asli digantikan dengan huruf lain yang berjarak beberapa posisi di abjad. Misalkan kita menggunakan pergeseran tiga posisi. Kata "HELLO" akan dienkripsi menjadi "KHOOR" dalam sandi Caesar dengan pergeseran tiga abjad.

2. Vigenere chiper:

Vigenere chipper adalah metode enkripsi substitusi yang menggunakan tabel Vigenere. Tabel ini terdiri dari beberapa baris alfabet yang digeser secara bertahap. Enkripsi dilakukan dengan menggabungkan pergeseran alfabet berdasarkan huruf kunci yang diulang dalam teks yang ingin dienkripsi. Misalkan kita ingin mengenkripsi kata "HELLO" dengan kata kunci "KEY". Menggunakan tabel Vigenere, kita mencocokkan huruf "H" dengan huruf kunci pertama "K" untuk mendapatkan huruf "R", huruf "E" dengan huruf kunci kedua "E" untuk mendapatkan huruf "J", dan seterusnya. Hasil enkripsi adalah "RJSSF".

3. Hill chiper:

Hill chiper menggunakan operasi matematika pada blok huruf dalam teks. Teks asli dibagi menjadi blok-blok huruf, dan setiap blok diubah menggunakan perkalian matriks. Setiap matriks kunci digunakan untuk mengenkripsi blok huruf. Misalkan kita ingin mengenkripsi blok huruf "HEL" dengan matriks kunci 2x2 [2, 3; 1, 4]. Setiap blok huruf diubah menjadi vektor kolom [7, 4]. Dalam operasi perkalian matriks, hasilnya adalah [2*7 + 3*4, 1*7 + 4*4], yang menjadi [29, 15]. Hasil enkripsi adalah vektor kolom [29, 15], yang dapat dikonversi kembali menjadi huruf atau simbol sesuai dengan konvensi yang digunakan.

- **Enkripsi modern**

1) Advanced Encryption Standard (AES):
   AES adalah salah satu algoritma enkripsi simetris yang paling banyak digunakan di seluruh dunia. Algoritma ini memiliki tiga varian, yaitu AES-128, AES-192, dan AES-256, yangmasing-masing menggunakan kunci dengan panjang yang berbeda. AES telah diadopsi oleh pemerintah AS sebagai standar enkripsi untuk data yang sensitif. Implementasinya dapat ditemukan dalam berbagai aplikasi dan protokol, seperti enkripsi data pada penyimpanan dan transfer file, protokol HTTPS, dan keamanan jaringan.

2) Rivest-Shamir-Adleman (RSA): teknik enkripsi kunci publik yang menggunakan pasangan kunci publik dan kunci privat untuk mengenkripsi dan mendekripsi pesan. Kunci publik digunakan untuk mengenkripsi pesan, sedangkan kunci privat digunakan untuk mendekripsi pesan. Contoh implementasinya adalah penggunaan RSA pada protokol SSL/TLS untuk melindungi data saat berkomunikasi di internet