**Tugas 1 – Enkripsi DES menggunakan metode OBF**

*KIJ F Kelompok F12 :*

* *Farhan Ramadhana 5114100078*
* *Shafly Nauval Adiant 5114100114*

**Pendahuluan**

Penggunaan teknologi informasi dan telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkumunikasi. Pada saat ini pertukaran informasi sering sekali melibatkan penggunaan internet. Namun dengan demikian perlu diperhatikan tingkat keamanan informasi tersebut, karena pada saat ini penggunaan jaringan internet yang merupakan infrastuktur telekomunikasi dengan standar terbuka yang dapat dipergunakan oleh banyak pihak. Penyadapan informasi merupakan hal yang sangat merugikan bagi pengguna jaringan komunikasi saat ini.

Pada tugas kali ini adalah membuat sebuah program yang dapat mengekripsi dan dekripsi data dengan DES (*data encryption standart*) dengan menggunakan metode OFB (*Output Feedback*).

**Dasar Teori**

***Keamanan jaringan***

Dalam jaringan computer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Keamanan jaringan suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

***Kriptografi***

Kriptografi merupakan salah satu teknik yang dapat meningkatkan keamanan informasi antara lain otentikasi dan kerahasiaan. Untuk menjaga kerahasiaan adalah dengan menjaga agar pesan tidak dapat dibaca oleh pihak yang tidak berhak yaitu melalui proses enkripsi dan dekripsi.

***Enkripsi dan Dekripsi***

Proses enkripsi yaitu mengubah pesan asli (*plaintext)* menjadi pesan dalam bentuk tersandi (*ciphertext*). Proses enkripsi akan menghasilkan data tersandi dan hanya dapat dibuka atau dibaca oleh pihak penerima yang memiliki kunci (*key*) sedangkan proses dekripsi adalah mengembalikan data tersandi menjadi bentuk asli.

***DES (Data Encryption Standart)***

DES merupakan algoritma enkripsi yang dikembangkan oleh NIST (National Institute of Standards and Technology) sebagai standar pengolahan informasi Federal AS. Secara umum, Data Encryption Standard (DES) terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit dan deskripsi data 64 bit, dimana satu kelompok saling berinteraksi satu dengan yang lainnya. Data dienkripsi dalam blok-blok 64 bit menggunakan kunci 56 bit, DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk lama block cipher dengan tahapan pemakaian kunci yang sama untuk deskripsinya.

***OFB* (*Output Feedback*)**

Mode *OFB* mirip dengan mode *CFB,* kecuali n-bit dari hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan di antrian. Dekripsi dilakukan sebagai kebalikan dari proses enkripsi.

