BAB I
Pendahuluan

I.1. Latar Belakang.

Kemajuan dibidang teknologi informasi terutama komputer berkembang sangat pesat sehingga memungkinkan berbagai macam institusi-institusi melakukan interaksi melalui jaringan komputer Masalah keamanan merupakan faktor yang penting dan kerahasian suatu data sangatlah penting dari suatu sistem informasi. Informasi rahasia tidak akan berguna lagi apabila ditengah jalan informasi itu berhasil disadap atau dicuri .

Integritas data merupakan salah satu aspek dari keamanan jaringan.Integritas data adalah dimana data tetap terjaga atau tidak mengalami perubahan ketika data dikirimkan.

Kriptografi merupakan teknologi yang sangat berperan dalam proses keamanan komunikasi elektronik, digunakan untuk melakukan penyandian (enkripsi) data yang ditransaksikan selama perjalanan dari sumber ke tujuan dan juga melakukan penyusunan kembali (dekripsi) data yang telah tersandi tersebut di penerima.

Fungsi hash merupakan salah satu cara untuk intergritas suatu data yang dikirimkan dengan memberikan *"checksum*" atau tanda bahwa data tersebut tidak berubah. Fungsi Hash merupakan fungsi yang bersifat satu arah, yaitu fungsi yang dapat dengan mudah dikalkulasi tetapi sangat sulit untuk dibalik/*inverse* atau *reverse* . Salah satu contoh adalah faktorisasi; biasanya akan sulit untuk memfaktorkan bilangan yang besar, akan tetapi mudah untuk melakukan faktorisasi. Contohnya, akan sangat sulit untuk memfaktorkan 4399 daripada memverifikasi bahwa 53 x 83 = 4399.

MD5 atau *Message Digest 5* merupakan salah satu kriptografi yang berdasarkan fungsi *Hash,*dengan menggunakan nilai 128 bit hash dan biasanya digunakan untuk mengetahui integritas suatu data. MD 5 dibuat oleh Ronald Rivest di tahun 1991 untuk menggantikan fungsi *hash* yang sebelumnya yaitu MD4. MD5 mengolah data masukan ke dalam blok-blok 512 bit, lalu dibagi ke dalam sub-sub blok 32 bit. Keluaran dari MD5 merupakan rangkaian dari keempat blok 32 bit, yang menghasilkan nilai hash 128 bit.

MD5 sedikit lebih lambat jika dibandingkan dengan MD4 tetapi lebih aman daripada MD4.

I.2. Indentifikasi Masalah.

Bagaimana membahas, menjelaskan, membuat program MD5 sebagai salah satu teknik yang dapat digunakan dalam menentukan integritas data.

I.3. Tujuan.

Menganalisa dan megerti algoritma Message Digest 5 ke dalam program bahasa Java jdk 1.4.

I.4. Pembatasan Masalah.

1. Membahas dan menjelaskan teknik-teknik yang digunakan pada MD5 dan fungsi *hash*.
2. Membahas dan menjelaskan cara kerja, algoritma, implementasi MD5.
3. Masukan berupa text ASCII
4. Program berbasis Java jdk1.4 .

I.5. Sistematika Pembahasan.

Pada penyusunan laporan Tugas Akhir ini akan digunakan sistematika penulisan sebagai berikut ini :

1. BAB I PENDAHULUAN

   Membahas latar belakang, indentifikasi masalah, tujuan, pembatasan masalah dan sistematika penulisan.

2. BAB II LANDASAN TEORI

   Berisi tentang landasan teori tentang MD5 salah satunya adalah fungsi hash

3. BAB III PERANCANGAN PROGRAM MD5

   Membahas tentang perancangan program MD5

4. BAB IV HASIL PERCOBAAN

   Membahas tentang hasil-hasil percobaan dari program MD5

5 BAB V PENUTUP

   Berisi kesimpulan dan saran untuk pokok pembahasan tentang MD5.