Perbandingan Algoritma MD4 dan MD5 serta Implementasinya dalam Kehidupan Sehari-hari

M. Pasca Nugraha (13507033)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
email : if17033@students.if.itb.ac.id

***Abstract*—Algoritma MD4 dan MD5 merupakan salah satu dari beberapa algoritma hashing yang sering dipakai dalam kehidupan sehari-hari, misalnya dalam pembuatan tanda tangan digital. Algoritma MD5 sebenarnya merupakan pengembangan dari algortima MD4. Namun kedua algoritma tersebut memiliki kelebihan dan kekurangannya masing-masing.**

Makalah ini membahas perbandingan antara kedua algoritma tersebut, melakukan analisis kelebihan dan kekurangannya, serta memberikan alternatif solusi untuk mengatasi kekurangan yang ada, terutama berkaitan dengan kolisi yang terjadi pada algoritma tersebut.

***Kata kunci*—algoritma MD4, algoritma MD5, fungsi hash, kolisi.**

I. PENDAHULUAN

Seiring perkembangan teknologi akhir-akhir ini, keamanan sebuah pesan, dalam hal ini otentifikasi sebuah dokumen sangat diperlukan. Oleh karena itu, algoritma fungsi hash yang digunakan untuk pembuatan tanda tangan digital juga semakin berkembang.

Berbagai fungsi hash telah dibuat dengan algoritmanya masing-masing. Di sisi lain, para kriptanalis saling berlomba untuk menemukan kelemahannya, yaitu kolisi, pada setiap fungsi hash yang telah dibuat tersebut. Demikian juga pembaharuan dan pengembangan terus dilakukan untuk mendapatkan algoritma hash yang benar-benar tanpa cacat.

Salah satu jenis algoritma fungsi hash yang terkenal adalah Message Diggest (MD) dengan versi-versinya, yaitu MD, MD2, MD3, MD4, MD5, dan yang terbaru adalah MD6. Setiap fungsi hash merupakan perbaikan dari fungsi hash sebelumnya, misalnya fungsi hash MD2 merupakan perbaikan dari MD2, dan seterusnya. Oleh karena itu seharusnya semakin baru algoritma fungsi hash tersebut, maka semakin baik dan kemungkinan terjadinya koloisi makin kecil. Demikian juga MD5, yang merupakan perbaikan dari versi sebelumnya, yaitu MD4.

II. DASAR TEORI

A. Fungsi Hash

Fungsi hash adalah fungsi yang menerima masukan string dengan panjang sembarang, lalu mentransformasikannya menjadi sebuah string lain yang panjangnya tetap untuk setiap masukan string. Fungsi hash biasa digunakan untuk menyederhanakan string yang sangat panjang sehingga pada umumnya string hasil keluaran fungsi hash jauh lebih kecil daripada string masukannya.

Persamaan fungsi hash adalah sebagai berikut :

$$h = H(M)$$

dimana :

h = nilai hash (keluaran dari fungsi hash)
M = string berukuran sembarang
H = fungsi hash

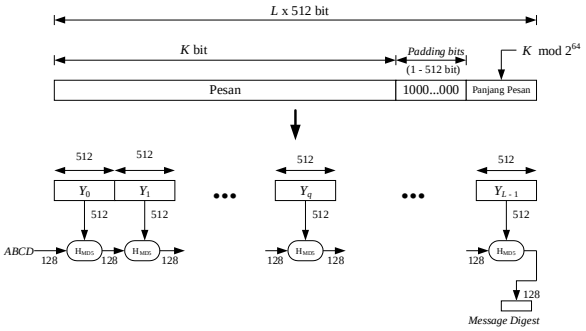
Fungsi hash satu arah adalah fungsi hash yang bekerja dalam satu arah, yaitu pesan yang sudah di-hash tidak dapat dikembalikan lagi menjadi pesan semula. Fungsi hash satu arah ini digunakan dalam pembuatan tanda tangan digital nantinya. Aplikasi fungsi hash satu arah dapat digunakan untuk menjaga integritas data, menghemat waktu pengeiriman, dan dapar menormalkan panjang data yang beraneka ragam.

B. Algoritma MD5

Algoritma MD5 atau Message Diggest 5 adalah fungsi hash satu arah yang dibuat oleh Ronald Rivest dari MIT pada tahun 1992. MD5 merupakan perbaikan dari MD4 setelah MD4 berhasil diserang oleh kriptanalis.

Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message diggest yang panjangnya 128 bit.

Gambaran umum algoritma MD5 dapat dilihat pada gambar di bawah ini :



Gambar 1. Gambaran umum MD5

Langkah-langkah pembuatan message diggest secara garis besar dapat dilihat pada gambar 1 di atas. Secara sistematis terdiri dari 4 langkah besar dan dapat diurutkan sebagai berikut :

1. Penambahan padding bits
2. Penambahan nilai panjang pesan semula
3. Inisialisasi penyangga MD
4. Pengolahan pesan dalam blok berukuran 512 bit

Pertama-tama pesan ditambah dengan sejumlah padding bits antara 1 sampai 512 sehingga panjang pesan kongruen dengan 448 modulo 512. Misalnya jika panjang pesan 448 bit, maka ditambahkan padding bit sebanyak 12 bit sehingga menjadi 960 bit. Padding bits terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.

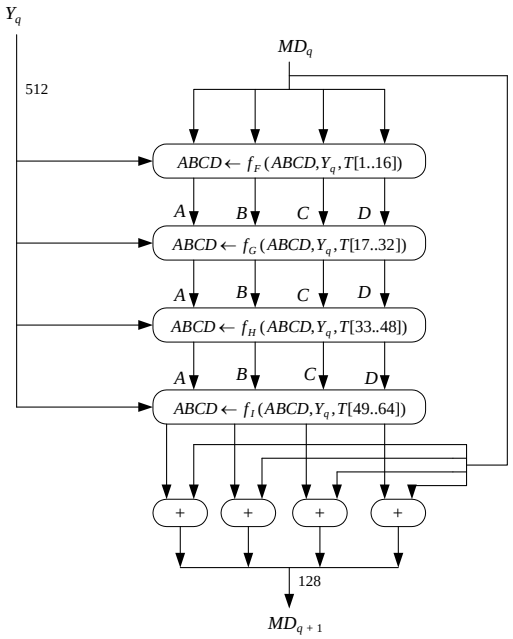
Setelah itu, pesan tadi selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula. Dengan kata lain, pesan yang telah dipaading tadi kemudian ditambahkan dengan panjang pesan dalam modulo 2^{64}. Misalnya, jika panjang pesan adalah K bit, maka pesan ditambahkan sebanyak K modulo 2^{64}.

Selanjutnya, dilakukan inisialisasi penyangga (buffer) MD. MD5 memerlukan 4 buah penyangga yang masing-masing berukuran 32 bit. Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga pada MD5 telah ditetukan nilainya yaitu sebagai berikut (dalam notasi hexa) :

A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210

Sebenarnya terdapat beberapa versi MD5 dengan nilai bit penyangga yang berbeda-beda. Hal ini karena pertimbangan keamanan. Nilai penyangga di atas merupakan yang terbaru.

Kemudian dilakukanlah pengolahan pesan. Pesan dibagi-bagi terlebih dahulu menjadi L buah blok yang masing-masing panjangnya 512 bit. Setiap blok kemudian diproses bersama dengan penyangga MD sehingga menghasilkan keluaran 128 bit. Proses ini disebut proses H_{MD5}. Gambaran proses MD5 dapat dilihat pada gambar berikut :



Gambar 2. Cara kerja MD5

Pada gambar di atas, Y adalah satu blok berukuran 512 bit tadi yang merupakan bagian dari pesan yang telah ditambahkan padding bit dan tambahan nilai panjang semula. MD adalah message diggest 128 bit yang dihasilkan. Proses HMD5 terdiri dari 4 buah putaran, yang masing-masing putaran melakukan operasi dasar MD5 sebanyak 16 kali dan setiap operasi dasar memakai sebuah elemen T.

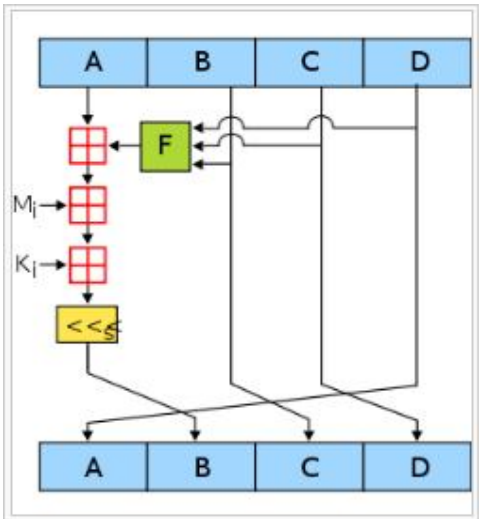
Fungsi-fungsi fF, fG, fH, dan fI masing-masing berisi 16 kali operasi dasar terhadap masukan menggunakan tabel T.

Hasil akhir atau string keluaran dari algoritma MD5 merupakan gabungan / penyambungan dari bit-bit di A, B, C, dan D.

C. Algoritma MD4

Algortma MD4 atau Message Diggest 4 merupakan salah satu seri algoritma Message Diggest yang dibuat oleh Ronald Rivest dari MIT pada tahun 1990, 2 tahun sebelum pembuatan MD5 yang menjadi perbaikannya. Proses fungsi hash MD4 terdiri atas 3 buah putaran dengan masing-masing putaran terdiri atas 16 buah operasi dasar.

Gambaran umum algoritma MD4 dapat dilihat pada gambar di bawah ini :



Gambar 3. Cara kerja MD4

III. ANALISIS MASALAH

A. Kolisi pada MD4 dan MD5

Kolisi merupakan kondisi dimana terdapat dua masukan string yang berbeda, namun memiliki message diggest keluaran fungsi hash yang sama. Hal ini sangat dihindari dalam pembuatan algoritma hash karena dapat membuktikan bahwa algoritma tersebut sudah tidak aman dan beresiko terjadinya pemalsuan dokumen.

Bayangkan saja terdapat sebuah file penting dengan message diggest tertentu. Kemudian datang pihak lain, katakanlah seorang hacker, yang mengubah-ubah file tersebut seenaknya. Namun message diggest dari file itu tidak berubah sehingga pemilik / pengguna file tersebut tidak menyadari bahwa file-nya telah berubah. Hal inilah yang dimaksud kolisi yang berpotensi terjadinya serangan pada dokumen.

Kelemahan pada MD4 mulai terkuak pada tahun 1991 dimana pihak lain dapat melakukan serangan terhadap putaran (*round*) terakhir pada operasi MD4. Hal ini menyebabkan MD4 tidak lagi aman. Kolisi pada MD4 ditemukan pada tahun 1995 oleh Hans Dobertin. Dia dapat menemukan dokumen atau file tertentu dengan message diggest yang sama hanya dalam hitungan detik. Pada tahun 2008, *resistance* atau tingkat keamanan MD4 benar-benar dipatahkan. Sejak saat itu algoritma MD4 sangat tidak aman digunakan.

Setelah diketahui kelemahan MD4, dibuatlah versi terbaru Message Diggest, yaitu MD5. Namun setelah beberapa tahun, ternyata terungkap pula bahwa MD5 juga memiliki kelemahan. Pada tahun 2009, *resistance* dari MD5 berhasil dipatahkan, sehingga seperti pendahulunya, MD5 pun sudah dianggap sangat tidak aman untuk digunakan.

B. Algoritma MD6

Algoritma MD6 merupakan algoritma MD terbaru yang dibuat oleh Ronald Rivest dan kawan-kawan pada tahun 2008. Algoritma ini merupakan perbaikan dari MD5. Namun karena cenderung masih baru, belum ada penelitian yang lengkap tentang keamanan dari algoritma ini dan apakah terdapat kolisi atau tidak.

IV. PERBANDINGAN ALGORITMA MD4 DAN MD5 SERTA IMPLEMENTASINYA

Perbedaan algoritma MD4 dan MD5 yang pertama adalah terletak pada jumlah putaran (round) yang dilakukan untuk setiap operasi. Pada MD4 hanya operasi hanya dilakukan sebanyak 3 putaran, sedangkan pada MD5 diperbaiki menjadi 4 putaran. Hal ini cukup efektif untuk mengurangi serangan pada putaran tersebut.

Perbedaan kedua, pada MD5, untuk setiap putaran ditambahkan sebuah konstanta baru yang unik untuk diproses / dioperasikan bersama-sama dengan string yang sudah ada. Hal ini tidak ada pada MD4 yang tetap memakai variabel yang sudah ada.

Perbedaan ketiga adalah pada fungsi g pada putaran kedua. Fungsi g pada MD4 adalah (XY v XZ v YZ) sedangkan pada MD5 adalah (XZ v Y not(Z)). Perubahan ini membuat fungsi g berkurang kesimetrisannya sehingga dinilai lebih aman.

Perbedaan keempat, pada MD5, hasil dari suatu putaran merupakan penambahan dari hasil putaran sebelumnya, sehingga menambah kompleksitas algoritma.

Sedangkan perbedaan yang kelima adalah urutan operasi pada MD4 sedikit diubah pada MD5 untuk meniadakan pola yang terjadi sehingga terkesan acak dan menambah keamanan.

Perbedaan-perbedaan di atas menunjukkan adanya *improvement* atau perkembangan algoritma menjadi lebih kompleks. Hal ini untuk mereduksi kelemahan-kelemahan pada MD4.

Oleh karena itu, dalam implementasinya, misalkan untuk pembuatan tandatangan digital, untuk verifikasi dokumen, dan lain-lain, algoritma MD5 jauh lebih aman daripada algoritma MD4. Walaupun begitu, algoritma MD5 juga masih memiliki kelemahan sehingga ada kemungkinan terjadi kolisi atau serangan terhadap algoritma ini. Namun paling tidak MD5 dapat memperkecil resiko keamanan tersebut daripada MD4.

V. KESIMPULAN

Algoritma MD5 merupakan perbaikan dari algoritma MD4. Desain yang sedikit berbeda membuat MD5 dinilai lebih aman daripada MD4. Serangan yang dilakukan pada putaran (*round*) terakhir pada MD4 berhasil direduksi dengan cara menambah putaran yang awalnya hanya 3 putaran pada MD4 menjadi 4 putaran pada MD5. Namun, hal tersebut ternyata tidak menjamin kemanan algoritma ini. Kolisi pada MD5 telah ditemukan sehingga dibutuhkan perbaikan kembali untuk mendapatkan algoritma hash yang aman.

Perbedaan antara algoritma MD4 dengan MD5 pada intinya dapat dilihat dari 5 hal :

1. Jumlah putaran (*round*) yang berbeda. Pada MD5 ditambahkan satu putaran menjadi 4 kali.
2. Masing-masing step pada MD5 ditambahkan sebuah konstanta yang unik.
3. Perubahan fungsi g pada MD5 untuk membuatnya lebih asimetris.
4. Pada MD5, hasil langkah yang satu ditambahkan ke langkah berikutnya sehingga hasil dari satu langkah merupakan kombinasi hasil langkah sebelumnya.
5. Urutan operasi MD4 dan MD5 sedikit diubah untuk menambah kompleksitas dan randomisasi.

REFERENCES

[1] Munir, Rinaldi. Diktat kuliah Kriptografi. Informatika : Bandung 2006

[2] Munir, Rinaldi. Slide-slide kuliah Kriptografi

[3] http://www.freesoft.org/CIE/RFC/1321/10.htm waktu akses : 16 Mei 2010

[4] http://www.rsa.com/rsalabs/node.asp?id=2253 waktu akses : 16 Mei 2010

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Mei 2010

M. Pasca Nugraha (13507033)