Implementasi Whirlpool Hash dalam Digital Signature dan Perbandingannya dengan SHA-1

Darwin - 13508102
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
Dawn0689@aol.com

Abstrak*— Fungsi hash merupakan fungsi yang digunakan untuk mentransformasikan sebuah data atau file ke dalam sebuah bentuk message digest berukuran kecil. Message digest tersebut dapat digunakan untuk mengetahui originalitas dari file tersebut ataupun untuk mengetahui apakah file tersebut pernah ditambah, dikurangi atau diubah isinya. Salah satu contoh penggunaan hash adalah dalam digital signature. Whirlpool hash merupakan suatu fungsi hash yang dikembangkan oleh Vincent Rijmen (salah satu pengembang Advanced Encription System) dan Paulo S. L. M. Barreto pada awal tahun 2000. SHA-1 adalah sebuah fungsi hash yang dirancang oleh National Security Agency dan dipublikasikan oleh NIST. Digital Signature adalah suatu teknik dimana kita mengotentikasi isi dari suatu file atau pesan yang dikirimkan. Penggunaan tanda tangan digital ini haruslah unik dan juga variasi untuk setiap orang. Pada beberapa aplikasi sebelumnya, penggunaan digital signature menggunakan SHA-1. Akan dilakukan uji coba terhadap pengaplikasian whirlpool hash terhadap digital signature dan dibandingkan dengan hasil dari SHA-1. Apakah keamanan dari digital signature tersebut lebih baik, apakah waktu proses tersebut lebih cepat dan apakah tanda tangan yang dihasilkan bersifat lebih unik.

***Index Terms*—Whirlpool Hash, SHA-1, *Digital Signature*, otentikasi.**

I. PENDAHULUAN

Pada masa sekarang ini, sekuritas dan privasi dari suatu data yang dikirimkan merupakan hal yang sangat penting. Salah satu hal yang penting dalam sekuritas adalah bagaimana kita dapat mengetahui pesan yang kita kirimkan tersebut merupakan pesan yang otentik. Perubahan pesan tersebut dapat mengakibatkan hal yang cukup berbahaya terutama dalam hal-hal yang bersifat penting, misalnya adalah perubahan isi dari lokasi transfer yang dilakukan. Apabila pesan yang dikirimkan tersebut diubah rekening tujuan tersebut maka akan merugikan pihak lainnya. Oleh karena itu kita perlu menggunakan suatu teknik yang dinamakan dengan *Digital Signature*. *Digital Signature* merupakan suatu cara yang digunakan untuk menyisipkan hasil dari message digest dari suatu pesan ataupun file ke dalamnya. Hasil dari message digest tersebut kemudian dapat kita gunakan kembali untuk dilakukan pengecekan terhadp otentikasi dari file tersebut.

Hash merupakan suatu fungsi yang diugnakan untuk menghasilkan suatu message digest yang bersifat unik antara pesan atau file yang satu dengan yang lainnya. Hasil dari message digest tersebut akan bersifat unik untuk antara yang satu dengan yang lainnya. Perubahan isi dari pesan tersebut akan menghasilkan suatu message digest yang akan berbeda sama sekali. Perubahan tersebut meliputi merubah isi dari pesan tersebut, menambahkan isi pesan tersebut ataupun mengurangi isi dari pesan tersebut meskipun hanya sedikit. Penggunaan fungsi hash ini juga digunakan pada otentikasi sidik jari pengguna dalam fungsi biometrik, pengecekan apakah DNA tersebut merupakan milik dari seseorang dan juga pada umumnya digunakan untuk melakukan otentikasi terhadap isi dari password yang digunakan untuk melakukan login. Penggunaan dari hash ini juga dilakukan dalam jaringan yaitu dengan menambahkannya pada bagian checksum. Checksum tersebut dapat digunakan untuk membandingkan isi dari hasil kiriman apakah rusak, diubah atau tidak lengkap. Dari hasil tersebu, maka kita dapat mengetahui apakah kita perlu melakukan request untuk mengirimkan kembali data tersebut atau apakah data sudah bagus dan dapat digunakan.

Pada saat sekarang ini, hash sudah memiliki banyak jenis. Salah satu jenis hash yang paling terkenal adalah *Secure Hash Algorithm* atau sering juga disebut sebagai SHA. SHA sudah memilik beberapa jenis yaitu SHA-0, SHA-1, SHA-256/22 dan juga SHA-512/384. Fungsi hash lainnya yang cukup terkenal adalah MD5. Salah satu fungsi hash yang cukup baru dan akan dibahas pada makalah ini adalah *whirlpool hash*.

II. WHIRLPOOL HASH

Whirlpool merupakan fungsi hash yang didesain oleh Vicent Rijmen (co-crator dari Advanced Encription Standard) dan Paulo S. L. M. Barreto pada tahun 2000. Fungsi hash ini telah direkomendasikan oleh NESSIE (New European Schemes for Signatures, Integrity and Encryption) dan diadopsi oleh International Organization for Standardization (ISO) dan International Electrotechnical Comm sebagai bagian dari ISO/IEC 10118-3.

Whirlpool adalah sebuah hash yang didesain dengan menggunakan block cipher square. Whirlpool menggunakan konstruksi Miyaguchi-Preneel sebagai basis dari fungsi AES yang telah diubah sebelumnya. Whirlpool menerima sebuah pesan yang berukuran lebih kecil dari 2^{256} bits dan mengembalikan sebuah message digest dalam ukuran 512-bit. Whirlpool hash diklaim bahwa fungsi ini tidak akan dipatenkan dan boleh digunakan oleh public dengan tujuan apapun.

Algoritma ini dinamakan sesudah galaxy Whirlpool di Canes Venatici. Dua program yang pertama kali menggunakan Whirlpool sebagai basis dari kriptografi mereka adalah FreeOTFE diikuti oleh TrueCrypt pada tahun 2005.

Figure 1 Galaxy Whirlpool

III. DIGITAL SIGNATURE

Otentikasi terhadap suatu isi dari pesan yang akan dikirimkan merupakan hal yang telah dilakukan sejak zaman dahulu. Hal tersebut dilakukan untuk mengetahui apakah pesan yang dikirimkan tersebut merupakan pesan yang otentik atau bukan. Tanda tangan yang digunakan setiap orang berbeda-beda sehingga dapat diketahui apakah pesan tersebut benar.

Untuk segala dokumen atau pesan yang dikirimkan dalam bentuk fisik, kita dapat membuktikan apakah pesan tersebut merupakan hasil kiriman dari seseorang dengan melihat tanda-tangan yang diberikan pada dokumen ataupun pesan tersebut. Tetapi hal tersebut tidak dapat dilakukan pada data yang bersifat digital.

Salah satu cara yang dapat digunakan adalah dengan menggunakan sistematika *Digital Signature*. *Digital Signature* akan melakukan otentikasi dengan 2 tahap :

1. Pada pihak pengirim, dimasukkan tanda tangan digital dari hasil message digest yang dihasilkan dengan fungsi hash tersebut. Message digest tersebut kemudian dienkripsi sehingga menghasilkan suatu hasil tanda tangan digital yang telah terenkripsi. Enkripsi tersebut menggunakan sebuah kunci privat.
2. Setelah pesan tersebut berhasil disisipkan sebuah tanda tangan digital, maka pesan tersebut dapat dilakukan pengecekan oleh penerima dengan memasukkan sebuah kunci publik yang telah dikirimkan oleh pengirim pesan tersebut. Dekripsi dengan menggunakan kunci publik akan menghasilkan message digest yang dihasilkan oleh pengirim pesan tersebut. Penerima pesan cukup menghasilkan kembali message digest dari pesan tersebut. Pada saat melakukan perbandingan terhadap kedua message digest tersebut, dapat terjadi 2 hal yaitu :
   - Message digest tersebut berbeda sehingga diketahui bahwa pesan tersebut bukan asli dari pengirim pesan tersebut.
   - Message digest tersebut sama sehingga kita mengetahui bahwa pengirim pesan tersebut merupakan "dia" dan pesan tersebut asli.

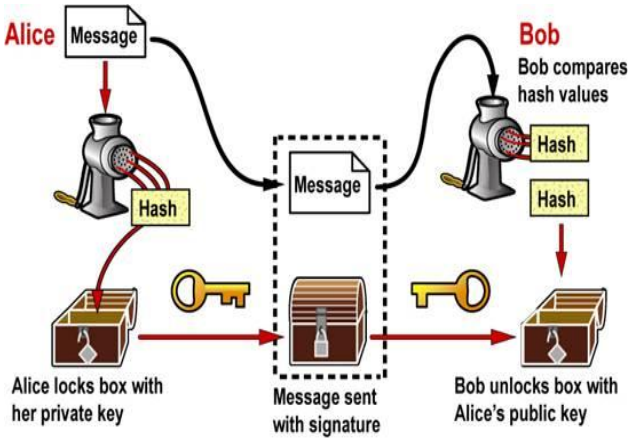


Figure 2 Digital Signature Authentication Process

Contoh skema hasil pencocokan kedua message digest yang digunakan untuk digital signature adalah sebagai berikut :

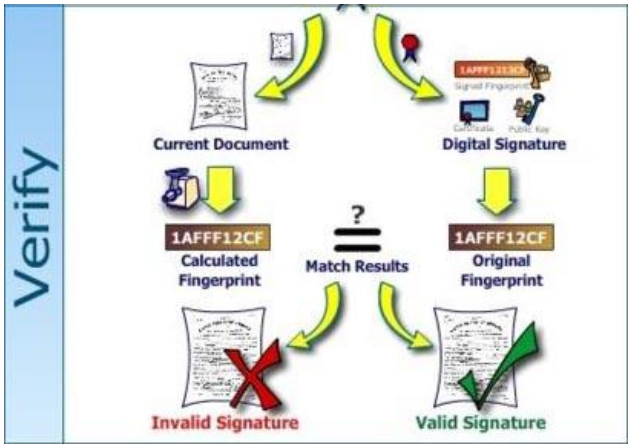


Figure 3 Digital Signature Verify

Pada makalah ini, akan dilakukan uji coba terhadap hash dengan menggunakan SHA-1 dan juga hash dengan menggunakan Whirlpool untuk mengetahui perbedaan hasil yang diperoleh. Untuk enkripsi yang digunakan, maka akan digunakan RSA sebagai kunci untuk menghasilkan hasil enkripsinya.

IV. IMPLEMENTASI WHIRLPOOL HASH

Pada bagian ini hanya akan dibahas mengenai bagaimana implementasi Whirlpool hash secara algoritmik. Hasil imlepmentasi dari Whirlpool hash tersebut akan diperjelas pada bagian selanjutnya yaitu pada saat pengujian ke dalam bentuk digital signature.

Primitif Whirlpool adalah sebuah fungsi hash Merkle yang berdasarkan pada sebuah blok cipher, W, yang beroperasi pada sebuah 512 data block yang mana block-block tersebut akan diturunkan lagi dari data masukan untuk menghasilkan message digest.

Berikut merupakan tahapan-tahapan dasar dalam pengimplementasian Whirlpool hash :

A. INPUT DAN OUTPUT

Suatu state dari hash dapat dilihat sebagai sebuah matriks yang berukuran $M_{8\times8}[GF(2^8)]$. Oleh karena itu, kita perlu memetakan seluruh blok data yang berukuran 512 bit tersebut ke dalam bentuk matriks tersebut. Proses ini dapat dilakukan dengan menggunakan fungsi μ : $GF(2^8)^{64} \rightarrow M^{8}\times^{8}[GF(2^8)]$ and inversnya adalah :

$$\mu(a) = b \leftrightarrow b_{ij} = a_{8i+j} , 0 \le i, j \le 7.$$

B. NON-LINEAR LAYER γ

Fungsi γ : $M_{8\times8}[GF(2^8)] \rightarrow M^{8}\times^{8}[GF(2^8)]$ terdiri aplikasi yang pararel terhadap sebuah substitusi non linear dalam bentuk S : $GF(2^8) \rightarrow GF(2^8)$, $x \rightarrow S[x]$ untuk seluruh byte yang ada dalam :

$$\gamma\ (a) = b \leftrightarrow b_{ij} = S[a_{ij}], 0 \le i, j \le 7$$

C. PERMUTASI SIKLIK π

Permutasi π : $M_{8\times8}[GF(2^8)] \rightarrow M^{8}\times^{8}[GF(2^8)]$ secara siklik berganti untuk setiap kolom sehingga kolom j terus bergerak turun sejauh j :

$$\pi\ (a) = b \leftrightarrow b_{ij} = a_{(i-j) \bmod 8,j} , 0 \le i, j \le 7.$$

D. DIFUSI LINEAR LAYER θ

Layer difusi θ : $M_{8\times8}[GF(2^8)] \rightarrow M^{8}\times^{8}[GF(2^8)]$ adalah sebuah pemetaan linear yang didasarkan pada kode MDS [16,8,9] dengan sebuah matriks generator Gc = [I C] dimana C = cir(01x, 01x, 04x, 01x, 08x, 05x, 02x, 09x) yang mana :

$$C = \begin{bmatrix} 01_x & 01_x & 04_x & 01_x & 08_x & 05_x & 02_x & 09_x \\ 09_x & 01_x & 01_x & 04_x & 01_x & 08_x & 05_x & 02_x \\ 02_x & 09_x & 01_x & 01_x & 04_x & 01_x & 08_x & 05_x \\ 05_x & 02_x & 09_x & 01_x & 01_x & 04_x & 01_x & 08_x \\ 08_x & 05_x & 02_x & 09_x & 01_x & 01_x & 04_x & 01_x \\ 01_x & 08_x & 05_x & 02_x & 09_x & 01_x & 01_x & 04_x \\ 04_x & 01_x & 08_x & 05_x & 02_x & 09_x & 01_x & 01_x \\ 01_x & 04_x & 01_x & 08_x & 05_x & 02_x & 09_x & 01_x \end{bmatrix}$$

Tujuan dari matriks ini adalah untuk mengacak byte-byte yang terdapat pada setiap baris.

E. KUNCI TAMBAHAN σ[k]

Kunci tambahan $\sigma[k]$: $M_{8\times8}[GF(2^8)] \rightarrow M^{8}\times^{8}[GF(2^8)]$ mengandung penambahan XOR dari sebuah matriks kunci $k \varepsilon M_{8\times8}[GF(2^8)]$:

$$\sigma[k](a) = b \leftrightarrow b_{ij} = a_{ij} \oplus k_{ij} , 0 \le i, j \le 7$$

F. PEMBULATAN KONSTAN c^r

Konstanta pembulatan pada putaran ke-r, r > 0,adalah matriks $c^r \varepsilon M_{8\times8}[GF(2^8)]$ yang didefinisikan sebagai :

$$\begin{aligned} c^r_{0j} &\equiv S[8(r-1)+j], 0 \leqslant j \leqslant 7, \\ c^r_{ij} &\equiv 0, \qquad\qquad 1 \leqslant i \leqslant 7, 0 \leqslant j \leqslant 7 \end{aligned}$$

G. PENJADWALAN KUNCI

Jadwal kunci tersebut dapat memperluas kunci 512 bit $K \varepsilon M_{8\times8}[GF(2^8)]$ ke dalam sekuens putaran K0, . . . ,KR:

$$K^0 = K,$$
$$K^r = \rho[c^r](K^{r-1}), r > 0$$

I. BLOCK CIPHER INTERNAL W

Block cipher 512-bit dengan W[K] : $M_{8\times8}[GF(2^8)] \rightarrow M^{8}\times^{8}[GF(2^8)]$ diparameterisasi dengan 512-bit cipher key K, didefinisikan dengan :

$$W[K] = \left(\bigcirc_{1}^{r=R} \rho[K^r] \right) \circ \sigma[K^0],$$

Dengan kunci putaran K0, …, KR yang diDengan kunci putaran K0, …, KR yang diperoleh dari K dengan jadwal kunci. Jumlah putaran standar yang digunakan adalah 10.

J. PADDING DAN PENGUATAN MD

Sebelum dilakukan hashing, sebuah pesan dengan bit dimana panjangnya $L < 2^{256}$ dilakukan padding dengan bit 1 kemduian degan beberapa bit 0 seperlunya. Banyaknya bit 0 tersebut disesuaikan dengan kelipatan dari 256 dan langkah terakhir yang dilakukan adalah dengan 256 bit yang telah jadi tersebut, dipartisi dalam t blok m1, …, mt. Blok-blok ini akan dipandang sebagai suatu kelompok byte yang mengandung 8-bit.

K.FUNGSI KOMPRESI

Whirlpool melakukan iterasi terhadap skema Miyaguchi-Preneel dalam pesan yang telah berhasil di padding tersebut menggunakan block cipher yang memiliki fungsi :

$$\eta_i = \mu(m_i),$$
$$H_0 = \mu(IV),$$
$$H_i = W[H_{i-1}](\eta_i) \oplus H_{i-1} \oplus \eta_i,\ 1 \leqslant i \leqslant t,$$

Dimana IV (Initial Vector) merupakan sebuah string yang mengandung 512-bit 0.

L.PENGHITUNGAN MESSAGE DIGEST

Pesan Whirlpool tersebut dihitungan dengan menggunakan sebuah pesan M yang mana keluaran Ht dari fungsi kompresi tersebut dilakukan pemetaan kembali ke sebuah string :

$$\text{WHIRLPOOL}(M) \equiv \mu^{-1}(Ht)$$

V. IMPLEMENTASI PROGRAM

A. IMPLEMENTASI WHIRLPOOL HASH

Program yang dibuat adalah program *Digital Signature* yang telah menggunakan fungsi hash dengan mengimplementasikan Whirlpool Hash. Setelah percobaan dengan menggunakan fungsi Whirlpool Hash tersebut, maka akan dibandingkan dengan menggunakan fungsi Hash SHA-1. Berikut adalah tampilan dari program yang akan digunakan.

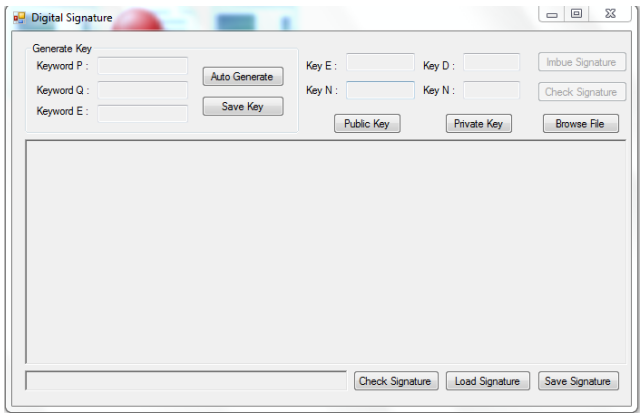


Figure 4 Tampilan Antarmuka Program

Akan dilakukan pemrosesan terhadap pesan yang sama dengan pesan yang digunakan adalah “This is just a test.”. Pesan tersebut akan diproses untuk menghasilkan suatu hash. Hash kemudian akan diproses dengan menggunakan kunci RSA dengan nilai 256-bit. Akan dilakukan analisis terhadap hasil yang diperoleh mengenai hasil yang digunakan tersebut.

Hasil dari whirlpool hash yang diperoleh pada “This is just a test.” :

fddda0d7eb5be3cd2542c5a36074bcb9f9d78bb2c725f15c7a6757201caa812b8d028fca9a83359d61fd28116bc8035eef44331e31859fa90669bf7e91bd5294

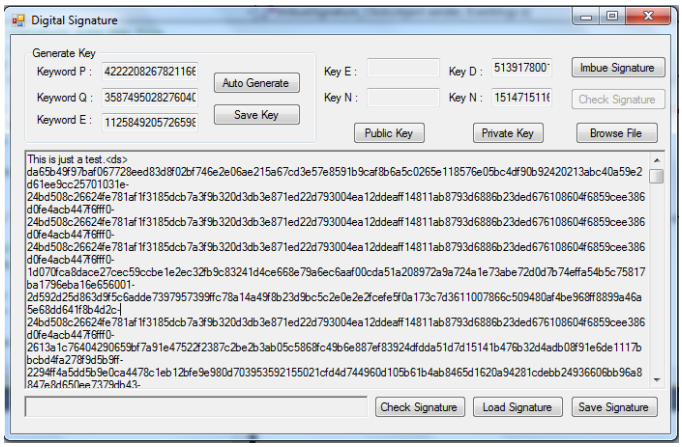


Figure 5 Tampilan hasil Whirlpool Hash

Dari hasil percobaan, diperoleh bahwa hasil dari teks tersebut memerlukan waktu sekitar 1,5 detik untuk melakukan proses terhadap proses tersebut dan proses tersebut memiliki tanda tangan digital yang sangat panjang. Hal yang menyebabkan tanda tangan digital yang sangat panjang adalah panjangnya kunci yang digunakan untuk melakukan enkripsi RSA dan juga panjangnya bit dari Whirlpool Hash.

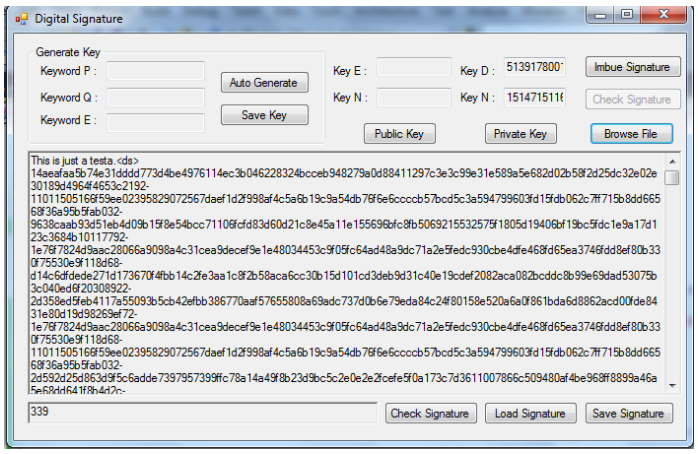


Figure 6 Tampilan hasil setelah penambahan huruf Whirlpool Hash

Percobaan lain juga membuktikan bahwa perbedaan isi sedikit saja menghasilkan suatu variasi hasil enkripsi yang sangat berbeda dengan sebelumnya.Hal ini menunjukkan bahwa keunikan yang dihasilkan sangat tinggi.

Hasil dari whirlpool hash yang diperoleh pada “This is just a testa.” :

b4198594032482ded46cdf3d494b3a18c0a98638763a67c68f78c408a6158cab20579ddb7570193d7010f6bcee764f35db1cc4bc2eb33d162fdb83b9ef1a9d80

Hasil yang diperoleh dari hasil enkripsi tersebut tentu saja juga akan memberikan hasil yang relatif berbeda

sesuai dengan hash yang dihasilkan oleh Whirlpool tersebut.

B. IMPLEMENTASI SHA-1 HASH

Pada bagian ini akan diberikan hasil-hasil percobaan yang dilakukan dengan menggunakan SHA-1 Hash. Tampilan yang digunakan memiliki model yang sama seperti pada penggunaan Whirlpool Hash. Yang berbeda hanyalah isi dari algoritma Hash yang digunakan.

Pengujian dilakukan terhadap pesan yang sama. Pesan "This is just a test." akan menghasilkan hash berikut : a292b6dafca8d0dc14a5a8cad70de12e640bbc92

Dengan menggunakan hash tersebut maka kita akan melakukan enkripsi dan digunakan sebagai sebuah digital signature. Berikut akan diberikan tampilan hasil implementasi dengan menggunakan kunci yang sama seperti pada contoh implementasi Whirlpool Hash :

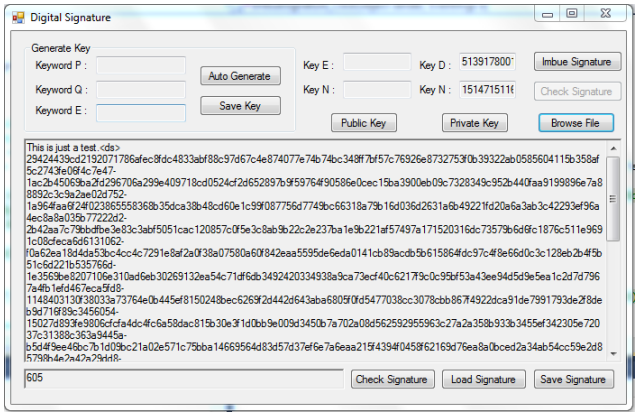


Figure 7 Tampilan hasil SHA-1 Hash

Dapat kita lihat melalui tampilan di atas bahwa pemrosesan dengan menggunakan SHA-1 lebih sedikit jika dibandingkan dengan Whirlpool Hash. Alhasil, maka waktu proses yang dibutuhkan juga lebih sedikit jika dibandingkan dengan proses yang dilakukan pada Whirlpool Hash. Waktu yang dibutuhkan untuk memproses hasil tersebut hanya sekitar 0,2 detik. Pengukuran tersebut dilakukan dengan menggunakan sebuah program lainnya yang berjalan secara bersamaan.

Selanjutnya dilakukan juga percobaan dengan melakukan perubahan terhadap isi dari teks tersebut sedikit. Hasil yang diperoleh dengan melakukan Hash pada teks "This is just a testa." : 1f574924bc86288bf9c63489b44f06fbe9bcaa01

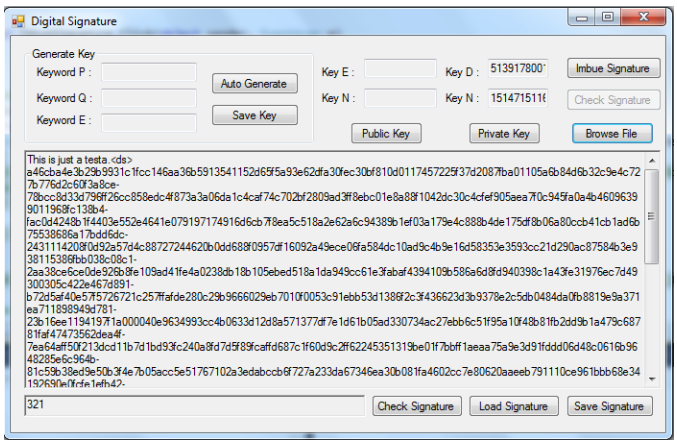


Figure 8 Tampilan setelah penambahan huruf SHA-1 Hash

Dengan menggunakan hasil hash yang baru tersebut maka kita juga memperoleh isi dari tanda tangan digital yang berbeda.

VI. ANALISIS

A. KEAMANAN WHIRLPOOL HASH DAN SHA-1 HASH

Dari hasil yang diperoleh diatas, kita melakukan perbandingan hasil yang diperoleh antara Whirlpool Hash dengan SHA-1 Hash dan diketahui bahwa penggunaan Whirlpool Hash sebagai hash lebih aman dibandingkan dengan SHA-1. Hal tersebut didukung juga dengan berbagai studi yang telah dilakukan terhadap SHA-1 dan berhasil dibuktikan bahwa SHA-1 memiliki kolisi sehingga kurang aman. Kolisi dapat menyebabkan 2 isi yang berbeda tetapi menghasilkan keluaran *message digest* yang sama. Pada SHA-1 dan Whirlpool Hash menggunakan 512-bit sebagai ukuran blok pesan. Untuk message digest yang dihasilkan, SHA-1 menghasilkan 160-bit sedangkan pada Whirlpool Hash menggunakan 512-bit.

Dari hasil keluaran message digest tersebut kita dapat melihat bahwa variasi yang dapat dihasilkan tentu saja lebih besar terdapat pada Whirlpool Hash dibandingkan dengan SHA-1 sehingga kolisi yang terjadi dapat diperkecil sampai dengan keadaan dimana kolisi tersebut tidak dapat terjadi. Tetapi apabila dengan menggunakan SHA-1 maka hasil dari Hash tersebut memiliki kemungkinan kolisi lebih besar. Dengan berkurangnya derajat kolisi yang dapat terjadi maka kemanan tersebut dapat terjaga dengan lebih baik.

B. WAKTU PROSES WHIRLPOOL HASH DAN SHA-1 HASH

Dari hasil ujicoba juga ditemukan bahwa proses terhadap Whirlpool Hash memerlukan waktu yang relatif lebih lama dibandingkan pada proses terhadap SHA-1. Hal tersebut disebabkan karena hasil message digest yang dikeluarkan pada Whirlpool jauh lebih besar dibandingkan dengan SHA-1.

Untuk pemrosesan pesan yang panjang, SHA-1 akan memiliki kecepatan yang jauh lebih cepat dibandingkan dengan Whirlpool Hash. Hal ini disebabkan karena SHA-

1 cukup menghasilkan 160-bit message digest. Untuk pesan yang cukup panjang pemrosesan dengan menggunakan Whirlpool akan memakan waktu yang cukup lama.

C. KEUNIKAN WHIRLPOOL HASH DAN SHA-1 HASH

Keunikan yang dihasilkan oleh Whirlpool Hash memiliki derajat yang lebih tinggi dibandingkan dengan menggunakan SHA-1. Hal tersebut didasari oleh besarnya message digest yang dihasilkan oleh Whirlpool Hash.

Derajat keunikan ini bertujuan untuk mengurangi kemungkinan terjadinya kolisi terhadap 2 isi file yang berbeda.

VII. KESIMPULAN

Dari seluruh hasil percobaan yang dilakukan pada makalah ini, maka dapat disimpulkan bahwa :

1. Tanda tangan digital dapat digunakan sebagai otentikasi terhadap isi dari pengirim. Apabila kita mendapatkan hasil yang berbeda dengan tanda tangan digital maka kita dapat mengetahui bahwa pesan tersebut tidak otentik.
2. Penggunaan Whirlpool Hash pada tanda tangan digital terutama dengan menggabungkannya dengan RSA akan menghasilkan derajat keamanan yang jauh lebih tinggi dibandingkan dengan menggunakan SHA-1.
3. Penggunaan Whirlpool Hash membutuhkan waktu proses yang lebih lama dibandingkan dengan menggunakan SHA-1. Hal tersebut dikarenakan Whirlpool Hash membutuhkan waktu proses yang lebih lama pada saat menghasilkan message digest dan juga melakukan enkripsi terhadap message digest terhadap pesan yang sangat panjang tersebut.
4. Whirlpool Hash memberikan sifat unik yang lebih baik dibandingkan dengan penggunaan SHA-1. Hal ini didasari oleh besarnya message digest yang diberikan.
5. Penggunaan Whirlpool Hash pada pesan yang pendek lebih baik karena pesan tesebut akan ditambahkan dengan jumlah byte yang relative besar. Penggunaan pada file yang memiliki ukuran yang besar akan menyebabkan ukuran file tersebut menggelembung dengan adanya tanda tangan digital dengan Whirlpool Hash.
6. Pelaksanaan kriptanalis terhadap tangan tangan digital yang dihasilkan sangatlah sukar untuk dilakukan karena kriptanalis harus mencari terhadap gabungan 512-bit karakter yang dihasilkan. Untuk setiap pesan tersebut juga dapat menghasilkan isi yang berbeda.

VIII. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih terutama kepada Tuhan Yang Maha Esa karena berkat anugerah yang diberikan-Nya makalah ini dapat diselesaikan. Penulis juga mengucapkan terima kasih kepada Bapak Ir. Rinaldi Munir, M.T. selaku dosen pengajar kuliah IF3051 Strategi Algoritma karena berkat kuliah yang diberikan dan buku diktat yang ditul` is oleh beliau makalah ini dapat disempurnakan.

REFERENCES

[1] http://en.wikipedia.org/wiki/Whirlpool_%28cryptography%29
Tanggal Akses : 1 May 2011.

[2] http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html
Tanggal Akses : 1 May 2011.

[3] http://www.cosic.esat.kuleuven.be/nessie/testvectors/hash/whirlpool/index.html
Tanggal Akses : 1 May 2011.

[4] T. Shirai, “On the diffusion matrix employed in the Whirlpool hashing function“
http://www.cosic.esat.kuleuven.be/nessie/reports/phase2/whirlpool-20030311.pdf
Tanggal akses : 1 May 2011.

[5] D. Kotturi, Y. Seong-Moo, “High-Speed Parallel Architecture of the Whirlpool Hash Function”
http://www.sersc.org/journals/IJAST/vol7/3.pdf
Tanggal akses : 1 May 2011.

[6] P. Barreto, V. Rijmen, “The Whirlpool Hashing Function”, 2003
http://saluc.engr.uconn.edu/refs/algorithms/hashalg/barreto00whirlpool.pdf
Tanggal akses : 1 May 2011.

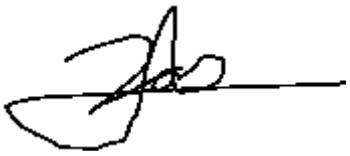
[7] Cryptographic Hash Algorithm.
http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
Tanggal akses : 5 May 2011.

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, 7 Mei 2011

ttd



Darwin -13508102