Algoritma dan struktur data

Nama : Nurazizah Zahra

NIM : 20220040089

Kelas : TI22 H

- **Enkripsi klasik**
  Berikut adalah tiga contoh enkripsi klasik beserta implementasinya secara singkat:

  - Substitusi Caesar:

  Enkripsi substitusi Caesar adalah metode enkripsi klasik yang menggunakan pergeseran huruf. Setiap huruf dalam pesan digantikan dengan huruf yang diperoleh dengan melakukan pergeseran sejumlah langkah tertentu dalam urutan abjad. Misalnya, dengan pergeseran tiga langkah, huruf A akan menjadi D, huruf B akan menjadi E, dan seterusnya. Implementasinya dapat dilakukan dengan menggunakan aturan pergeseran dan menerapkan perubahan pada setiap karakter dalam pesan.

  Contoh implementasi:

  Pesan: HELLO
  Pergeseran: 3
  Pesan Terenkripsi: KHOOR

  - Atbash:

  Enkripsi Atbash adalah metode enkripsi klasik yang menggunakan substitusi huruf dengan aturan yang sederhana. Setiap huruf dalam pesan digantikan dengan huruf yang berada pada posisi yang berlawanan di dalam urutan abjad. Misalnya, huruf A akan menjadi Z, huruf B akan menjadi Y, dan seterusnya. Implementasinya dapat dilakukan dengan membuat peta penggantian huruf dan menggantikan setiap huruf dalam pesan dengan huruf yang sesuai dalam peta tersebut.

  Contoh implementasi:

  Pesan: HELLO
  Pesan Terenkripsi: SVOOL

  - Rail Fence:

  Enkripsi Rail Fence adalah metode enkripsi klasik yang mengatur huruf-huruf pesan dalam pola gelombang. Huruf-huruf pesan ditulis dalam pola zigzag pada beberapa "rail" atau garis paralel. Kemudian huruf-huruf tersebut dikumpulkan secara berurutan untuk membentuk pesan terenkripsi. Implementasinya melibatkan pembuatan pola zigzag dan mengumpulkan huruf-huruf dalam urutan yang tepat.

Contoh implementasi:

Pesan: HELLO WORLD
Jumlah Rail: 3
Pesan Terenkripsi: HOLELWRDLL O

- **enkripsi modern**

implementasinya adalah Advanced Encryption Standard (AES). AES adalah salah satu algoritma enkripsi blok yang digunakan secara luas saat ini. Ini menggunakan kunci simetris untuk mengenkripsi dan mendekripsi data.

Implementasi AES melibatkan beberapa tahap utama:

- Inisialisasi: Mengambil data input (blok) dan kunci enkripsi yang telah ditentukan.
- SubBytes: Setiap byte dalam blok di-substitusikan dengan byte baru menggunakan tabel substitusi (S-Box).
- ShiftRows: Melakukan pergeseran baris pada blok, di mana byte dalam setiap baris digeser ke kiri dengan jumlah yang sesuai.
- MixColumns: Melakukan operasi linier pada kolom-kolom blok menggunakan matriks yang telah ditentukan.
- AddRoundKey: Setiap byte dalam blok di-XOR-kan dengan byte kunci ronde yang sesuai.

Langkah-langkah ini dilakukan dalam serangkaian ronde, dan setiap ronde melibatkan penggunaan kunci ronde yang dihasilkan dari kunci enkripsi awal.

Implementasi AES sebenarnya melibatkan operasi bit-level yang kompleks, tetapi pseudocode di atas memberikan gambaran umum tentang alur enkripsi AES. Implementasi nyata dari AES umumnya menggunakan bahasa pemrograman dan menerapkan operasi-operasi bit-level sesuai dengan spesifikasi algoritma AES.