Konsep Enkripsi dan Dekripsi Berdasarkan Kunci Simetris

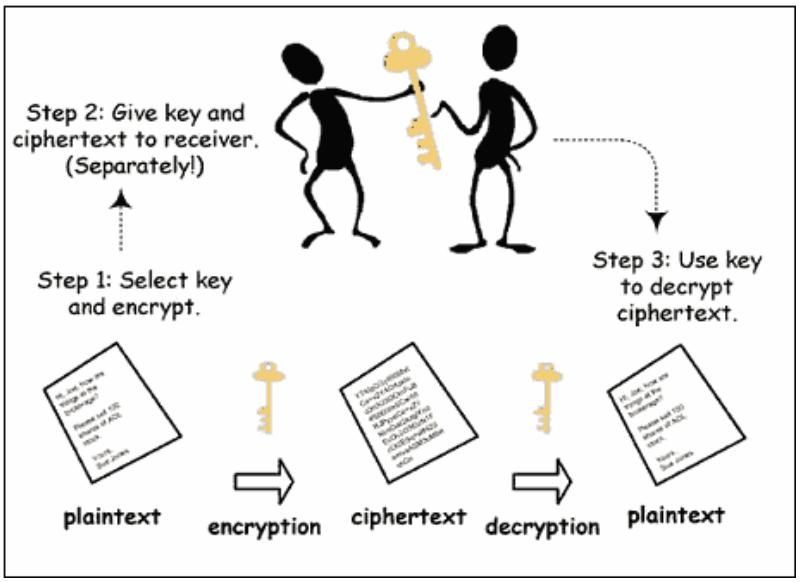
Oleh: Benfano Soewito

Setelah internet dikenal oleh sebagian besar pengguna, maka transfer data, pengiriman informasi, dan cara berbisnis telah berubah. Hampir semua kegiatan kita sehari hari tidak terlepas dari internet. Seiring dengan banyaknya applikasi di internet, maka bertambah pula pengguna internet. Aplikasi aplikasi yang menggunakan internet ini, semua bertujuan untuk lebih mempermudah semua kegiatan kita, baik itu untuk pendidikan, kegiatan bisnis, social, dan sebagainya. Oleh karena itu data atau informasi yang dulunya disimpan dalam media kertas atau media lainnya, sekarang data dan informasi tersebut lebih banyak disimpan dalam bentuk digital. Tujuannya adalah agar mudah dikirim melalui internet. Tetapi seiring dengan banyaknya aplikasi, pengguna internet, dan data digital, maka makin banyak juga celah celah yang terbuka bagi orang orang yang ingin berbuat jahat. Oleh karena itu faktor keamanan menjadi suatu hal yang serius dalam semua applikasi yang ada di internet, terutama aplikasi aplikasi yang berhubungan dengan keuangan. Salah satu cara untuk melindungi atau mencegah data kita dibaca oleh orang orang yang tidak bertanggung jawab adalah dengan mengenkrip data tersebut.

Enkripsi adalah suatu proses untuk merubah sebuah pesan, data atau informasi (biasa disebut plaintext), sehingga informasi tersebut tidak dapat dibaca oleh orang yang tidak bertanggung jawab (ciphertext). Jadi plaintext adalah informasi yang dapat dimengerti dan ciphertext adalah informasi yang tidak dapat dimengerti atau dibaca. Enkripsi adalah bagian dari sebuah ilmu yang disebut kriptologi atau kriptografi. Kriptografi adalah sebuah ilmu yang mempelajari teknik untuk membuat sebuah pesan atau informasi tidak dapat dibaca oleh orang yang tidak berhak. Ada dua teknik yang cukup terkenal dalam kriptografi yaitu: symmetric key encryption dan public key encryption.

Dalam symmetric-key encryption, proses enkripsi suatu informasi menggunakan kunci atau kode. Kemudian untuk mengdekrip informasi yang telah di enkrip, diperlukan kunci yang sama. Dekripsi adalah proses kebalikannya yaitu suatu proses untuk mengembalikan informasi yang sudah di enkrip menjadi bisa dibaca kembali. Secara umum juga proses enkripsi ini dapat digambarkan sebagai berikut:

Plaintext > Algoritma Enkripsi > Ciphertext >Algoritma Dekripsi > Plaintext



Informasi asal yang dapat di mengerti di simbolkan oleh Plain teks, yang kemudian oleh algoritma Enkripsi diterjemahkan menjadi informasi yang tidak dapat untuk dimengerti yang disimbolkan dengan cipher teks. Proses enkripsi terdiri dari dua yaitu algoritma dan kunci. Kunci biasanya merupakan suatu string bit yang pendek yang mengontrol algoritma. Algoritma enkripsi akan menghasilkan hasil yang berbeda tergantung pada kunci yang digunakan. Mengubah kunci dari enkripsi akan mengubah output dari algortima enkripsi. Sekali cipher teks telah dihasilkan, kemudian ditransmisikan. Pada bagian penerima selanjutnya cipher teks yang diterima diubah kembali ke plain teks dengan algoritma dan dan kunci yang sama.

Secara matematis operasi enkripsi dan dekripsi dapat digambarkan sebagai berikut:

$Y = E_K(X)$ or $Y = E(K, X)$

$X = D_K(Y)$ or $X = D(K, Y)$

- X = plaintext
- Y = ciphertext
- K = secret key
- E = encryption algorithm
- D = decryption algorithm

Pada proses enkripsi pesan atau informasi *X* dengan suatu kunci *K* disandikan menjadi informasi *Y*. pada proses dekripsi informasi *Y* dengan kunci *K* disandikan menjadi informasi semula yaitu *X*. Dimana pesan *X* adalah plaintext dan *Y* adalah ciphertext.

Keamanan dari enkripsi simetris ini bergantung pada beberapa faktor. Pertama algoritma enkripsi harus cukup kuat sehingga menjadikan sangat sulit untuk mendekripsi cipher teks dengan dasar cipher teks tersebut. Lebih jauh dari itu keamanan dari algoritma enkripsi simetris bergantung pada kerahasian dari kuncinya bukan algoritmanya. Yaitu dengan asumsi bahwa adalah sangat tidak praktis untuk mendekripsikan informasi dengan dasar cipher teks dan pengetahuan tentang algoritma diskripsi / enkripsi. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya. Algoritma enkripsi simetris sangat mudah dalam penggunaan secara luas. Dengan kenyataan bahwa algoritma ini tidak perlu dijaga kerahasiaannya dengan maksud bahwa pembuat dapat dan mampu membuat suatu implementasi dalam bentuk chip atau software.

Pada dasarnya enkripsi simetris ini dapat dibedakan menjadi tiga macam teknik yaitu:

1. Substitusi: dalam kriptografi, substitusi adalah metode enkripsi dimana unit plaintext digantikan dengan ciphertext menurut sistem yang teratur, "unit" tersebut dapat berupa huruf tunggal (yang paling umum), berpasangan, atau campuran di atas, dan sebagainya. Penerima harus mendekrip ciphertext dengan melakukan substitusi terbalik.
2. Transposisi: dalam teknik transposisi, unit-unit dalam plaintext di atur ulang posisinya berbeda dengan awalnya dan biasanya dengan dengan order yang sulit, jumlah unit pada setiap suku kata akan berubah, tetapi jumlah total unit unit tersebut tidak berubah.
3. Campuran: adalah teknik yang menggabungkan kedua teknik tersebut.

Salah satu contoh teknik substitusi yang terkenal dari enkripsi simetris ini adalah Caesar Cipher, juga dikenal Caesar Shift, ini adalah salah satu teknik enkripsi yang paling sederhana dan paling dikenal secara luas. Ini adalah jenis cipher substitusi di mana setiap huruf dalam plaintext digantikan oleh huruf yang lain dalam alphabet secara tetap posisinya. Misalnya, dengan pergeseran ke kiri sebanyak 3, D akan digantikan oleh A, E akan menjadi B, dan seterusnya. Metode ini dinamai Julius Caesar, yang digunakan dalam korespondensi pribadinya.

Salah satu cara untuk menerapkan Caesar Cipher ini adalah dengan menggunakan alat rotasi yang sederhana seperti gambar disamping. Dengan memutar lingkaran bagian dalam (ciphertext) dan menggantikan alphabet yang ada dilingkar luar (plaintext) atau sebaliknya. Contohnya adalah sebagai berikut:

Plaintext: *ATTACK*

Ciphertext: *DWWDFN*

Teknik enkripsi berdasarkan substitusi yang sederhana ini sangat mudah di tebak, misalnya dengan cara menganalisa abjad yang sering muncul pada ciphertext.

Contoh teknik enkripsi yang lebih baik dengan teknik substitusi adalah teknik Vigenere. Teknik ini diperkenalkan oleh Blaise de Vigenere pada abad ke 16 dan telah menjadi sebuah teknik yang cukup baik serta sudah digunakan selama 300 tahun. Contoh penggunaan teknik ini adalah sebagai berikut: misal kunci adalah BIRU. Kemudian konversi BIRU berdasarkan shift atau rotasi menjadi 1-8-17-20. Gunakan kunci ini berulang ulang sesuai dengan jumlah huruf yang akan di enkrip 1-8-17-20-1-8-17-20-1-8 …. dan seterusnya.

Contoh: Plaintext: ATTACK

Kunci: BIRU (1-8-17-20)

Ciphertext: BBKUDS