**BAB II**

**DASAR TEORI**

* 1. **Kriptografi**

Ilmu kriptografi adalah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dari penyandian pesan asli menjadi pesan yang tidak dapat diartikan seperti aslinya. Dekripsi sendiri berarti merubah pesan yang sudah disandikan menjadi pesan aslinya. Pesan asli biasanya disebut plaintext, sedangkan pesan yang sudah disandikan disebut ciphertext .

Kriptografi (cryptography) berasal dari bahasa Yunani ”cryptos” artinya ”secret” (rahasia), sedangkan ”graphein” artinya ”writing” (tulisan). Jadi kriptografi berarti ”secret writing” (tulisan rahasia).

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Bruce Schneier, 1996). Dalam kriptografi sering ditemukan istilah atau terminologi, seperti pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (plaintext) atau teks jelas (cleartext). Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran telekomunikasi, dsb) atau yang disimpan di dalam media perekaman (kertas, storage, dsb). Pesan yang tersimpan tidak hanya berupa teks, tetapi dapat berbentuk citra (image), suara (audio), dan video, atau berkas biner lainnya.

Supaya pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk yang tersandi disebut ciphertext atau kriptogram yang harus bisa ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Gambar 1 memperlihatkan enkripsi dan dekripsi.

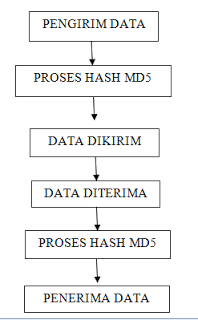


Gambar 1.1 Proses Enkripsi dan Deskripsi

* 1. **Algoritma Kiptrografi MD5**

MD5 adalah algoritma message digest yang dikembangkan oleh Ronald Rivest pada tahun 1991. MD5 mengambil pesan dengan panjang sembarang dan menghasilkan message digest 128 bit. Pada MD5 pesan diproses dalam blok 512 bit dengan empat round berbeda.

Message Digest 5 (MD5) ialah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. Pada standart Internet (RFC 1321), MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan, dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file. MD5 adalah salah satu dari serangkaian algortima message digest yang didesain oleh Profesor Ronald Rivest dari MIT (Rivest, 1994). Saat kerja analitik menunjukkan bahwa pendahulu MD5-MD4- mulai tidak aman, MD5 kemudian didesain pada tahun 1991 sebagai pengganti dari MD4 (kelemahan MD4 ditemukan oleh Hans Dobbertin) [2]. Algoritma Metode MD5, setiap pesan yang akan di-enkripsi, terlebih dahulu dicari berapa banyak bit yang terdapat pada pesan, anggap sebanyak b bit. Di sinib adalah bit non negative integer, b bisa saja nol dan tidak harus selalu kelipatan delapan.



Gambar 1. 2 proses alur pengiriman data

Fungsi hash yang banyak digunakan dalam kriptografi MD5 dan SHA. Dalam artikel ini fungsi hash yang digunakan algoritma MD5. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.

* 1. **Enkripsi**

Suatu proses dimana system yang metode untuk megubah suatu informasi sehingga tidak dapat dilihat tanpa membuka kunci pembukanya. Metode ini adalah metode paling efektif untuk menamankan data. Untuk membaca data yang telah di-encrip, dan kita harus mempunyai kunci untuk men-dekrip pesan atau data tersebut.

* 1. **Fungsi Hash**

Hash function atau fungsi hash adalah suatu cara menciptakan “fingerprint” dari berbagai data masukan. Hash function akan mengganti atau mentranspose-kan data tersebut untuk menciptakan fingerprint, yang biasa disebut hash value. Hash value biasanya digambarkan sebagai suatu string pendek yang terdiri atas huruf dan angka yang terlihat random (data biner yang ditulis dalam notasi heksadesimal). Suatu hash function adalah sebuah fungsi matematika, yang mengambil sebuah panjang variabel string input, yang disebut pre-image dan mengkonversikannya ke sebuah string output dengan panjang yang tetap dan biasanya lebih kecil, yang disebut message digest5. Hash function digunakan untuk melakukan fingerprint pada pre-image, yaitu menghasilkan sebuah nilai yang dapat menandai (mewakili) pre-image sesungguhnya. Fungsi hash satu arah (one-way hash function) adalah hash function yang bekerja satu arah, yaitu suatu hash function yang dengan mudah dapat menghitung hash value dari pre-image, tetapi sangat sukar untuk menghitung pre-image dari hash value. Sebuah fungsi hash satu arah, H(M), beroperasi pada suatu pre-image pesan M dengan panjang sembarang, dan mengembalikan nilai hash h yang memiliki panjang tetap. Dalam notasi matematika fungsi hash satu arah dapat ditulis sebagai:

*h = H(M), dengan h memiliki panjang b*

Ada banyak fungsi yang mampu menerima input dengan panjang sembarang dan menghasilkan output dengan panjang tetap, tetapi fungsi hash satu arah memiliki karakteristik tambahan yang membuatnya satu arah :

*Diberikan M, mudah menghitung h.*

*Diberikan h, sulit menghitung M agar H(M) = h.*

*Diberikan M, sulit menemukan pesan lain, M', agar*

*H(M) = H(M').*

Dalam dunia nyata, fungsi hash satu arah dikembangkan berdasarkan ide sebuah fungsi kompresi. Fungsi satu arah ini menghasilkan nilai hash berukuran n bila diberikan input berukuran b. Input untuk fungsi kompresi adalah suatu blok pesan dan hasil blok teks sebelumnya. Sehingga hash suatu blok M, adalah :

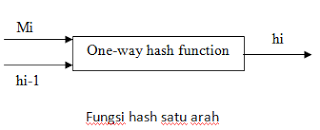
*hi = f(Mi,hi-1)*

dengan

*hi = hash value saat ini.*

*Mi = blok pesan saat ini.*

*hi-1 = hash value blok teks sebelumnya.*

[](http://2.bp.blogspot.com/-1jPVEoNhuKE/UfIbngYfRrI/AAAAAAAAAG8/KAPTtjpzzLY/s1600/Capture.PNG)

Gambar 1.3 Fungsi hash satu arah

Fungsi hash sangat berguna untuk menjaga integritas sebuah data. Sudah banyak algoritma hash function yang diciptakan, namun hash function yang umum digunakan saat ini adalah MD5 dan SHA (Secure Hash Algorithm). Algoritma hash function yang baik adalah yang menghasilkan sedikit hash collision.