Message Digest 5 (MD5)

Anugrah Adeputra
13505093

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha no.10, Bandung

e-mail : if15093@students.informatika.org

ABSTRAK

Pada era globalisasi seperti sekarang ini, lalu lintas informasi menjadi suatu hal yang sangat vital bagi manusia dalam menjalani kehidupannya sehari-hari. Lalu lintas informasi yang dimaksud di sini adalah proses penerimaan dan pengiriman informasi. Saat seseorang melakukan proses penerimaan atau pengiriman informasi terdapat enam buah hal yang menjadi sorotan utama dan merupakan aspek keamanan informasi, yaitu confidentiality, integrity, non-repuditation, authentication, data signature, dan access control.

Kata Kunci: *Kriptografi, Fungsi Hash, Message Digest 5*

1. Pendahuluan

Pada era globalisasi seperti sekarang ini, lalu lintas informasi menjadi suatu hal yang sangat vital bagi manusia dalam menjalani kehidupannya sehari-hari. Lalu lintas informasi yang dimaksud di sini adalah proses penerimaan dan pengiriman informasi. Saat seseorang melakukan proses penerimaan atau pengiriman informasi terdapat enam buah hal yang menjadi sorotan utama dan merupakan aspek keamanan informasi, yaitu confidentiality, integrity, non-repuditation, authentication, data signature, dan access control.

Kriptografi merupakan salah satu cara penanggulangan terhadap hal-hal yang disebutkan di atas. Penggunaan kriptografi yang bertujuan untuk mengaburkan isi pesan/informasi(bukan menghilangkan keberadaan informasi tersebut) dapat menanggulangi hal-hal yang merupakan aspek keamanan informasi seperti yang telah disebutkan di atas.

1.1 Tujuan

Pembuatan makalah ini bertujuan untuk menyelesaikan tugas akhir mata kuliah

Matematika Diskrit, serta diharapkan dengan pembuatan makalah ini, setidaknya, dapat membuka mata kita terhadap dunia kriptografi yang memegang peranan penting dalam aspek keamanan informasi.

1.2 Topik Pembahasan

Salah satu bagian kriptografi yang akan dibahas cukup mendalam pada makalah ini adalah fungsi hash satu arah. Fungsi hash satu arah adalah suatu fungsi kriptografis yang kita dapat dengan mudah melakukan enkripsi untuk mendapatkan ciphertext-nya tetapi sangat sulit untuk mendapatkan plaintext-nya. Salah satu fungsi hash yang paling banyak digunakan dan menjadi topik utama pembahasan makalah ini adalah Message Digest 5 (MD-5), yaitu suatu fungsi Hash kriptografis yang dibuat oleh Ronald Rivest pada tahun 1991.

2.1 Sekilas Kriptografi

Kriptografi (atau dikenal juga dengan sebutan kriptologi) berasal dari bahasa Yunani, yaitu kryptos yang berarti tersembunyi dan grafo yang berarti menulis. Jadi, Kriptografi adalah sebuah ilmu yang berguna untuk mengacak (kata yang lebih tepat adalah masking/ menyamarkan) data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga. Tentu saja data yang diacak harus bisa dikembalikan ke bentuk semula oleh pihak yang berwenang.

Kriptografi memiliki pengertian sebagai studi tentang penyembunyian pesan. Pada masa sekarang ini, kriptografi telah menjadi sebuah cabang dari teori informasi, sebagai studi matematikal dari informasi dan cara penyampaiannya dari satu tempat ke tempat lain

Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Salah seorang kriptografer terkenal, Ron Rivest, menyatakan bahwa: “cryptography is about communication in the presence of adversaries”. Kriptografi memiliki peran sentral di berbagai bidang seperti: keamanan informasi, autentikasi, dan akses kontrol. Tujuan utama dari kriptografi adalah menyembunyikan makna dari suatu pesan agar informasi yang ada tidak dapat diketahui oleh pihak selain yang dikirimi pesan tersebut, bukan menyembunyikan keberadaan pesan itu sendiri.

Ada enam tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan (Confidentiality).

Sederhananya, kerahasiaan adalah proses penyembunyian data dari orang-orang yang tidak punya otoritas. Dengan kata lain, kerahasiaan merupakan layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

2. Integritas Data (Integrity)

Proses untuk menjaga agar sebuah data tidak dirubah-rubah sewaktu ditransfer atau disimpan, berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. Penghindaran Penolakan (Non-repuditation)

Non repuditasi atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat. Proses untuk menjaga bukti-bukti bahwa suatu data berasal dari seseorang. Seseorang yang ingin menyangkal bahwa data tersebut bukan berasal darinya, dapat saja melenyapkan bukti-bukti yang ada. Karenanya diperlukan teknik untuk melindungi data-data tersebut.

4. Autentikasi (Authentication)

Proses untuk menjamin keaslian suatu data. Hal ini berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

5. Tanda Tangan Data (Data Signature)

Dapat disebut juga sebagai tanda tangan digital. Berguna untuk menandatangi data digital. Contohnya adalah Digital Signature Algorithm (DSA)

6. Kontrol Akses (Access Control)

Untuk mengontrol akses terhadap suatu entity.

Contoh penggunaan kriptografi di dunia internet antara lain: Secure Shell (SSH), SSL (Secure Socket Layer),Secure Hypertext Transfer Protocol (HTTP), dan lain lain.

Kriptografi juga memiliki peran sentral di bidang Ilmu Pengetahuan Komputer, khususnya mengenai kerahasiaan informasi dan akses kontrol. Contoh penggunaannya dalam kehidupan sehari-hari antara lain pada: Mesin ATM, Password Komputer, dan E-Commerce. Sedikit tambahan, saat ini belum ada definisi electronic commerce yang disepakati bersama sehingga sering terjadi kerancuan. Ada yang mengatakan bahwa eCommerce adalah web site yang digunakan untuk berdagang (semacam storefront), ada yang dimaksud eCommerce adalah EDI, dan seterusnya. Sebagai contoh, berikut ini adalah definisi eCommerce:

E-Commerce is a dynamic set of technologies, applications, and business

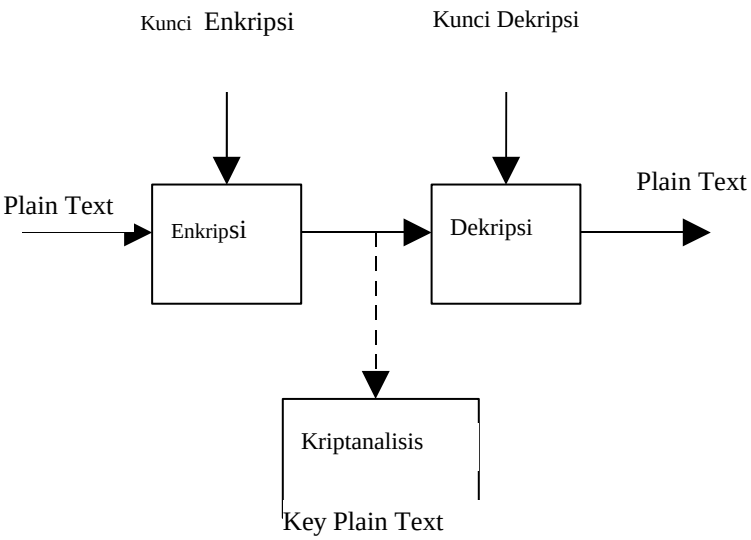
process that link enterprises, consumers, and communities through electronic

transactions and the electronic exchange of goods, services, and information.

Pada kriptografi, data yang ingin diacak biasanya disebut Plain Teks (Plain Text). Data diacak dengan menggunakan Kunci Enkripsi (Encryption Key). Proses pengacakan itu sendiri disebut Enkripsi (Encryption). Plain Teks yang telah diacak disebut Cipher Teks (Chiper Text). Kemudian proses untuk mengembalikan Cipher Teks ke Plain Teks disebut Dekripsi (Decryption). Kunci yang digunakan pada tahap Dekripsi disebut Kunci Dekripsi (Decryption Key).

Pada prakteknya, selain pihak yang berwenang ada pihak ketiga yang selalu berusaha untuk mengembalikan Cipher Teks ke Plain Teks atau memecahkan Kunci Dekripsi. Usaha oleh pihak ketiga ini disebut Kriptanalisis (Cryptanalysis).

Gambaran kriptografi dapat dilihat dari gambar pada halaman berikut



2.2 Enkripsi dan Dekripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang

bisa dimengerti (plaintext) menjadi sebuah kode yang tidak bisa dimengerti

(ciphertext). Sedangkan proses kebalikannya untuk mengubah ciphertext menjadi

plaintext disebut dekripsi. Sebuah sistem pengkodean menggunakan suatu tabel

atau kamus yang telah didefinisikan untuk mengganti kata atau informasi atau yang

merupakan bagian dari informasi yang dikirim. Secara umum operasi enkripsi dan

dekripsi secara matematis dapat digambarkan sebagai berikut :

EK (M) = C {proses enkripsi}

DK (C) = M {proses dekripsi}

Pada proses enkripsi pesan M dengan suatu kunci K disandikan menjadi pesan C.

Pada proses dekripsi pesan C dengan kunci K disandikan menjadi pesan semula

yaitu M. Misalnya S (sender) mengirim sebuah pesan ke R (receiver) dengan media

transmisi T. Di luar, ada O yang menginginkan pesan tersebut dan mencoba untuk

mengakses secara ilegal pesan tersebut. O disebut interceptor atau intruder. Setelah

S mengirim pesan ke R melalui media T, O bisa mengakses pesan tersebut dengan

cara-cara sebagai berikut :

a. Menganggu pesan, dengan mencegah pesan sampai ke R.

b. Mencegat pesan, dengan cara engetahui isi pesan tersebut.

c. Mengubah pesan dari bentuk aslinya dengan cara apapun.

d. Memalsukan pesan yangterlihat asli, jadi seolah-olah sebuah pesan dikirim oleh S.

Untuk melindungi pesan asli dari gangguan seperti ini dan menjamin keamanan dan

kerahasiaan data maka mulai dikenal sistem kriptografi untuk melindungi data, yaitu

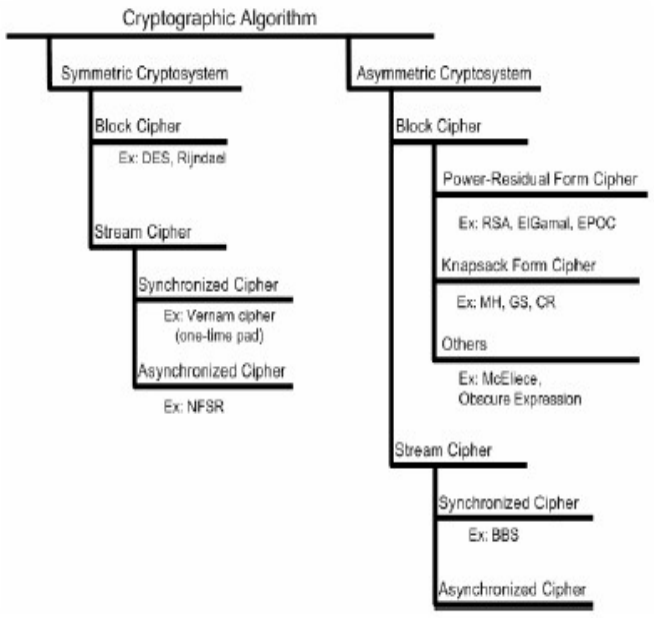
dengan mengenkripsi pesan dan untuk bisa membaca pesan kembali seperti aslinya

pesan harus didekripsi. Kriptografi merupakan cara yang paling praktis untuk

melindungi data yang ditransmisikan melalui sarana telekomunikasi. Dekripsi

sendiri berarti merubah pesan yang sudah disandikan menjadi pesan aslinya. Pesan asli biasanya disebut plaintext, sedangkan pesan yang sudah disandikan disebut ciphertext.

2.2 Gambar Pengelompokan Kriptografi



2.3 Algoritma Sandi

Algoritma sandi adalah algoritma yang berfungsi untuk melakukan tujuan kriptografis.

Algoritma tersebut harus memiliki kekuatan untuk melakukan (dikemukakan oleh Shannon):

- konfusi/pembingungan (confusion), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya
- difusi/peleburan (difusion), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

sehingga dapat digunakan untuk mengamankan informasi. Pada implementasinya sebuah algoritmas sandi harus memperhatikan kualitas layanan/Quality of Service atau QoS dari keseluruhan sistem dimana dia diimplementasikan. Algoritma sandi yang handal adalah algoritma sandi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri. Teknik dan metode untuk menguji kehandalan algoritma sandi adalah kriptanalisa.

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen teks terang /plaintext dan yang berisi elemen teks sandi/ciphertext. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen teks terang dinotasikan dengan P, elemen-elemen teks sandi dinotasikan dengan C, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D.

Enkripsi : E(P) = C

Dekripsi : D(C) = P atau D(E(P)) = P

Teknik kriptografi modern yang ada saat ini dapat dikelompokkan sebagaimana ditunjukkan pada gambar di halaman sebelumnya.

Kriptosistem Simetrik (Symmetric Cryptosystem) atau disebut juga Kunci Pribadi (Private Key) adalah metode kriptografi dimana kunci enkripsi bisa diperoleh dari kunci deskripsi atau sebaliknya. Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci – kunci ini harus dirahasiakan. Oleh sebab itu sistem ini sering disebut sebagai secret key cipher system. Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

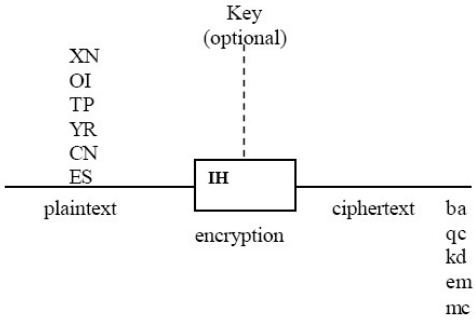
Kebalikan dari sistem ini adalah Kriptosistem Asimetrik (Asymmetric Cryptosystem) atau disebut juga Kunci Publik (Public Key). Kunci Pribadi disini berarti bahwa pemegang kunci enkripsi maupun dekripsi hanyalah pihak-pihak berwenang saja.

Karena melihat kembali sifatnya, bila pihak ketiga memperoleh salah satu kunci tersebut maka dia bisa memperoleh kunci yang lain. Kunci Publik berarti Kunci Enkripsi dapat disebarluaskan ke publik sedangkan pihak berwenang cukup menjaga kerahasiaan Kunci Deskripsi. Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut: bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca pesan tersebut , ia perlu mendekripsikannya dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal pesan serta keaslian pesan tersebut, karena adanya mekanisme ini. Contoh dari sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

Berdasarkan dari jenis data yang diolah, teknik kriptografi dapat dibagi menjadi dua bagian:

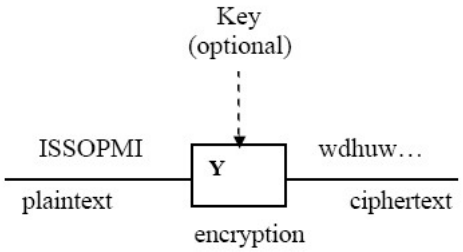
Block Cipher dan Stream Cipher. Pada Block Cipher, sesuai namanya data Plain Teks diolah per blok data. Sistem block cipher mengkodekan data dengan cara membagi plaintext menjadi per blok dengan ukuran yang sama dan tetap. Kemudian setiap bloknya dienkripsi atau didekripsi sekaligus. Cara ini bekerja lebih cepat karena plaintext dibagi atas beberapa blok. Biasanya proses enkripsi dan dekripsi dilakukan dalam ukuran blok tertentu.
Transposisi merupakan contoh dari penggunaan block cipher. Pada transposisi kolumnar dengan menggunakan matriks, pesan diterjemahkan sebagai satu blok.
Ukuran blok yang dibutuhkan tidak memiliki kesamaan dengan ukuran sebuah karakter. Block cipher bekerja pada blok plaintext dan menghasilkan blok – blok ciphertext.

Sistem Block Cipher dapat dilihat pada gambar:



Di lain pihak, pada Stream Cipher, data Plain Teks diolah per satuan data terkecil, misalnya per bit atau per karakter. Stream cipher adalah suatu sistem dimana proses enkripsi dan dekripsinya dilakukan dengan cara bit per bit. Pada sistem ini aliran bit kuncinya dihasilkan oleh suatu pembangkit bit acak. Aliran kunci ini dikenakan operasi XOR dengan aliran bit – bit dari plaintext untuk menghasilkan aliran bit – bit ciphertext. Pada proses dekripsi alliran bit ciphertext dikenakan operasi XOR dengan aliran bit kunci yang identik untuk menghasilkan plaintext.
Keamanan dari sistem ini tergantung dari pembangkit kunci, jika pembangkit
kunci menghasilkan aliran bit – bit 0 maka ciphertext yang dihasilkan akan sama
dengan plaintext, sehingga seluruh operasi akan menjadi tidak berguna oleh
karena itu diperlukan sebuah pembangkit kunci yang dapat menghasilkan aliran
bit – bit kunci yang acak dan tidak berulang. Semakin acak aliran kunci yang
dihasilkan oleh pembangkit kunci, maka ciphertext akan semakin sulit dipecahkan.

Sistem Stream Cipher dapat dilihat pada gambar:



Teknik Kriptografi kemudian dibagi lagi menjadi dua kelompok, yaitu *Synchronized Cipher* dimana Kunci Enkripsi dan Kunci Dekripsi perlu disinkronisasi, dan *Asynchronized Cipher* dimana sinkronisasi tidak diperlukan. Stream Cipher dapat dibagi menjadi dua kelompok ini, sedangkan pada Block Cipher hanya ada *Synchronized Cipher*. *Power-Residual Form Cipher* adalah teknik dimana dalam proses enkripsinya menggunakan rumus matematika XY (mod N) atau rumus yang mirip seperti itu. *Knapsack Form Cipher* adalah teknik yang menggunakan *Knapsack Problem* yang merupakan problem komputasi kelas NP-Komplit (*NP-Complete/ NP-Hard*).

2.4 Fungsi Hash Kriptografis

Fungsi hash Kriptografis adalah fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data. Umumnya digunakan untuk keperluan autentikasi dan integritas data. Fungsi hash adalah fungsi yang secara efisien mengubah string input dengan panjang berhingga menjadi string output dengan panjang tetap yang disebut nilai hash.

Sifat-Sifat Fungsi Hash Kriptografi

• Tahan preimej (Preimage resistant): bila diketahui nilai hash h maka sulit (secara komputasi tidak layak) untuk mendapatkan m dimana h = hash(m).

• Tahan preimej kedua (Second preimage resistant): bila diketahui input m1 maka sulit mencari input m2 (tidak sama dengan m1) yang menyebabkan hash(m1) = hash(m2).

• Tahan tumbukan (Collision-resistant): sulit mencari dua input berbeda m1 dan m2 yang menyebabkan hash(m1) = hash(m2)

Algoritma-Algoritma Fungsi Hash Kriptografi

Beberapa contoh algoritma fungsi hash Kriptografi:

- MD4
- MD5
- SHA-0
- SHA-1
- SHA-256
- SHA-512

2.5 TEKNIK DASAR KRIPTOGRAFI

Plaintext: “5 TEKNIK DASAR KRIPTOGRAFI”

1. Subsitusi

Langkah pertama dari teknik ini adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak.

Contoh Tabel Subtitusi:

A B C D E F G H I J K L MN O P Q R S T U V WX Y Z 1 2 3 4 5 6 7 8 9 0 , #
B F 1 K Q G A T P J 6 H Y D 2 X 5 M V 7 C 8 4 I 9 N R E U 3 L S W, # O Z 0

Tabel substitusi diatas dibuat secara acak. Tanda spasi akan diganti dengan tanda ‘#’. Dengan menggunakan tabel tersebut, dari plaintext di atas akan dihasilkan ciphertext "L07Q6DP60KBVBM06MPX72AMBGP". Dengan menggunakan tabel substitusi yang sama secara dengan arah yang terbalik (reverse), plaintext dapat diperoleh kembali dari ciphertext-nya.

2. Blocking

Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan secara independen. Plaintext yang dienkripsikan dengan menggunakan teknik blocking adalah :

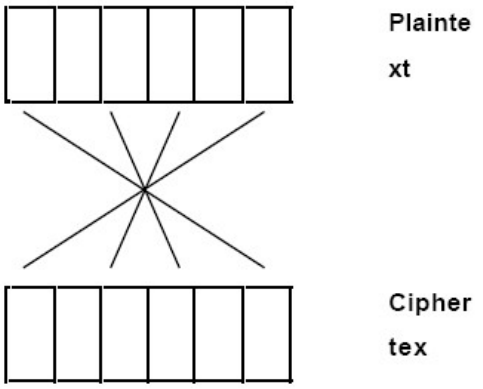
5	K		G	Blok 1
		K	R	Blok 2
T	D	R	A	Blok 3
E	A	I	F	Blok 4
K	S	P	I	Blok 5
N	A	T		Blok 6
I	R	O		Blok 7

Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk

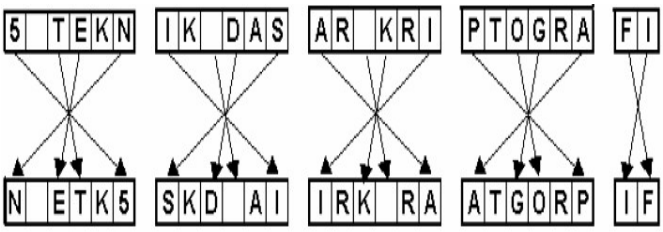
penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan
teknik ini. Plaintext d ituliskan secara vertikal ke bawah berurutan pada lajur, dan
dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya
adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan
blok-nya. Jadi ciphertext yang dihasilkan dengan teknik ini adalah "5K G
KRTDRAEAIFKSPINAT IRO". Plaintext dapat pula ditulis secara horizontal dan
ciphertextnya adalah hasil pembacaan secara vertikal.

3. Permutasi

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga
disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan
aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam
teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang
diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang
diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi
menjadi blok-blok dengan panjang yang sama.
Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 6
karakter, dengan aturan permutasi sebagai berikut :



Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi
dari plaintext adalah sebagai berikut :



Ciphertext yang dihasilkan dengan teknik permutasi ini adalah "N ETK5 SKD
AIIRK RAATGORP FI".

4. Ekspansi

Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan
pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini
adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi
awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu
kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i".
Proses enkripsi dengan cara ekspansi terhadap plaintext terjadi sebagai berikut :

Ciphertext yang dihasilkan

Ciphertextnya adalah "5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN". Aturan ekspansi dapat dibuat lebih kompleks. Terkadang teknik ekspansi digabungkan dengan teknik lainnya, karena teknik ini bila berdiri sendiri terlalu mudah untuk dipecahkan.

5. Pemampatan (Compaction)

Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&". Proses yang terjadi untuk plaintext kita adalah :

Aturan penghilangan karakter dan karakter khusus yang berfungsi sebagai pemisah menjadi dasar untuk proses dekripsi ciphertext menjadi plaintext kembali.

Dengan menggunakan kelima teknik dasar kriptografi diatas, dapat diciptakan kombinasi teknik kriptografi yang amat banyak, dengan faktor yang membatasi semata-mata hanyalah kreativitas dan imajinasi kita. Walaupun sekilas terlihat sederhana, kombinasi teknik dasar kriptografi dapat menghasilkan teknik kriptografi turunan yang cukup kompleks, dan beberapa teknik dasar kriptografi masih digunakan dalam kriptografi modern.

3. Pembahasan

Yang akan menjadi topik pembahasan adalah salah satu jenis Fungsi Hash Kriptografis yang cukup dikenal dan digunakan oleh banyak kalangan yaitu MD5(Message Digest 5).

MD5(Message Digest 5)

MD5 merupakan sebuah fungsi Hash kriptografis yang didesain oleh Ronald Rivest (yang merupakan salah satu penemu dari Algoritma RSA) pada tahun 1991.

Dalam kriptografi, MD5 (Message-Digest algortihm 5) 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 digunkan untuk melakukan pengujian integritas sebuah file.

MD5 di desain oleh Ronald Rivest pada tahun 1991 untuk menggantikan hash function sebelumnya, MD4. Pada tahun 1996, sebuah kecacatan ditemukan dalam desainnya, walau bukan kelemahan fatal, pengguna kriptografi mulai menganjurkan menggunakan algoritma lain, seperti SHA-1 (klaim terbaru menyatakan bahwa SHA-1 juga cacat). Pada tahun 2004, kecacatan-kecacatan yang lebih serius ditemukan menyebabkan penggunaan algoritma tersebut dalam tujuan untuk keamanan jadi makin dipertanyakan.

Pada tahun 1993, den Boer dan Bosselaers memberikan awal, bahkan terbatas, hasil dari penemuan pseudo-collision dari fungsi kompresi MD5. Dua vektor inisialisasi berbeda I dan J dengan beda 4-bit diantara keduanya.

MD5compress(I,X) = MD5compress(J,X)

Pada tahun 1996 Dobbertin mengumumkan sebuah kerusakan pada fungsi kompresi MD5. Dikarenakan hal ini bukanlah serangan terhadap fungsi hash MD5 sepenuhnya, hal ini menyebabkan para pengguna kriptografi menganjurkan pengganti seperti WHIRLPOOL, SHA-1 atau RIPEMD-160.

Ukuran dari hash — 128-bit — cukup kecil untuk terjadinya serangan brute force birthday attack. MD5CRK adalah proyek distribusi mulai Maret 2004 dengan tujuan untuk menunjukka kelemahan dari MD5 dengan menemukan kerusakan kompresi menggunakan brute force attack.

Bagaimanapun juga, MD5CRK berhenti pada tanggal 17 Agustus 2004, saat [[kerusakan hash]] pada MD5 diumumkan oleh Xiaoyun Wang, Dengguo Feng, Xuejia Lai dan Hongbo Yu [1][2]. Serangan analitik mereka dikabarkan hanya memerlukan satu jam dengan menggunakan IBM P690 cluster.

Pada tanggal 1 Maret 2005, Arjen Lenstra, Xiaoyun Wang, and Benne de Weger mendemontrasikan[3] kunstruksi dari dua buah sertifikat X.509 dengan public key yang berbeda dan hash MD5 yang sama, hasil dari demontrasi menunjukkan adanya kerusakan. Konstruksi tersebut melibatkan private key untuk kedua public key tersebut. Dan beberapa hari setelahnya, Vlastimil Klima menjabarkan[4] dan mengembangkan algortima, mampu membuat kerusakan Md5 dalam beberapa jam dengan menggunakan sebuah komputer notebook. Hal ini menyebabkan MD5 tidak bebas dari kerusakan.

Dikarenakan MD5 hanya menggunakan satu langkah pada data, jika dua buah awalan dengan hash yang sama dapat dibangun, sebuah akhiran yang umum dapat ditambahkan pada keduanya untuk membuat kerusakan lebih masuk akal. Dan dikarenakan teknik penemuan kerusakan mengijinkan pendahuluan kondisi hash menjadi arbitari tertentu, sebuah kerusakan dapat ditemukan dengan awalan apapun. Proses tersebut memerlukan pembangkitan dua buah file perusak sebagai file templat, dengan menggunakan blok 128-byte dari tatanan data pada 64-byte batasan, file-file tersebut dapat

mengubah dengan bebas dengan menggunakan algoritma penemuan kerusakan.

Efek Nyata dari Kriptoanalisis

Saat ini dapat diketahui, dengan beberapa jam kerja, bagaimana proses pembangkitan kerusakan MD5. Yaitu dengan membangkitkan dua byte string dengan hash yang sama. Dikarenakan terdapat bilangan yang terbatas pada keluaran MD5 (2128), tetapi terdapat bilangan yang tak terbatas sebagai masukannya, hal ini harus dipahami sebelum kerusakan dapat ditimbulkan, tapi hal ini telah diyakini benar bahwa menemukannya adalah hal yang sulit.

Sebagai hasilnya bahwa hash MD5 dari informasi tertentu tidak dapat lagi mengenalinya secara berbeda. Jika ditunjukkan informasi dari sebuah public key, hash MD5 tidak mengenalinya secata berbeda jika terdapat public key selanjutnya yang mempunyai hash MD5 yang sama.

Bagaimanapun juga, penyerangan tersebut memerlukan kemampuan untuk memilih kedua pesan kerusakan. Kedua pesan tersebut tidak dengan mudah untuk memberikan serangan preimage, menemukan pesan dengan hash MD5 yang sudah ditentukan, ataupun serangan preimage kedua, menemukan pesan dengan hash MD5 yang sama sebagai pesan yang diinginkan.

Hash MD5 lama, yang dibuat sebelum serangan-serangan tersebut diungkap, masih dinilai aman untuk saat ini. Khususnya pada digital signature lama masih dianggap layak pakai. Seorang user boleh saja tidak ingin membangkitkan atau mempercayai signature baru menggunakan MD5 jika masih ada kemungkinan kecil pada teks (kerusakan dilakukan dengan melibatkan pelompatan beberapa bit pada bagian 128-byte pada masukan hash) akan memberikan perubahan yang berarti.

Penjaminan ini berdasar pada posisi saat ini dari kriptoanalisis. Situasi bisa saja berubah secara tiba-tiba, tetapi menemukan kerusakan dengan beberapa data yang belum-ada adalah permasalahan yang lebih susah lagi, dan akan selalu butuh waktu untuk terjadinya sebuah transisi.

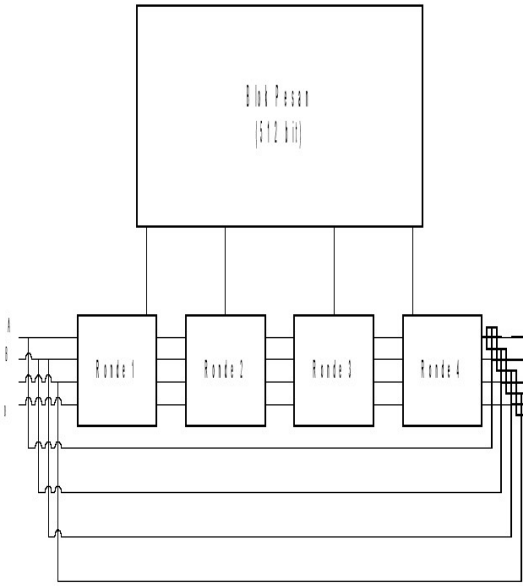
Prinsip Dasar MD5

Message Digest 5 (MD-5) adalah salah satu penggunaan fungsi hash satu arah yang paling banyak digunakan. MD-5 merupakan fungsi hash kelima yang dirancang oleh Ron Rivest dan
didefinisikan pada RFC 1321[10]. MD-5 merupakan pengembangan dari MD-4 dimana terjadi
penambahan satu ronde[1,3,10]. MD-5 memproses teks masukan ke dalam blok-blok bit sebanyak 512 bit, kemudian dibagi ke dalam 32 bit sub blok sebanyak 16 buah.

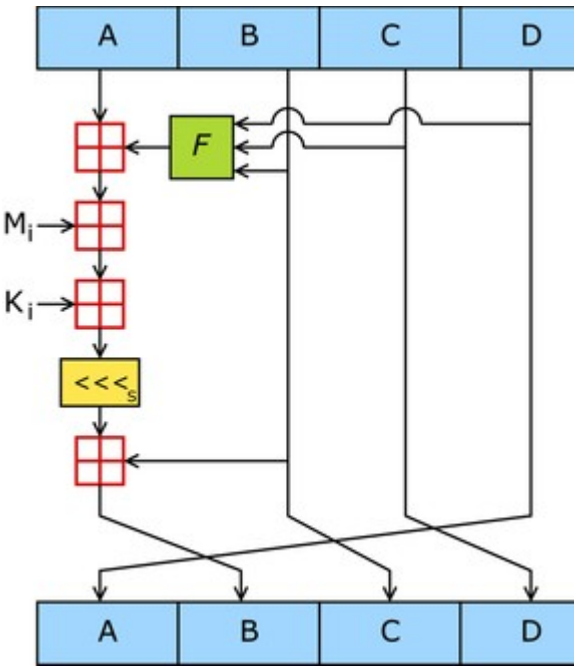
Keluaran dari MD-5 berupa 4 buah blok yang masing-masing 32 bit yang mana akan menjadi 128 bit yang biasa disebut nilai hash[3,10].

Pada Gambar terlihat simpul utama dari MD-5. Simpul utama MD5 mempunyai blok pesan dengan panjang 512 bit yang masuk ke dalam 4 buah ronde.

Hasil keluaran dari MD-5 adalah berupa 128 bit dari byte terendah A dan tertinggi byte D.



Algoritma



Satu operasi MD5 — MD5 terdiri atas 64 operasi, dikelompokkan dalam empat putaran dari 16 operasi. F adalah fungsi nonlinear; satu fungsi digunakan pada tiap-tiap putaran. Mi menujukkan blok 32-bit dari masukan pesan, dan Ki menunjukkan konstanta 32-bit, berbeda untuk tiap-tiap operasi.

s menunjukkan perputaran bit kiri oleh s; s bervariasi untuk tiap-tiap operasi. menunjukan tambahan modulo 232. MD5 memproses variasi panjang pesan kedalam keluaran 128-bit dengan panjang yang tetap. Pesan masukan dipecah menjadi dua gumpalan blok 512-bit; Pesan ditata sehingga panjang pesan dapat dibagi 512. Penataan bekerja sebagai berikut: bit tunggal pertama, 1, diletakkan pada akhir pedan. Proses ini diikuti dengan serangkaian nol (0) yang diperlukan agar panjang pesan lebih dari 64-bit dan kurang dari kelipatan 512. Bit-bit sisa diisi dengan 64-bit integer untuk menunjukkan panjang pesan yang asli. Sebuah pesan selalu ditata setidaknya dengan 1-bit tunggal, seperti jika panjang pesan adalah kelipatan 512 dikurangi 64-bit untuk informasi panjang (panjang mod(512) = 448), sebuah blok baru dari 512-bit ditambahkan dengan 1-bit diikuti dengan 447 bit-bit nol (0) diikuti dengan panjang 64-bit.

Algoritma MD5 yang utama beroperasi pada kondisi 128-bit, dibagi menjadi empat word 32-bit, menunjukkan A, B, C dan D. Operasi tersebut di inisialisasi dijaga untuk tetap konstan. Algoritma utama kemudian beroperasi pada masing-masing blok pesan 512-bit, masing-masing blok melakukan pengubahan terhadap kondisi.Pemrosesan blok pesan terdiri atas empat tahap, batasan putaran; tiap putasan membuat 16 operasi serupa berdasar pada fungsi non-linear F, tambahan modular, dan rotasi ke kiri. Gambar satu mengilustrasikan satu operasi dalam putaran. Ada empat macam kemungkinan fungsi F, berbeda dari yang digunakan pada tiap-tiap putaran:

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$

$H(X,Y,Z) = X \oplus Y \oplus Z$
$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$
$\oplus, \wedge, \vee, \neg$ menunjukkan operasi logikan XOR, AND, OR dan NOT.

Pseudocode pada algoritma MD5 adalah sebagai berikut.

//Catatan: Seluruh variable tidak pada 32-bit dan dan wrap modulo 2^32 saat melakukan perhitungan

//Mendefinisikan r sebagai berikut

```
var int[64] r, k
r[ 0..15] := {7, 12, 17, 22,  7, 12, 17,
22,  7, 12, 17, 22,  7, 12, 17, 22}
r[16..31] := {5,  9, 14, 20,  5,  9, 14,
20,  5,  9, 14, 20,  5,  9, 14, 20}
r[32..47] := {4, 11, 16, 23,  4, 11, 16,
23,  4, 11, 16, 23,  4, 11, 16, 23}
r[48..63] := {6, 10, 15, 21,  6, 10, 15,
21,  6, 10, 15, 21,  6, 10, 15, 21}

//Menggunakan bagian fraksional biner
dari integral sinus sebagai konstanta:
for i from 0 to 63
    k[i] := floor(abs(sin(i + 1)) ×
2^32)

//Inisialisasi variabel:
var int h0 := 0x67452301
var int h1 := 0xEFCDAB89
var int h2 := 0x98BADCFE
var int h3 := 0x10325476

//Pemrosesan awal:
append "1" bit to message
append "0" bits until message length in
bits ≡ 448 (mod 512)
append bit length of message as 64-bit
little-endian integer to message

//Pengolahan pesan paada kondisi
gumpalan 512-bit:
for each 512-bit chunk of message
    break chunk into sixteen 32-bit
little-endian words w(i), 0 ≤ i ≤ 15

    //Inisialisasi nilai hash pada
gumpalan ini:
    var int a := h0
    var int b := h1
    var int c := h2
    var int d := h3

    //Kalang utama:
    for i from 0 to 63
        if 0 ≤ i ≤ 15 then
            f := (b and c) or ((not b)
and d)
            g := i
        else if 16 ≤ i ≤ 31
            f := (d and b) or ((not d)
and c)
            g := (5×i + 1) mod 16
        else if 32 ≤ i ≤ 47
            f := b xor c xor d
            g := (3×i + 5) mod 16
        else if 48 ≤ i ≤ 63
            f := c xor (b or (not d))
            g := (7×i) mod 16

        temp := d
        d := c
        c := b
        b := ((a + f + k(i) + w(g))
leftrotate r(i)) + b
        a := temp

    //Tambahkan hash dari gumpalan
sebagai hasil:
    h0 := h0 + a
    h1 := h1 + b
    h2 := h2 + c
    h3 := h3 + d

var int digest := h0 append h1 append h2
append h3 //(diwujudkan dalam little-
endian)

Catatan: Meskipun rumusan dari yang
tertera pada RFC 1321, berikut ini
sering digunakan untuk meningkatkan
efisiensi:

(0  ≤ i ≤ 15): f := d xor (b and (c xor
d))
(16 ≤ i ≤ 31): f := c xor (d and (b xor
c))
```

Hash-Hash MD5

Hash-hash MD5 sepanjang 128-bit (16-byte), yang dikenal juga sebagai *ringkasan pesan*, secara tipikal ditampilkan dalam bilangan heksadesimal 32-digit. Berikut ini merupakan contoh pesan ASCII sepanjang 43-byte sebagai masukan dan *hash* MD5 terkait:

MD5("The quick brown fox jumps over the lazy dog") = 9e107d9d372bb6826bd81d3542a419d6

Bahkan perubahan yang kecil pada pesan akan (dengan probabilitas lebih) menghasilkan *hash* yang benar-benar berbeda, misalnya pada kata "dog", huruf d diganti menjadi c:

MD5("The quick brown fox jumps over the lazy cog") = 1055d3e698d289f2af8663725127bd4b

Hash dari panjang-nol ialah:

MD5("") = d41d8cd98f00b204e9800998ecf8427e

Penutup

Informasi memegang peranan penting di era globalisasi seperti sekarang ini, oleh karena itu lalu lintas informasi memerlukan fasilitas-fasilitas yang menunjang aspek keamanan informasi agar informasi yang tidak berhak diketahui orang selain pihak yang berwenang dapat tetap terjaga kerahasiaannya. Kriptografi merupakan suatu solusi terhadap permasalahan ini.

Dari pembahasan yang disampaikan pada makalah ini, dapat kita lihat pentingnya peranan kriptografi dalam aspek keamanan informasi.

Dengan kombinasi beberapa jenis kriptografi, maka akan semakin sulit bagi seseorang yang tidak berwenang mengetahui informasi untuk mencari tahu isi informasi yang disampaikan.

MD5 merupakan salah satu jenis fungsi Hash satu arah yang cukup popular digunakan dalam dunia kriptografi. Meskipun fungsi ini memiliki beberapa kelemahan, namun dunia kriptografi yang terus berkembang berhasil mengembangkan jenis-jenis fungsi kriptografis baru yang merupakan penyempurnaan dari fungsi tersebut.

Daftar Pustaka

- Tanenbaum, Andrew S, Jaringan Komputer Edisi Indonesia Dari Computer Network
  Edisi III, Prenhallindo, Jakarta, 1997
- http:// www.counterpane.com/
- http:// www.cryptography.com.
- http:// www.cryptography.org
- http://www.eskino.com/~weidai/benchrarks.html.
- http:// www.cwi.nl/~kik/persb-UK.html.
- http://www.faqs.org/ftp/rfc/ rfc1321.txt
- http://www.spitzner.net/pubs.html
- http://www.secure-hash-algorithm-md5-sha-1.co.uk/index.htm
- Wikipedia
- Microsot Encarta

Makalah Aghus Sofwan tentang *Aplikasi dengan Algoritma Kriptografi MD5*