Penjelasan Kode dan Algoritma DES

Proses enkripsi dan dekripsi dalam kode yang telah Anda berikan terkait dengan algoritma kriptografi DES (Data Encryption Standard) yang menggunakan permutasi dan jaringan penggantian-permutasi (substitution-permutation network). Berikut adalah penjelasan singkat tentang proses enkripsi (encryption) dan dekripsi (decryption) yang terjadi dalam kode tersebut:

**Proses Enkripsi (Encryption):**

1. **Input Pesan**: Pesan asli yang ingin dienkripsi (plaintext) diwakili dalam bentuk biner (0 dan 1) dan dipecah menjadi dua bagian, yaitu bagian kiri (left) dan bagian kanan (right).
2. **Subkunci (Subkeys) dan Permutasi Awal (Initial Permutation)**: Proses dimulai dengan menghasilkan kunci enkripsi (subkeys) dari kunci rahasia yang telah diberikan. Kunci ini disusun dan diubah bentuk dengan menggunakan tabel permutasi tertentu (misalnya, PC1 dan PC2) untuk menghasilkan subkunci yang akan digunakan dalam setiap putaran.
3. **16 Putaran Feistel**: Proses enkripsi DES terdiri dari 16 putaran Feistel yang saling terkait. Setiap putaran terdiri dari langkah-langkah berikut:
   * **Penggantian Eksklusif (XOR)**: Bagian kanan pesan (right) digabungkan dengan hasil fungsi F yang menggunakan subkunci khusus untuk putaran tersebut.
   * **Fungsi F**: Fungsi ini melibatkan permutasi lain, yaitu pemilihan bit khusus dari bagian kanan pesan dan permutasi dengan tabel yang telah didefinisikan (E-Bit Selection Table). Selanjutnya, data dipecah menjadi 6-bit blok dan melewati kotak penggantian (S-Box) yang menggantikan nilai-nilai ini dengan nilai-nilai lain.
   * **Permutasi P**: Hasil dari fungsi F diubah kembali dengan menggunakan tabel permutasi (P-Table) untuk menghasilkan permutasi baru.
   * **Pertukaran**: Bagian kanan pesan sebelumnya menjadi bagian kiri pesan yang baru, dan bagian kiri pesan sebelumnya digabungkan dengan hasil permutasi F dan XOR dengan bagian kanan pesan sebelumnya.
4. **Pertukaran Akhir dan Permutasi Akhir (Final Permutation)**: Setelah 16 putaran Feistel, bagian kiri dan kanan pesan ditukar, dan hasil dari putaran terakhir dipersempit dengan menggunakan tabel permutasi akhir (Reverse IP Table).
5. **Output Pesan Terenkripsi**: Hasil akhir dari proses enkripsi adalah pesan terenkripsi dalam bentuk biner. Pesan ini kemudian dapat dikonversi kembali menjadi format heksadesimal atau format lainnya sesuai kebutuhan.

**Proses Dekripsi (Decryption):**

1. **Input Pesan Terenkripsi**: Pesan terenkripsi (ciphertext) dalam bentuk biner adalah input ke proses dekripsi.
2. **Subkunci (Subkeys) dan Permutasi Awal (Initial Permutation)**: Seperti dalam proses enkripsi, subkunci yang sama digunakan dalam urutan terbalik, dan permutasi awal juga dilakukan.
3. **16 Putaran Feistel Terbalik**: Proses dekripsi DES melibatkan 16 putaran Feistel yang terbalik dibandingkan dengan proses enkripsi. Ini berarti subkunci digunakan dalam urutan terbalik.
4. **Pertukaran Akhir dan Permutasi Akhir (Final Permutation)**: Setelah 16 putaran Feistel terbalik, bagian kiri dan kanan pesan terbalik dibandingkan dengan proses enkripsi. Hasil akhirnya adalah pesan dekripsi dalam bentuk biner.
5. **Output Pesan Asli**: Pesan dekripsi dalam bentuk biner dapat dikonversi kembali menjadi pesan asli dalam format yang sesuai, seperti teks biasa.

Kunci utama dalam DES adalah penggantian, permutasi, dan perpindahan bit secara terstruktur yang terjadi selama proses enkripsi dan dekripsi. Semua ini dirancang untuk menghasilkan tingkat keamanan yang tinggi dan membuat serangan terhadap pesan terenkripsi menjadi sangat sulit tanpa pengetahuan kunci rahasia.

Feistel adalah suatu struktur yang digunakan dalam desain berbagai algoritma kriptografi, terutama dalam konteks kriptografi simetris seperti DES (Data Encryption Standard) dan beberapa algoritma lainnya. Struktur Feistel membagi data masukan (biasanya pesan yang akan dienkripsi) menjadi dua bagian yang disebut "bagian kiri" dan "bagian kanan," lalu melakukan serangkaian putaran pada kedua bagian tersebut dengan menggunakan fungsi kunci.

Ciri-ciri utama dari struktur Feistel adalah sebagai berikut:

1. **Pemisahan Data**: Data masukan dibagi menjadi dua bagian yang sama panjang, yaitu bagian kiri dan bagian kanan.
2. **Putaran Berulang**: Struktur Feistel melibatkan serangkaian putaran yang diulang beberapa kali. Biasanya, ada 16 putaran dalam DES.
3. **Operasi XOR**: Pada setiap putaran, bagian kanan data di-XOR-kan dengan hasil dari fungsi yang menggunakan bagian kanan sebagai masukan dan kunci putaran sebagai kunci.
4. **Swap Bagian**: Setelah setiap putaran, bagian kiri dan bagian kanan data dibalik atau ditukar. Bagian kanan sebelumnya menjadi bagian kiri baru, dan bagian kiri sebelumnya di-XOR-kan dengan hasil operasi di atas menjadi bagian kanan baru.
5. **Fungsi Kunci**: Sebuah fungsi kunci digunakan untuk menghasilkan kunci yang berbeda pada setiap putaran. Kunci ini bergantung pada kunci utama algoritma kriptografi.
6. **Kemampuan Dekripsi**: Salah satu keunggulan struktur Feistel adalah kemampuannya untuk digunakan dalam proses enkripsi dan dekripsi yang sama dengan mengubah urutan kunci.

Algoritma DES, yang dijelaskan dalam kode yang Anda berikan sebelumnya, adalah salah satu contoh algoritma kriptografi yang menggunakan struktur Feistel. Struktur ini membantu meningkatkan keamanan data dengan melakukan serangkaian operasi permutasi, substitusi, dan transformasi pada data masukan, yang membuatnya sulit untuk dipecahkan tanpa kunci yang benar.

Top of Form