Analisis Kelemahan Fungsi Hash, Pemanfaatan, dan Penanggulangannya

Zakka Fauzan Muhammad [1)]
1) Teknik Informatika ITB, Bandung, email: if14020@students.if.itb.ac.id

Abstraksi – *Akhir-akhir ini, keamanan terhadap data sangat diperhatikan dalam pengiriman dan penerimaan sebuah dokumen dari satu pihak kepada pihak lainnya. Untuk itulah diciptakan kriptografi, sebuah seni untuk mengamankan data, dan pada awalnya bertujuan untuk menyandikan pesan yang dikirim dari satu pihak kepada pihak lainnya. Akan tetapi, kini, dengan era yang semakin maju, hal yang perlu diperhatikan, selain dari penyandian sebuah pesan, adalah bagaimana penerima pesan dapat memastikan bahwa pesan yang ia terima benar-benar berasal dari sumber yang benar. Pada umumnya, teknik kriptografi untuk hal semacam ini adalah dengan menggunakan kriptografi kunci publik, akan tetapi kunci publiknya adalah kunci untuk mendekripsi pesan dan kunci privatnya adalah kunci untuk mengenkripsi pesan. Merupakan kebalikan dari teknik kriptografi yang biasa digunakan, dimana pesan dienkripsi dengan menggunakan kunci publik, dan untuk mendekripsikannya harus menggunakan kunci privat.*

Kata Kunci*: kriptografi, fungsi hash*

1. PENDAHULUAN

Fungsi Hash, termasuk fungsi MD yang pertama sampai yang terakhir ada, yaitu MD5, merupakan salah satu teknik penyandian pesan yang sangat bisa diandalkan, dengan kekuatannya terletak pada pengubahan satu karakter di dalam dokumen atau data yang dipetakan akan menyebabkan perubahan yang cukup signifikan pada hasil fungsi hash-nya, sehingga dapat dengan mudah diketahui bahwa data atau dokumennya telah berubah. Kegunaan fungsi hash terutama digunakan pada implementasi tanda tangan dijital. Hal ini disebabkan, fungsi hash dapat diimplementasikan dengan menggunakan kunci publik sekalipun, dan implementasi dengan kunci publik ini jelas tidak cocok untuk enkripsi dan dekripsi yang biasa dilakukan, karena jika algoritma yang digunakan oleh pengenkripsi pesan diketahui, siapapun dapat mendekripsikannya, karena kunci publik akan dimiliki oleh siapapun juga.

Tanda tangan dijital sangat cocok digunakan untuk membuktikan keaslian suatu dokumen, termasuk didalamnya pembuktian bahwa pesan yang dikirim berasal dari orang yang seharusnya, ataupun pesan yang dikirim memang tidak pernah mengalami perubahan sama sekali setelah ditandatangani oleh si penulis pesan tersebut. Akan tetapi, fungsi hash, bukannya tanpa kelemahan sama sekali. Pada umumnya fungsi hash akan selalu menghasilkan satu panjang hasil hashing yang selalu tetap, misal selalu 32 bit, yang berarti jumlah kemungkinan nilai hash dari suatu pesan hanya 2^{32} kemungkinan saja, dengan demikian mungkin saja ada dua pesan yang berbeda yang menghasilkan nilai hash yang sama.

Pada makalah ini, fungsi hash yang digunakan akan selalu menggunakan kunci, untuk sedikit menyulitkan proses dekripsi yang dilakukan oleh kriptanalis. Pada kenyataannya, fungsi hash mungkin dan pada umumnya digunakan tanpa menggunakan kunci sama sekali, akan tetapi hal tersebut memudahkan proses dekripsi yang dilakukan oleh seorang kriptanalis. Kunci ini sendiri nantinya akan berperan sama dengan dokumen, yaitu sebagai bagian yang akan ikut dienkripsi. Pada umumnya proses dekripsi atau verifikasi dari sebuah dokumen atau data dapat dilakukan tanpa menggunakan kunci sama sekali, akan tetapi di dokumen ini, kunci tersebut dibutuhkan karena merupakan bagian yang akan ikut dienkripsi dan juga sebagai bagian yang terdekripsi nantinya, meskipun tidak ditampilkan ke dalam dokumen yang dapat dibaca.

2. KELEMAHAN FUNGSI HASH

Secara umum, ada dua hal yang bisa menjadi kelemahan dari fungsi hash. Yang pertama adalah, seperti pada umumnya kriptografi, tidak ada ilmu penyandian pesan yang sempurna, begitu pula dengan fungsi hash. Selalu saja ada cara dari seorang kriptanalis atau pemecah kode untuk memecahkan kode dari suatu algoritma kriptografi. Untuk pemecahan kode ini, beberapa diantaranya bahkan sudah dipublikasikan di umum, dan dapat diakses oleh siapapun yang ingin menggunakannya, meskipun mungkin pembuatnya menciptakan teknik penyerangan ini hanya sebagai bahan penelitian, sebagai bahan ujicoba, dan sebagai bukti bahwa fungsi hash, termasuk fungsi hash yang paling populer saat ini, yaitu MD5, bukannya tanpa kelemahan. Karena semakin berkembangnya ilmu pengetahuan untuk penyandian pesan ini, semakin

berkembang pula ilmu untuk memecahkan penyandian pesan tersebut.

Kelemahan kedua, seperti yang telah dijelaskan pada bagian pendahuluan, adalah bahwa fungsi hash akan selalu menghasilkan panjang yang tetap. Ini memungkinkan terjadinya benturan (kolisi) antara dua pesan. Benturan ini memang sangat jarang terjadi, akan tetapi sangat mungkin terjadi. Jadi andaikan kita memiliki dua pesan, mungkin saja dua pesan tersebut memiliki hasil fungsi hash yang sama persis, padahal perbedaan antara dua pesan tersebut sangatlah mencolok.

Kedua kelemahan ini, oleh seorang kriptanalis, dapat dimanfaatkan untuk tujuan tertentu, misalnya untuk melakukan penipuan, pengubahan pesan, serta hal-hal yang lainnya. Untuk lebih detil, hal ini akan dibahas pada bab 3.

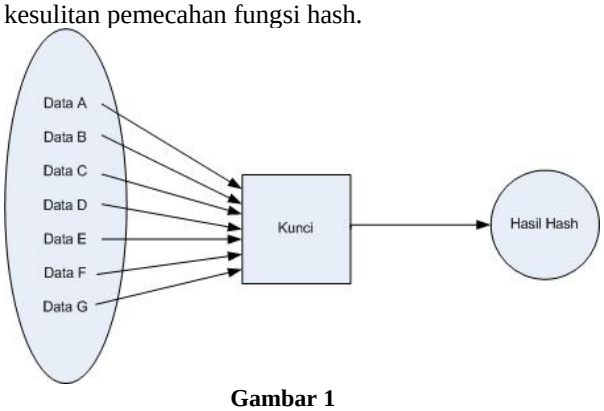
3. PEMANFAATAN KELEMAHAN FUNGSI HASH

Pemanfaatan Kelemahan Fungsi Hash dengan Memecahkan Kunci yang Digunakan untuk Pemetaan Fungsi Hash itu Sendiri

Dari kelemahan-kelemahan yang dimiliki oleh fungsi hash, seorang kriptanalis dapat memanfaatkannya. Untuk kasus pertama, dimana seorang kriptanalis dapat memecahkan fungsi hash, sebenarnya hal ini dapat dipertanyakan terlebih dahulu, karena pemecahan fungsi hash terdiri dari dua tahap:

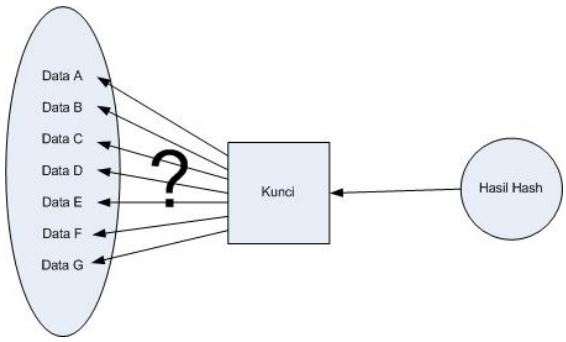
a. Pemecahan data hasil fungsi hash-nya itu sendiri, kembali menjadi dokumen aslinya
b. Verifikasi dan validasi data hasil pembalikan fungsi hash.

Dua tahap ini sangat diperlukan terutama diakibatkan oleh adanya kemungkinan kolisi dari fungsi hash. Jadi selain merugikan pemakai fungsi hash, kriptanalis yang ingin menyerang fungsi hash juga akan mengalami kesulitan dengan adanya kolisi ini. Berikut ini akan dipaparkan alasan kesulitan pemecahan fungsi hash.



Gambar 1

Dari gambar itu, terlihat adanya kolisi data A, data B, sampai data G terhadap satu kunci, karena akan selalu menghasilkan nilai hash yang sama. Hal ini akan sedikit membingungkan kriptanalis untuk proses dehash, atau proses pembalikan fungsi hash. Kebingungan yang menimpa seorang kriptanalis dapat terlihat pada gambar 2.



Gambar 2

Dari gambar 2 tersebut dapat terlihat, bahwa terdapat kebingungan dari pihak kriptanalis, dalam mendekripsikan pesan yang sudah terenkripsi oleh seseorang.

Untuk mengatasi permasalahan ini, biasanya seorang kriptanalis menggunakan pemeriksa kevalidan suatu data, termasuk di dalamnya terdapat proses validasi atau verifikasi suatu kalimat menggunakan suatu metode tertentu yang pada umumnya menggunakan sistem berbasis pengetahuan.

Setelah permasalahan tersebut teratasi, seorang kriptanalis dapat dengan mudah mendekripsi suatu pesan, termasuk diantaranya pemilihan hasil dekripsi yang tepat, yang sesuai. Dari sini, apapun dapat dilakukan oleh seorang kriptanalis dengan sangat mudah, hal ini disebabkan ia sudah dapat memecahkan fungsi hash yang digunakan oleh seseorang yang berusaha mengirimkan pesan kepada orang lain.

Pemanfaatan akibat kemungkinan ini sangat banyak, pesan apapun dapat diubah menjadi sesuatu yang sangat berbeda. Contohnya adalah sebagai berikut:

Pesan asli:

```
Saudara diharapkan hadir pada
hari Minggu, 13 Januari 2008,
untuk mengikuti proses wawancara
dan proses seleksi lebih lanjut.
```

Pesan itu, kemudian, dapat diubah menjadi apapun oleh seorang kriptanalis, salah satu contohnya adalah menjadi sebagai berikut:

```
Saudara tidak diterima, karena
kami merasa kemampuan saudara
masih sangat kurang. Kami mohon
maaf atas pemberitahuan ini.
```

Apapun isi dari pesan, dapat diubah menjadi pesan lain yang sama sekali tidak berhubungan dengan pesan sebelumnya. Hal ini sama sekali tidak dapat dicurigai oleh penerima pesan, karena begitu ia memverifikasi pesan tersebut dengan kunci publik yang ia miliki, ia akan mengetahui bahwa data tersebut benar adanya, dan merupakan dokumen yang asli yang telah ditandatangani dengan kunci privat yang sesuai oleh pengirim pesan tersebut.

Pemecahan Fungsi Hash dengan Menggunakan Teknik Kolisi Dua Buah Data atau Dokumen

Seperti terlihat pada gambar 1 dan pada uraian permasalahan, kolisi sangat mungkin terjadi pada dokumen-dokumen atau data-data yang berbeda sekalipun. Selain itu, untuk menambah jumlah kemungkinan pengkolisian dilakukan oleh seorang kriptanalis, perlu diketahui bahwa ada tak berhingga dokumen yang dapat mempunyai hasil hash yang sama persis. Hal ini tentunya merupakan kerugian bagi pihak yang memanfaatkan fungsi hash untuk mengamankan datanya, akan tetapi merupakan sebuah keuntungan besar bagi kriptanalis dan oleh orang-orang yang berusaha memanfaatkan hal tersebut untuk melakukan kejahatan.

Contoh pemanfaatan dari pengkolisian ini adalah sebagai berikut.

Seseorang (sebut saja A) ingin meminta orang lain (sebut saja B), untuk mengirimkan uang kepadanya. Untuk memastikan bahwa ia tidak berbohong, A terlebih dahulu menelepon B, mengatakan kebutuhannya tersebut, dan B mempercayainya. Kemudian A mengatakan, agar aman, ia akan mengirimkan jumlah uang yang ia butuhkan dan nomor rekening yang ia pakai melalui email, dan ia berjanji akan menandatanganinya secara dijital, agar B tahu bahwa pesan tersebut asli berasal dari A.

Selain itu, A dan B merupakan dua orang yang cukup ahli dalam bidang kriptografi, sehingga mereka khawatir bahwa ada orang yang akan melakukan kriptanalis, oleh karena itu, sebelum A mengirimkan pesan kepada B, ia memberitahu bahwa hasil verifikasi tanda tangan dijitalnya harus bernilai sesuatu (sebut saja ‘A03912FB’), kemudian B mencatat nomor tersebut untuk memastikan kevalidan pesan yang nantinya dikirim oleh A.

Isi pesan dari A kurang lebih sebagai berikut:

```
Dari: A
Untuk: B
File terlampir, silakan dibaca.
```

Dan isi pesannya, dalam bentuk berkas terenkripsi adalah sebagai berikut:

```
B, saya sangat butuh uang, tolong kirimkan Rp 10 juta ke rekening saya, nomor 192.168.1.10 bank XX cabang YY.
```

Kemudian C sebagai pihak ketiga, atau pihak penyadap mengetahui hal tersebut. C adalah orang yang cukup ahli dalam kriptografi, ia mampu memecahkan fungsi hash, akan tetapi ia mengetahui bahwa A telah mengirimkan hasil dekripsi kepada B, jadi ia tidak mungkin sembarang mengganti pesan seperti teknik pemecahan fungsi hash. Oleh karena itu ia menggunakan teknik kolisi pesan.

Pertama, ia mengganti pesan 192.168.1.10 menjadi 202.134.2.5, nomor rekening yang ia punya, bank WW cabang ZZ, dan menambah jumlah uangnya menjadi 100 juta rupiah. Akan tetapi ia tahu bahwa hasil hash-nya tidak sama dengan yang diberitahukan oleh A kepada B, oleh karena itu, ia mengakal-akali dengan menambahkan beberapa karakter di akhir pesan untuk B tersebut, agar hasilnya merupakan kolisi dari pesan yang sebelumnya, atau yang seharusnya dikirimkan oleh A kepada B.

Email yang dikirim ulang dari C kepada B adalah sebagai berikut:

```
Dari: A
Untuk: B
File terlampir, di bagian bawah file terdapat beberapa error, abaikan saja. Komputer saya memang agak bermasalah. Terima kasih.
```

Dan isi pesannya pun berubah menjadi sebagai berikut:

```
B, saya sangat butuh uang, tolong kirimkan Rp 100 juta ke rekening saya, 202.134.2.5, bank WW cabang ZZ.


@!apT#%0=\W^B SG/?]@
```

B, sebagai orang yang menerima pesan tersebut, meskipun timbul sedikit kecurigaan terhadap A, terutama karena di akhir pesan banyak karakter aneh, mempercayai saja apa yang dianggapnya dikatakan oleh A. Di balik itu semua, ia tidak mengetahui bahwa karakter-karakter aneh di akhir

file yang dikirimkan C (yang diaku sebagai A), adalah teknik untuk mengkolisikan pesan yang seharusnya dikirimkan oleh A kepada B dengan pesan yang dikirim C kepada B atas nama A. Dengan demikian, B dan A sudah tertipu oleh C, dan B hanya melakukan apa yang diminta oleh pengirim yang ia kira A.

Teknik ini jelas jauh lebih efektif, akan tetapi dapat dikatakan bahwa teknik ini jauh lebih rumit daripada teknik pemecahan kode hash, karena bagaimanapun juga, mencari kolisi terhadap suatu dokumen itu sangat sulit. Memang bahwa suatu data atau dokumen berkolisi dengan tak berhingga banyaknya data atau dokumen yang lain, akan tetapi mencari tak berhingga data atau dokumen yang lain tersebut sangatlah sulit.

4. PENANGGULANGAN KELEMAHAN FUNGSI HASH

Untuk menangani permasalahan ini, baik pihak pengirim maupun pihak penerima sudah seharusnya mengantisipasi hal tersebut dari awal.

Untuk menangani masalah pemecahan fungsi hash, yang dianggap cukup sulit dipecahkan ini, harus dibuat sebuah fungsi hash yang jauh lebih rumit, dengan tingkat kesulitan pemecahannya yang jauh lebih tinggi, serta jika perlu, hasil fungsi hash-nya jauh lebih panjang, misalnya 1024 bit, 2048 bit, atau 8192 bit.

Untuk permasalahan serangan dengan penggunaan kolisi, salah satu cara yang digunakan adalah, pihak pengirim juga harus memberitahukan jumlah karakter yang ia kirim dalam sebuah file, jadi perubahan sekecil apapun akan sangat sulit dilakukan oleh pihak kriptanalis. Karena jika kita lihat lagi contoh pemanfaatan yang dilakukan oleh C terhadap A melalui pesan palsu yang ia kirim kepada B, jelas terlihat bahwa panjang pesan asli berbeda dengan panjang pesan palsu, sehingga pemalsuan pesan yang dilakukan oleh C tidak lagi dapat dilakukan.

Teknik lain untuk mengamankan pesan, yang serupa dengan teknik pengamanan pesan pada permasalahan pemecahan fungsi hash adalah dengan menambahkan jumlah dijit hasil fungsi hash, semakin banyak fungsi hash yang mungkin dihasilkan dari suatu data atau dokumen, akan semakin sulit menemukan data atau dokumen yang berkolisi dengan data tersebut. Tentunya juga, untuk menemukan kolisinya akan menghabiskan waktu yang lebih lama. Hal ini dapat dimanfaatkan oleh pengirim pesan dengan teknik lainnya.

Misalnya, A pada kasus kolisi tersebut mengatakan kepada B, “B, pesan ini seharusnya sudah sampai kepadamu paling lama dalam waktu lima menit, jika pesan sampai dalam waktu lebih dari lima menit dari sekarang, abaikan pesan tersebut, karena dikhawatirkan pesan tersebut palsu”. Hal ini tentunya akan semakin menyulitkan kriptanalis yang berusaha membongkar pesan tersebut, karena selain panjang fungsi hash yang semakin panjang, yang berarti waktu yang dibutuhkan semakin lama, ia terjepit dalam situasi, ia harus memecahkan kode tersebut dalam waktu lebih cepat lagi.

5. ANALISIS PENANGGULANGAN KELEMAHAN FUNGSI HASH

Sekali lagi, seperti yang penulis tuliskan di bagian abstraksi, setiap ada kemajuan dalam teknik kriptografi, pasti ada kemajuan lagi dalam bidang pemecahan kode kriptografi tersebut, kriptanalis pun tentunya sudah memiliki teknik yang lebih baik. Pada proses kriptanalisis yang membutuhkan waktu sangat cepat, kriptanalis mungkin saja memprosesnya dengan menggunakan beberapa komputer sekaligus, sehingga permasalahan waktu bukan lagi permasalahan yang krusial bagi mereka. Karena setiap makin lambat proses, makin banyak komputer yang digunakan, dan untuk pemecahan kode yang sangat rumit yang mungkin menghasilkan keuntungan yang sangat besar, hal tersebut tentunya bukanlah masalah yang cukup besar bagi kriptanalis.

Selain itu, pembuatan fungsi hash yang lebih baru, yang lebih rumit, yang lebih sulit dipecahkan juga tetap saja tidak mungkin terbebas dari kemungkinan penjebolan yang dilakukan kriptanalis, karena selama ada cara untuk mengenkripsi pesan, maka pasti akan selalu ada cara juga untuk mendekripsikan pesan terenkripsi tersebut.

Untuk mengatasi hal tersebut, ada dua cara yang terbaik:

1. Dalam setiap penyandian pesan yang dilakukan, seorang pengirim pesan ada baiknya mengenkripsi pesan dalam dua metode secara sekaligus. Pengenkripsian pesan menggunakan kunci privat digunakan agar penerima pesan dapat memastikan bahwa pengirim pesan adalah pengirim pesan yang benar. Kemudian untuk memastikan bahwa pesan tidak dapat terbaca sama sekali oleh orang lain selain penerima pesan yang seharusnya, pengirim pesan juga melakukan enkripsi dengan menggunakan kunci publik yang berbeda, agar tidak ada orang sama sekali yang dapat mengubah pesan yang ia kirimkan kepada penerima pesan.
2. Untuk komunikasi yang paling aman, ada baiknya pengirim pesan dan penerima pesan bertatap muka, teknik ini adalah

teknik yang paling sederhana dan paling kuno, akan tetapi tidak seorang pun dapat melakukan perubahan terhadap data yang akan diberikan oleh pengirim pesan kepada penerima pesan sama sekali.

6. KESIMPULAN

Dari permasalahan, teknik pemanfaatan permasalahan, teknik penanggulangan pemanfaatan permasalahan, dan analisis mengenai penanggulangan pemanfaatan permasalahan tersebut, fungsi hash dapat dikatakan sebagai fungsi yang cukup baik. Terutama untuk pengiriman pesan-pesan yang tidak terlalu krusial, karena bagaimanapun juga, selama ada teknik kriptografi, pasti akan selalu ada teknik kriptanalisisnya. Untuk memastikan semuanya aman, langkah terbaik adalah bertatap muka

DAFTAR REFERENSI

[1] R.Munir, *Diktat Kuliah IF5054 Kriptografi*, Program Studi Teknik Informatika Institut Teknologi Bandung, 2006.