Tugas Algoritma dan Struktur Data

Sebutkan 3 buah Enkripsi klasik dan 1 buah enkripsi modern berikut implementasinya pada JAVA!

1. Sandi Caesar:

Enkripsi Caesar adalah salah satu teknik enkripsi klasik yang paling sederhana. Sandi ini bekerja dengan mengganti setiap huruf pada teks asli dengan huruf yang terletak beberapa posisi di depannya dalam alfabet. Misalnya, dengan pergeseran tiga posisi, huruf A akan menjadi D, huruf B menjadi E, dan seterusnya. Enkripsi ini menggunakan kunci pergeseran yang sama untuk seluruh teks.

Contoh:

Teks asli: HELLO

Kunci pergeseran: 3

Teks terenkripsi: KHOOR

2. Sandi Vigenere:

Sandi Vigenere menggunakan kunci yang terdiri dari serangkaian huruf untuk mengenkripsi teks. Setiap huruf kunci digunakan untuk melakukan pergeseran Caesar pada huruf-huruf yang sesuai dalam teks asli. Kunci akan diulang secara terus-menerus hingga mencapai panjang teks yang akan dienkripsi.

Contoh:

Teks asli: HELLO

Kunci: KEY

Teks terenkripsi: RIJVS

3. Sandi Substitusi:

Sandi substitusi melibatkan penggantian setiap huruf pada teks asli dengan huruf atau simbol lain yang telah ditentukan sebelumnya. Pada sandi substitusi tunggal, setiap huruf memiliki penggantinya sendiri. Pada sandi substitusi polyalphabetic, setiap huruf dapat memiliki beberapa penggantinya yang berbeda, tergantung pada posisinya dalam kata atau teks.

Contoh:

Teks asli: HELLO

Teks terenkripsi: SVRRG

4. Advanced Encryption Standard (AES):

AES adalah algoritma enkripsi simetris yang digunakan secara luas. Algoritma ini menerapkan operasi penggantian (substitusi), pergeseran (shift), dan pemisahan bit (xor) untuk mengenkripsi data. AES memiliki beberapa variasi kunci, termasuk AES-128, AES-192, dan AES-256, yang masing-masing mengacu pada panjang kunci yang digunakan (128 bit, 192 bit, dan 256 bit). Contoh penggunaan AES adalah dalam enkripsi data pada protokol HTTPS.