Analisis dan Perbandingan Algoritma Whirlpool dan SHA-512 sebagai Fungsi Hash

Willy Setiawan - 13508043
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18043@students.if.itb.ac.id

Abstrak— **Fungsi hash merupakan fungsi satu arah yang mengubah sekumpulan string menjadi sekumpulan string yang ukurannya lebih kecil daripada ukuran semula. Fungsi hash memiliki banyak kegunaan, seperti untuk menjaga integritas data, menghemat waktu pengiriman, serta untuk menormalkan panjang data yang beraneka ragam. Aplikasi pada dunia nyata dari fungsi hash bermacam-macam, seperti digunakan untuk mengecek suatu keabsahan data, untuk menyimpan kata kunci pada basis data, dan masih banyak lagi. Pada makalah ini akan dibahas mengenai 2 buah fungsi hash yang ada, yaitu fungsi hash SHA-512, serta fungsi hash whirlpool. SHA-512 merupakan varian dari SHA-2 yang didesain oleh National Security Agency (NSA), sedangkan algoritma hash Whirlpool dikembangkan oleh 2 orang, Vincent Rijmen dan Paulo S.L.M. Barreto. Kedua fungsi hash ini adalah fungsi hash yang dinilai memiliki keamanan yang tinggi. Pada kedua algoritma hash ini, masih belum ditemukannya adanya kolisi pada nilai hash. Makalah ini juga akan membahas perbedaan dari kedua algoritma tersebut, serta seberapa kuat nilai hash yang diberikan jika diimplementasikan sebagai kata kunci.**

***Kata Kunci*— fungsi hash , SHA-512, whirlpool**

I. PENDAHULUAN

Pada jaman digital seperti sekarang ini, informasi adalah hal yang berharga. Oleh karena itu, diperlukanlah teknik-teknik untuk mengamankan suatu informasi. Ilmu yang mempelajari bagaimana menjaga kerahasiaan informasi disebut juga dengan kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Kriptografi muncul karena adanya usaha untuk mendapatkan informasi pesan oleh pihak yang sebenarnya tidak berhak untuk mendapatkan pesan tersebut.

Terdapat empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi,yaitu:

1. Kerahasiaan
   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
   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 pensubstitusian data lain ke dalam data yang sebenarnya.
3. Autentikasi
   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.
4. Non-repudiasi
   Usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/ terciptanya suatu informasi oleh yang mengirimkan/membuat.

Fungsi hash merupakan salah satu bagian dari kriptografi. Fungsi hash adalah fungsi yang dapat memberikan nilai terhadap data masukan. Fungsi hash menerima masukan string yang panjangnya sembarang, kemudian mentransformasikannya menjadi string keluaran yang panjangnya tetap (umumnya berukuran jauh lebih kecil daripada ukuran semula). String keluaran tersebut disebut juga dengan nilai hash. Umumnya, fungsi hash ini digunakan untuk keperluan autentikasi dan integritas data.

Ada 2 jenis fungsi hash yang akan dibahas pada makalah ini. Yang pertama adalah fungsi hash SHA-512. Fungsi hash SHA-512 merupakan variasi dari SHA-2. SHA-2 adalah perkembangan dari fungsi SHA-1. Yang menjadikannya perbedaan adalah ukuran blok yang dipakai. Fungsi hash SHA-2 didesain oleh National Security Agency (NSA) dan dipublikasikan oleh NIST. Hal yang melatarbelakangi fungsi hash SHA-2 adalah karena SHA-1 sudah tidak aman lagi. Sehingga, diperlukan sebuah algoritma hash baru yang lebih kuat. Walaupun desainnya mirip dengan SHA-1, tetapi berbagai serangan tidak dapat dilancarkan pada SHA-2 ini.

Fungsi hash kedua yang akan dibahas adalah fungsi hash whirlpool. Whirlpool adalah sebuah fungsi hash kriptografik yang didesain oleh Vincent Rijmen dan Paulo S. L. M. Barreto pada tahun 2000. Hash ini juga direkomendasikan oleh project NESSIE. Dan juga, hash ini diadaptasi oleh International Standard Organization

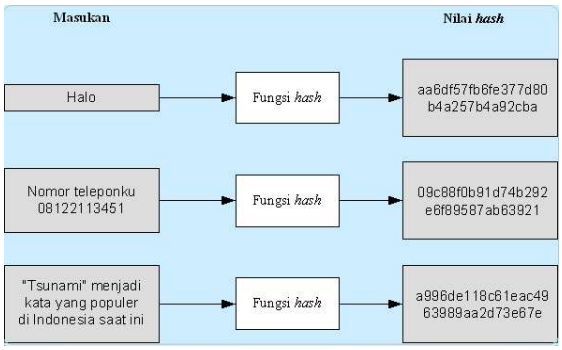
dan International Electrotechnical Commision (IEC) sebagai bagian dari ISO/IEC 10118-3 standard.

II. PEMBAHASAN

A.Fungsi Hash

Fungsi hash adalah fungsi yang menerima masukan berupa string yang panjangnya sembarang dan memberikan nilai berupa suatu string yang memiliki ukuran panjang yang tetap. Fungsi yang dilakukan pada fungsi hash disebut juga sebagai fungsi kompresi. Berbeda dengan fungsi kompresi biasa (seperti pada file zip), fungsi hash tidak bisa mendekompresi file hasil hash yang telah dilakukan. Dengan kata lain, kompresi yang dilakukan adalah kompresi satu arah.

Dalam kriptografi, fungsi hash harus memiliki 2 properti untuk dapat berguna : mereka harus satu arah dan harus kebal terhadap kolisi. Satu arah mengartikan bahwa keluaran dari fungsi hash, mempelajari sesuatu yang berguna tentang masukan adalah tidak mungkin. Hal ini adalah bagian penting dari hash, karena mereka sering digunakan bersamaan dengan data seed RNG dan user password. Kebal terhadap kolisi mengartikan bahwa jika diberikan suatu keluaran dari hash, mencari input lain yang menghasilkan output yang sama adalah tidak mungkin.



Gambar 1. Contoh fungsi hash

Selama bertahun-tahun, terdapat beberapa proposal untuk fungsi hash yang aman. Contoh-contoh yang ada seperti MD4, MD5,atau HAVAL. Tetapi, kebanyakan dari algoritma lama tersebut sudah ditemukan kolisinya.

SHA-1 adalah fungsi hash pertama yang ditawarkan oleh NIST. SHA-1 merupakan perbaikan dari SHA-0. SHA-1 adalah fungsi hash 160 bit, yang mengartikan bahwa keluarannya, atau yang disebut juga *digest*, memiliki panjang 160bit. SHA-1 masih aman untuk digunakan, tetapi orang dapat juga menggunakan algoritma SHA-2.

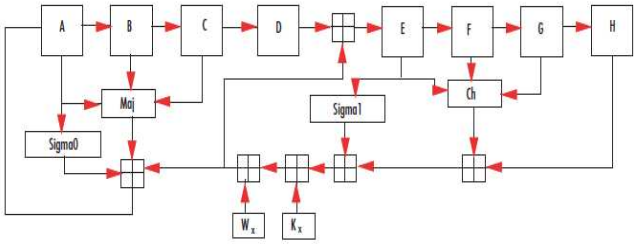
SHA-2 adalah nama informal untuk algoritma SHS putaran kedua yang didesain oleh NIST. Termasuk juga SHA-224, SHA-256, SHA-384, dan SHA-512. Nilai 224,256,384,atau 512 menyatakan panjang digest yang dikeluarkan. Rekomendasi yang didapatkan adalah setidaknya menggunakan SHA-256 sebagai algoritma hash standard.

B.Algoritma SHA-512

Fungsi yang terjadi pada algoritma SHA-2 mirip dengan yang terjadi pada SHA-1. Proses yang terjadi pada SHA-512 adalah :

+ Sebelum pemrosesan
- Mengubah string masukan menjadi kumpulan bit 0 dan 1
- Penambahan bit ‘1’ ke pesan
- Penambahan *k* bit ‘0’,dimana k adalah nilai minimum > = 0 sehingga pesan yang memiliki kelipatan 1024 bit
- Tambahkan panjang pesan, dalam bit, sebagai 64-bit integer.

+ Pada saat pemrosesan
- Memiliki 8 buah penyangga yang berukuran 64 bit
- Memiliki 80 buah konstanta yang berukuran 64 bit
- Bagi kumpulan bit setiap 1024 bit
- Pada tiap kumpulan 1024 bit tersebut, bagi tiap bit tersebut menjadi 16 bagian
- Perpanjang jadi 80 bagian, dengan menggunakan fungsi Gamma0 dan Gamma1
- Operasi yang terjadi pada tiap putaran adalah :



Gambar 2. Operasi fungsi hash SHA-2

Nilai A sampai H adalah 8 buah penyangga yang telah ditentukan sebelumnya. Fungsi Maj yang ada pada gambar diatas adalah fungsi yang menerima 3 buah variabel dengan aturan melakukan operasi : (((A ∨ B) ∧ C) ∨ (A ∧ B)).

Sedangkan fungsi Sigma0 adalah fungsi yang melakukan operasi : (ROR (x,28) ⊕ ROR (x,34) ⊕ ROR (x,39)). Yang dimaksud dengan ROR adalah rotasi bit yang ada ke kanan. Sehingga, yang terjadi pada fungsi Sigma0 adalah rotasikan x ke kanan sebanyak 2 kali , kemudian dilakukan operasi xor dengan x yang dirotasi ke kanan sebanyak 13 kali dan xor dengan x yang dirotasi kanan sebanyak 22 kali. Fungsi Sigma1 juga memiliki operasi yang mirip, yaitu : (ROR (x,14) ⊕ ROR (x,18) ⊕ ROR (x,41)).

Fungsi Gamma0 dan Gamma1 adalah fungsi yang dilakukan untuk memperbanyak jumlah potongan pada tiap bagian menjadi 80 bagian dari 16 bagian. Fungsi ini mirip dengan fungsi sebelumnya, yaitu fungsi Sigma0 dan Sigma1.Fungsi Gamma0 memiliki persamaan (ROR (x,1) ⊕ ROR (x,8) ⊕ R (x,7)). Fungsi R berbeda dengan fungsi rotasi kanan. Fungsi R merupakan fungsi untuk melakukan shift bit ke kanan sebanyak yang telah ditentukan. Sedangkan, fungsi Gamma1 memiliki persamaan (ROR (x,19) ⊕ ROR (x,61) ⊕ R (x,6)).

Pada gambar terlihat ada W_x dan K_x. Yang dimaksud dengan nilai K_x adalah nilai konstanta yang telah ditentukan pada tiap putaran. Sedangkan, nilai W_x adalah nilai dari tulisan yang akan di-*hash* yang sudah ditambah bitnya dan diperpanjang ukurannya sampai 80 buah potongan. Untuk mendapatkan nilai W ke 16 sampai dengan 79 (jika nilai W pertama adalah nilai W ke 0), operasi yang dilakukan adalah melakukan operasi penambahan antara Gamma1 dari W[i-2] dengan W[i-7] dan juga ditambah dengan hasil penjumlahan antara Gamma0 dari W[i-15] dan W[i-16]

Kemudian, terdapat juga fungsi Ch. Fungsi ini melakukan operasi (G ⊕ (E ∧ (F ⊕ G))). Setelah melakukan operasi-operasi yang ada, nilai selanjutnya dapat ditentukan. Penentuan nilai selanjutnya dilakukan dari H sampai ke A. Nilai H ditentukan dari nilai G, nilai G ditentukan dari nilai F, nilai F ditentukan dari nilai E, nilai E ditentukan dari penjumlahan dari D dan operasi penjumlahan, nilai D ditentukan dari nilai C, nilai C ditentukan dari nilai B,nilai B ditentukan dari nilai A,dan nilai A diperoleh dari penjumlahan.

Fungsi hash diperoleh dengan menggabungkan nilai-nilai hasil penjumlahan sebelumnya. Fungsi hash SHA-512 melakukan operasi hash yang sama dengan operasi SHA-2 pada umumnya. Yang menjadi perbedaan dengan algoritma hash SHA-2 yang lainnya adalah angkanya memiliki panjang 64 bit, sedangkan SHA-256 hanya memiliki panjang 32 bit. Selain itu, pada SHA-512 terdapat 80 buah putaran, sedangkan SHA-256 hanya memiliki 64 putaran. Pada SHA-512, nilai 8 buah penyangganya dan konstanta penambahnya diperpanjang mencapai 64 bit. Operasi shift dan rotasi yang dilakukan pada SHA-512 juga berbeda.

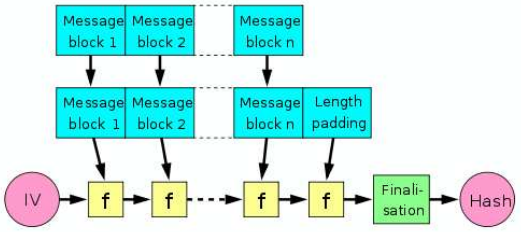
C. Algoritma Hash Whirlpool

Whirlpool adalah fungsi hash yang didesain oleh Vincent Rijmen dan Paulo S. L. M. Barreto yang beroperasi pada pesan yang memiliki ukuran kurang dari 2^{256} bit, dan menghasilkan message digest berukuran 512 bit. Whirlpool memiliki 3 buah versi. Versi pertama, Whirlpool-0 diajukan ke proyek NESSIE. Versi selanjutnya, yaitu Whirlpool-T, yang merupakan perbaikan dari versi sebelumnya, dipilih sebagai portfolio NESSIE untuk primitive kriptografik.Kesalahan pada diffusion layer dikemukakan oleh Shirai dan Shibutani dan kemudian diperbaiki lagi, dan versi finalnya (yang disebut juga sebagai Whirlpool) diadopsi oleh International Organization for Standardization (ISO) pada standard ISO/IEC 10118-3:2004.

Whirlpool menggunakan penguatan Merkle-Damgård dan skema hash Miyaguchi-Preenel dengan blok berukuran 512 bit yang disebut W. Cara kerjanya adalah sebagai berikut :

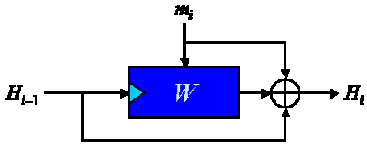
1. String dari bit yang akan di-hash di padding dengan bit ‘1’
2. Lakukan padding dengan kumpualn bit ‘0’.
3. Kemudian, lakukan padding dengan nilai bit dari panjang pesan semula, sehingga panjang pesan setelah di padding merupakan kelipatan 512 bit.
4. Pesan hasil dibagi-bagi menjadi kumpulan $m_1,m_2,\ldots,m_t$ yang kemudian akan digunakan untuk membangkitkan nilai hash $H_0,H_1,H_2,\ldots,H_t$. Nilai H_0 adalah string dari 512 buah bit ‘0’. Untuk menghitung H_i, W melakukan enkripsi m_i dengan menggunakan H_{i-1} sebagai kunci, dan melakukan XOR dari cipherteks yang dihasilkan dengan H_{i-1} dan m_i. Nilai dari hash adalah H_t.

Skema Merkle-Damgård adalah salah satu metode untuk membangun fungsi hash kriptografik yang tahan terhadap kolisi. Inti dari penggunaan skema ini adalah membagi pesan menjadi kumpulan blok yang memiliki ukuran tertentu, kemudian memrosesnya per blok.



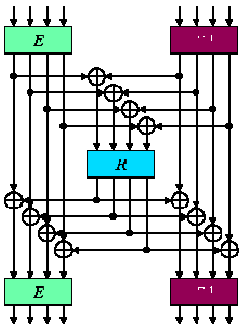
Gambar 3. Skema Merkle-Damgård

Sedangkan, skema Miyaguchi-Preneel adalah skema yang digunakan untuk mendapatkan nilai hash, pada kasus algoritma Whirlpool ini adalah cara untuk memperoleh nilai H_i sampai H_t.



Gambar 4. Skema hash dengan Miyaguchi-Preenel

Blok cipher W yang digunakan oleh Whirlpool mirip dengan algoritma AES, Rijndael. Perbedaannya dapat dilihat pada Tabel 1.



Gambar 5. Struktrur rekursif dari S-box

	Rijndael	W
Ukuran blok (bit)	128 , 160, 192 , 224 , atau 256	selalu 512
Banyaknya putaran	10, 11 , 12 ,13, atau 14	selalu 10
Penjadwalan kunci	Algoritma prioritas	Fungsi putaran sendiri
Reduksi polinomial GF (2^8)	$x^8 + x^4 + x^3 + x + 1$ (0x11B)	$x^8 + x^4 + x^3 + x^2 + 1$ (0x11D)
Asal S-Box	Pemetaan u -> u^{-1} ditambah fungsi affinitas	struktur rekursif
Asal konstanta putaran	polynomial x^i diatas GF (2^8)	Masukan dari S-box
Diffusion layer	Perkalian kiri dengan matriks 4x4 circulant MDS	Perkalian kanan oleh matriks 8x8 MDS circulant

Tabel 1. Perbedaan Cipherteks Rijndael dan Whirlpool

S-Box yang dimiliki W, yang pada awalnya dibangkitkan secara acak (tidak memiliki struktur internal), oleh sebuah struktur rekursif: kotak substitusi 8x8 yang dibentuk dari mini box berukuran 4x4. Gambar dari struktur S-box dapat dilihat pada Gambar 5.

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E(u)$	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

Gambar 6. Isi dari mini-box E

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E^{-1}(u)$	F	0	D	7	B	E	5	A	9	2	C	1	3	4	8	6

Gambar 7. Isi dari mini-box E^{-1}

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$R(u)$	7	C	B	D	E	4	9	F	6	3	8	A	2	5	1	0

Gambar 8. Isi dari mini-box R

III. IMPLEMENTASI

Pada bab ini akan membahas mengenai implementasi terhadap kedua algoritma ini. Implementasi dari algoritma menggunakan Java.

Implementasi algoritma hash SHA-512 menggunakan kelas Message Digest yang ada pada library java.security, sedangkan implementasi dari hash Whirlpool menggunakan library dari gnu.crypto.hash.Whirlpool. Implementasi dari Whirlpool yang dipakai adalah Whirlpool-T. Hasil dari nilai hash tersebut berupa kumpulan heksadesimal yang memiliki panjang 128 byte.

Aplikasi yang dibuat cukup sederhana. Pengguna memasukkan string yang akan dicek nilai hashnya. Lalu dengan menekan tombol hash, maka pengguna dapat melihat nilai hash yang dihasilkan oleh kedua algoritma tersebut.

Gambar 9. Tampilan Program Hash

Gambar 10. Tampilan Ketika Melakukan Pemrosesan

Pada Gambar 9, terlihat bahwa pengguna hanya bisa memasukkan teks yang berasal dari masukan papan kunci, atau hasil copy paste dari dokumen yang ada. Sedangkan, pada Gambar 10, terlihat bahwa pengguna dapat melihat hasil hash SHA-512 dan hash Whirlpool-T dari teks yang dimasukkan oleh pengguna, beserta memory yang dipakai untuk melakukan pemrosesan tersebut. Untuk mencari nilai hash, pengguna cukup menekan tombol hash yang

ada di program.

Akan dilakukan percobaan untuk melakukan hash terhadap beberapa buah teks, dan akan dilakukan percobaan tentang kekuatan nilai hash yang digunakan sebagai kata kunci. Pengujian terhadap kata kunci dilakukan, karena nilai hash sering digunakan untuk menyimpan kata kunci pada server website.

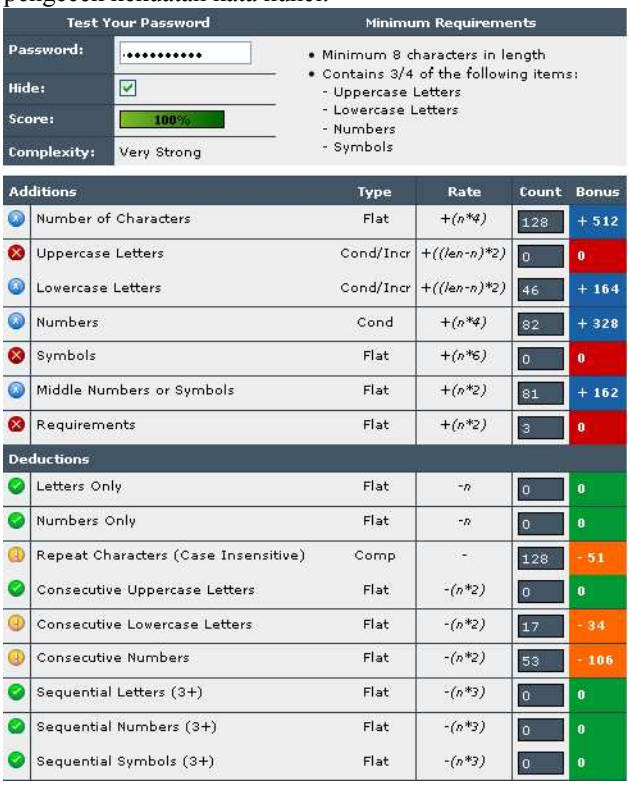
Teks pertama yang akan dicoba adalah : "udin pergi ke pasar". Nilai hash SHA-512 nya adalah f6a639cf4a78c837bda76a201c0aac0068960a0748cd9712988cbbc982416b64695218b226e5ba042bba4b6bb0105b411de3f610d512fcbe733d3e8d30f9e674. Sedangkan, nilai hash whirlpoolnya adalah 593653cd9d145af4316a971c0d8f14623bb65ebf3c5038da3ad415c87565601f91a214fc2931b775f9171cc2c3e96ca64e59912e34d12c9c3c51dbfcfeb23fab. Memori yang dibutuhkan untuk melakukan pemrosesan dengan SHA-512 adalah 651.928 byte, sedangkan dengan melakukan hash whirlpool membutuhkan 741.200 byte.

Teks kedua yang akan dicoba adalah dengan mengubah 1 buah kata pada teks pertama menjadi "udinpergi ke pasar". Nilai hash dengan metode SHA-512 adalah 9ae7642aeda3e993a5d4f1ba08452261aa5b51697e36f864972c8249edd6432a704c46e4f31c23d90742db3e59a243559e10d08f71bcdde5642447a36f322c54. Sedangkan nilai dari hash menggunakan Whirlpool adalah 7b8d4306348f370fad650f4d0b8a20e20e80d12eabeb84f3f6a455a17cf65a1dddff7ef90ed8e4afcafb70da33240e866c99a68f2ae8702cf6da3d2191608305. Memori yang dibutuhkan untuk melakukan hash dengan SHA-512 adalah 629.256 byte, sedangkan memori yang dibutuhkan untuk melakukan hash dengan Whirlpool adalah 674.352 byte.

Gambar 11. Contoh pemrosesan pada teks kedua

Teks ketiga yang akan dicoba adalah teks yang mirip dengan teks pertama, tetapi ada pengubahan pada teks yang dimasukkan. Teks yang akan dicoba adalah "udin pergi ke pasal". Nilai hash SHA-512 adalah 208c7823c52c74dab26a21d2a382727b3fdd0caa6a2379dcf4371335947379cf944aaec8fd4880993c304238ca7ce4f77e4d564569d1cf8ae68db598e0b99951. Sedangkan, nilai hash dengan menggunakan hash Whirlpool adalah df67b5d0e1791b225960e3b74a1b228314f736264dfb23a1bc6f8a5aa08ef14c2d6041d3d00ebfc315e17a0c1cb0ad925bbb20b5e8939ff5cb41ed21f9fe386a. Memori yang digunakan untuk melakukan hash dengan SHA-512 adalah 646.368 byte, sedangkan dengan Whirlpool membutuhkan 691.496 byte.

Untuk melakukan pengecekan kekuatan nilai hash sebagai kata kunci, akan dilakukan pengecekan kekuatan kata kunci berdasarkan atribut-atribut tertentu. Pengecekkan dilakukan dengan menggunakan website pengecek kekuatan kata kunci.



Gambar 12. Hasil pengecekan kekuatan kata kunci

Penghitungan kekuatan kata kunci dihitung berdasarkan total dari nilai tambah dan nilai kurang dari kata kunci yang digunakan, yaitu total nilai yang berada pada bagian Additions dikurangi dengan total nilai dari Deductions.

Dengan menggunakan hash SHA-512, nilai kata kunci yang diperoleh dari hash untuk masing-masing teks yang sudah dicek adalah 975, 931, dan 810 (secara berurutan: teks 1,teks 2, dan teks 3). Nilai rata-ratanya adalah 905

Sedangkan, untuk algoritma hash Whirlpool, nilai dari hash terhadap tiap teks adalah 920, 876, 962. Nilai rata-ratanya adalah 919.

IV. ANALISIS

Jika dilihat dari struktur algoritma hash yang dipakai, terdapat beberapa persamaan yang dapat dilihat dari algoritma hash dengan menggunakan SHA-512 dan Whirlpool. Pertama, nilai hash yang dihasilkan sama-sama berukuran 512 bit. Hasil hash yang memiliki panjang 512 bit juga memberikan perlindungan yang lebih baik terhadap birthday attack. Selain itu, keduanya menggunakan metode pemrosesan tiap blok data, atau yang disebut juga konstruksi Merkle–Damgård. Konstruksi ini sering dipakai pada algoritma hash yang popular dan terbukti dapat menciptakan algoritma yang tahan terhadap serangan jika menggunakan fungsi kompresi yang tepat.

Perbedaan dari masing-masing algoritma dari segi struktur yang digunakan adalah pada algoritma SHA-512 hanya menggunakan operasi-operasi standard seperti shift kanan dan rotasi bit ke kanan. Dan juga, operasi yang dilakukan pada SHA-512 ini mirip dengan apa yang dilakukan pada SHA-1. Sedangkan, pada algoritma hash Whirlpool menggunakan algoritma pemrosesan yang lebih bersifat matematis. Hash Whirlpool menggunakan penjadwalan kunci, S-box, serta diffusion layer untuk melakukan pemrosesan fungsi hash nya. Selain itu juga, hash Whirlpool menggunakan skema Miyaguchi-Preneel. Skema ini adalah skema sederhana yang Yang menjadi kekurangan pada algoritma hash Whirlpool adalah jumlah putarannya yang berjumlah 10, sedangkan hash SHA-512 memiliki 80 putaran.

Kedua metode memberikan nilai hash yang baik. Keduanya memberikan hasil yang benar-benar berbeda jika terjadi pengurangan kata atau perubahan kata sebanyak 1 huruf saja.

Dari segi memori yang dipakai, algoritma hash dengan SHA-512 menggunakan memori yang lebih sedikit daripada hash Whirlpool. Tetapi, perbedaan memori yang dipakai tidak cukup berbeda jauh. Perbedaan memori yang digunakan berkisar antara 50.000 byte sampai 100.000 byte. Perbedaan yang tidak terlalu besar ini tidak memberikan perbedaan performansi yang signifikan jika ingin diimplementasikan pada hardware.

Dilihat dari kekuatan hash jika digunakan sebagai kata kunci, algoritma Whirlpool lebih baik dari segi rata-rata point yang diperoleh. Tetapi, yang patut menjadi pertimbangan adalah pada kedua teks pertama yang dicoba, algoritma hash SHA-512 memberikan hasil yang lebih baik daripada hash dengan menggunakan algoritma Whirlpool. Pada percobaan dengan teks ketiga, algoritma hash SHA-512 memberikan point yang berkurang drastis jika dibandingkan dengan sebelumnya, yaitu hanya 810. Pada sisi lain, algoritma Whirlpool memberikan nilai yang cukup stabil, yaitu 920, 876, dan 962. Jika diurutkan pointnya dari yang terkecil sampai yang terbesar, maka nilai yang diperoleh adalah 876,920, dan 962. Rentang antara nilai pertama dan nilai kedua, serta nilai kedua dan nilai ketiga adalah 44 dan 42.

V. KESIMPULAN

Dari analisis yang dilakukan , dapat diperoleh bahwa kedua algoritma memiliki kelebihan dan kekurangannya masing-masing. Algoritma hash SHA-512 yang memiliki algoritma yang sederhana, tetapi dapat menghasilkan nilai hash yang kuat, serta menggunakan memori yang lebih sedikit jika dibandingkan dengan algoritma hash Whirlpool. Tetapi, nilai hash yang dihasilkan memiliki kekuatan sebagai kata kunci yang tidak stabil. Terkadang nilai kata kunci yang diberikan sangat kuat, tetapi terkadang nilai kata kunci yang diberikan sangat lemah.

Hal ini berbanding terbalik dengan algoritma hash Whirlpool. Algoritma hash ini membutuhkan proses yang lebih kompleks dibanding dengan algoritma hash SHA-512. Memori yang dibutuhkan juga lebih banyak jika dibandingkan dengan algoritma hash SHA-512, walaupun jumlah putaran yang dilakukan SHA-512 jauh lebih banyak dibandingkan dengan algoritma hash Whirlpool. Tetapi, hasil hash yang diberikan lebih stabil jika ingin digunakan sebagai kata kunci.

REFERENSI

[1] Denis, Tom St., *Cryptography for Developers,* Syngress Publishing, 2007.

[2] Halaman website pengecek kekuatan kata kunci : http://www.passwordmeter.com/ Diakses pada tanggal 8 Mei 2011.

[3] Halaman website GNU-crypto : http://www.gnu.org/software/gnu-crypto/ Diakses pada tanggal 19 Maret 2011

[4] Rijmen, Vincent, Barreto, Paulo S.L.M., *The Whirlpool Hashing Function*,(online),http://saluc.engr.uconn.edu/refs/algorithms/hash alg/barreto00whirlpool.pdf (diakses pada tanggal 8 Mei 2011).

[5] Halaman website mengenai algoritma hash SHA-2 : http://en.wikipedia.org/wiki/SHA-2 Diakses pada tanggal 8 Mei 2011

[6] Halaman website mengenai algoritma hash Whirlpool : http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html Diakses pada tanggal 8 Mei 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, 8 April 2011

Willy Setiawan
13508043