**Modul 9**

1. **Tujuan**

1. Mampu menjelaskan definisi dan konsep Data Encryption Standard (DES)

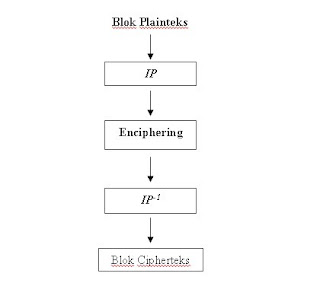
2. Mampu memahami konsep dasar Data Encryption Standard (DES)

1. **Dasar teori**
2. **Data Encryption Standard**

DES merupakan salah satu algoritma kriptografi cipher block dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. Algoritma DES dibuat di IBM, dan merupakan modifikasi daripada algoritma terdahulu yang bernama Lucifer. Lucifer merupakan algoritma cipher block yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 28 bit. Pengurangan jumlah bit kunci pada DES dilakukan dengan alasan agar mekanisme algoritma ini bisa diimplementasikan dalam satu chip.

DES pertama kali dipublikasikan di Federal Register pada 17 Maret 1975. Setelah melalui banyak diskusi, akhirnya algortima DES diadopsi sebagai algoritma standar yang digunakan oleh NBS (National Bureau of Standards) pada 15 Januari 1977. Sejak saat itu, DES banyak digunakan pada dunia penyebaran informasi untuk melindungi data agar tidak bisa dibaca oleh orang lain.

1. **Algoritma DES**
2. **Enkripsi**



Penjelasan :

1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).

2. Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kaH (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.

Secara umum, algoritma DES terbagi menjadi 3 kelompok di mana kelompok yang satu dengan yang lain saling berinteraksi dan terkait antara satu dengan yang lain. Kelompok-kelompok tersebut adalah : Pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit.

Algoritma DES dirancang untuk menulis dan membaca berita blok data yang terdiri dari 64 bit di bawah kontrol kunci 64 bit. Dalam pembacaan berita harus dikerjakan dengan menggunakan kunci yang sama dengan waktu menulis berita, dengan penjadualan alamat kunci bit yang diubah sehingga proses membaca adalah kebalikan dari proses menulis.

Sebuah blok ditulis dan ditujukan pada permutasi dengan inisial IP, kemudian melewati perhitungan dan perhitungan tersebut sangat tergantung pada kunci kompleks dan pada akhirnya melewati permutasi yang invers dari permutasi dengan inisial IP-1.

Perhitungan yang tergantung pada kunci tersebut dapat didefinisikan sebagai fungsi f, yang disebut fungsi cipher dan fungsi KS, yang disebut Key Schedule.

Sebuah dekripsi perhitungan diberikan pada awal, sepanjang algoritma yang digunakan dalam penulisan pesan. Berikutnya, penggunaan algoritma untuk 3 pembacaan pesan didekripsikan. Akhirnya, definisi dari fungsi cipher f menjadi fungsi seleksi Si dan fungsi permutasi adalah P.

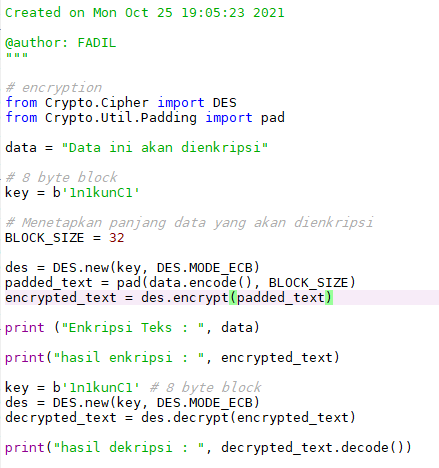
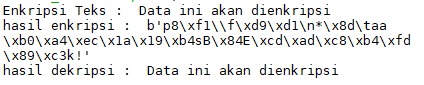
1. **Keamanan**

Algoritma DES mengundang banyak kontroversi dari para ahli di seluruh dunia. Salah satu kontroversi tersebut adalah S-Box yang digunakan pada DES. S-Box merupakan bagian vital dari DES karena merupakan bagian yang paling sulit dipecahkan. Hal ini disebabkan karena S-Box merupakan satu – satunya bagian dari DES yang komputasinya tidak linear. Sementara itu, rancangan dari S-Box sendiri tidak diberitahukan kepada publik. Karena itulah, banyak yang curiga bahwa S-Box dirancang sedemikian rupa sehingga memberikan trapdoor kepada NSA agar NSA bisa membongkar semua ciphertext yang dienkripsi dengan DES kapan saja.



Kontroversi yang kedua adalah jumlah bit pada kunci DES yang dianggap terlalu kecil, hanya 56 bit. Akibatnya DES rawan terhadap serangan brute force. Walaupun terdapat kerawanan tersebut, DES tetap digunakan pada banyak aplikasi seperti pada enkripsi PIN (Personal Identification Numbers) pada mesin ATM (Automatic Teller Machine) dan transaksi perbankan lewat internet. Bahkan, organisasi – organisasi pemerintahan di Amerika seperti Department of Energy, Justice Department, dan Federal Reserve System menggunakan DES untuk melindungi penyebaran data mereka.

**D. Contoh Program Python**

**E. TUGAS Kelompok**

1. Mencari dua jurnal yang berkaitan dengan algoritma Data Encrytion Standard (DES). Jurnal tiap kelompok tidak boleh sama.

2. Buatlah resume berdasarkan jurnal-jurnal tersebut dengan bahasa mu sendiri. Resume jurnal harus memuat poin-poin berikut :

a. Judul dan Latar Belakang Masalah

b. Tujuan Penelitian

c. Algoritma yang dipakai beserta alur penelitiannya

d. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

3. Kerjakan tugas diatas pada Ms. Word. Tuliskan nama kelompok dan anggota masing-masing

3. Pengumpulan Tugas Praktikum

* **Upload file word** ke SPADA
* **Untuk kelas TI E** paling lambat tanggal 1 November 2021 Jam 23.59

**Untuk kelas TI D** paling lambat tanggal 2 November 2021 Jam 23.59

* Format penamaan file SKD\_namakelas\_nim\_nama