Studi Perbandingan dan Implementasi Kombinasi Fungsi Hash dan Kriptografi Kunci-Publik

Aditya Pratama - 13507084
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17084@students.if.itb.ac.id

Tanda-tangan digital adalah salah satu bentuk implementasi dari kriptografi. Tanda-tangan digital memberikan aspek keamanan yang tidak bisa diberikan oleh proses enkripsi-dekripsi. Aspek keamanan tersebut adalah autentikasi, keaslian pesan, dan anti-penyangkalan. Tanda-tangan digital berfungsi sama halnya seperti tanda-tangan pada dokumen cetak, bedanya adalah jika pada dokumen cetak bentuk dari tanda-tangan tetap sama apa pun isi dokumennya,nilai tanda-tangan digital selalu berubah bergantung pada isi dokumen digitalnya. Tanda-tangan digital bukanlah tanda-tangan yang didigitalisasi, melainkan sebuah nilai matematis yang besar nilainya bergantung pada isi dokumen dan kunci yang digunakan.

Implementasi dari tanda-tangan digital sendiri bisa dilakukan dengan dua cara. Yang pertama adalah dengan mengenkripsi pesan atau dokumen digital. Cara kedua adalah dengan menggunakan kombinasi algoritma fungsi hash dan algoritma kriptografi kunci-publik. Saat ini sudah banyak algoritma dari fungsi hash dan kriptografi kunci-publik yang dikembangkan sehingga menyebabkan implementasi dari tanda-tangan digital pun bermacam-macam pilihannya.

Dalam makalah ini penulis berusaha untuk membandingkan beberapa kombinasi fungsi hash dan kriptografi kunci-publik yang mungkin digunakan. Penulis akan mencoba membandingkan dua algoritma fungsi hash dan dua algoritma kriptografi kunci-publik. Dua algoritma fungsi hash yang dibandingkan adalah algoritma SHA-1 dan WHIRLPOOL dan dua algoritma kriptografi kunci-publik yang dibandingkan adalah algoritma RSA dan Paillier.

Kata kunci: **Fungsi hash, kriptografi, kriptografi kunci-publik, tanda-tangan digital.**

I. PENDAHULUAN

Informasi merupakan hal yang sangat penting bagi semua orang. Dengan semakin pesatnya perkembangan teknologi khususnya teknologi informasi dan komunikasi maka informasi menjadi makin berharga. Dengan semakin berharganya suatu informasi maka akan terdapat usaha-usaha yang menjamin bahwa informasi tersebut benar dikirim oleh pengirim dan belum diubah sama sekali oleh siapa pun di masa pengiriman. Salah satu usaha penjaminan keaslian pengirim pada dokumen tercetak adalah dengan menggunakan tanda tangan.

Tanda tangan adalah salah satu usaha yang digunakan untuk autentikasi dokumen cetak dan sudah digunakan sejak zaman dahulu. Tanda tangan memiliki beberapa karakteristik, yaitu:

- Tanda tangan adalah bukti autentik.
- Tanda tangan tidak dapat dilupakan.
- Tanda tangan tidak dapat dipindah untuk digunakan ulang.
- Dokumen yang telah ditandatangani tidak dapat diubah.
- Tanda tangan tidak dapat disangkal.

Konsep tanda tangan pada dokumen cetak pun bisa diterapkan pada data digital. Tanda tangan pada data digital atau yang biasa dikenal dengan istilah tanda tangan digital bukanlah tulisan tanda tangan yang didigitalisasi, melainkan sebuah nilai yang bergantung pada isi pesan atau data dan kunci yang digunakan. Perbedaan antara tanda tangan cetak dengan tanda tangan digital adalah tanda tangan cetak selalu sama tergantung pengirimnya terlepas dari isi dokumennya sedangkan tanda tangan digital selalu berbeda antara satu data digital dengan data digital lainnya.

Tanda tangan digital bisa diterapkan dengan melakukan enkripsi pada pesan dan juga menggunakan kombinasi fungsi hash dan kriptografi kunci-publik. Saat ini penerapan tanda tangan digital lebih banyak menggunakan kombinasi fungsi hash dan kriptografi kunci-publik. Algoritma fungsi hash dan kriptografi kunci-publik pun bermacam-macam. Contoh dari algoritma fungsi hash antara lain algoritma MD5, SHA-1, dan WHIRLPOOL sedangkan contoh dari algoritma kunci-publik antara lain RSA, Paillier, dan ElGamal.

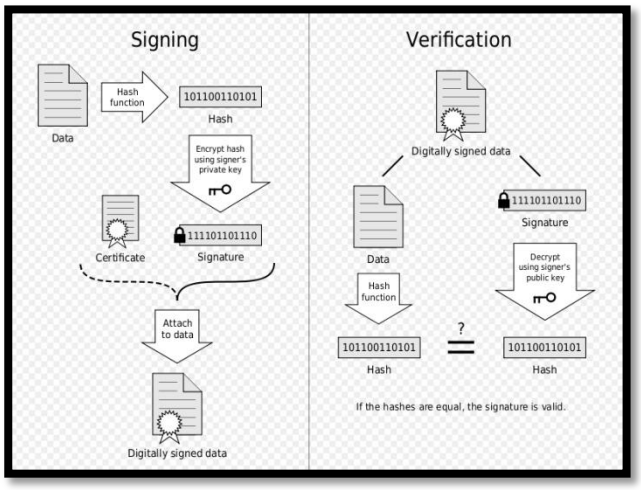
II. DASAR TEORI

2.1 Tanda-Tangan Digital

Tanda-tangan digital adalah salah satu bentuk turunan dari kriptografi yang memberikan aspek keamanan yang tidak bisa diberikan oleh proses enkripsi-dekripsi, yaitu autentikasi, keaslian pesan, dan anti-penyangkalan. Tanda-tangan digital menghasilkan sebuah nilai kriptografis yang hasilnya bergantung pada isi dari data

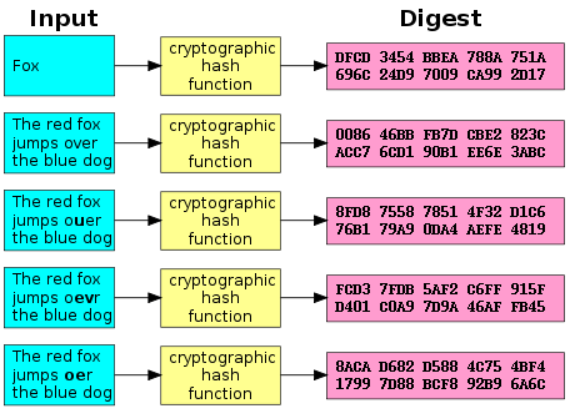
digital dan kunci yang digunakan.

Mayoritas penerapan tanda-tangan digital saat ini memanfaatkan kombinasi antara fungsi hash dengan kriptografi kunci-publik.



2.2 Fungsi Hash

Fungsi hash adalah sebuah prosedur atau fungsi matematis yang mengonversi mengonversi data berukuran tertentu menjadi sebuah nilai yang ukurannya statis untuk setiap fungsi. Biasanya masukan yang diterima adalah string dengan panjang yang sembarang dan ditransformasikan menjadi string keluaran yang panjangnya tetap dan biasanya berukuran lebih kecil dari ukuran string semula.



Fungsi hash yang ideal empat sifat utama, yaitu:

1. Mudah menghasilkan nilai hash untuk pesan apa pun.
2. Tidak bisa menghasilkan pesan dari sebuah nilai hash.
3. Tidak bisa mengubah pesan tanpa mengubah nilai hash-nya.
4. Tidak bisa menemukan dua pesan berbeda yang menghasilkan nilai hash yang sama.

Banyak sekali bentuk aplikasi dari fungsi hash dalam keamanan informasi yang kebanyakan berfungsi utama untuk autentikasi, seperti di tanda-tangan digital dan MAC (*Message Authentication Code*). Fungsi hash juga bisa digunakan sebagai indeks pada tabel hash, untuk sidik jari, dan lain-lain.

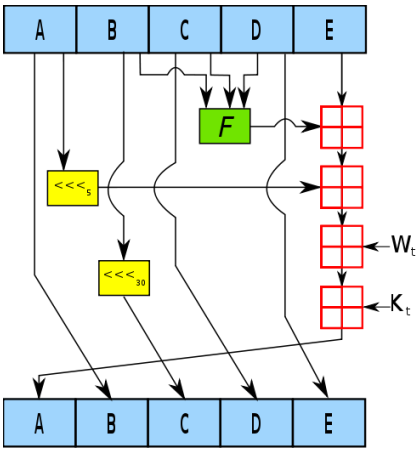
Contoh dari algoritma fungsi hash antara lain:

- SHA-1
- WHIRLPOOL
- MD5
- GOST

2.2.1 Algoritma SHA-1

SHA-1 adalah sebuah fungsi hash yang dikembangkan oleh NSA (*National Security Agency*). SHA-1 merupakan perkembangan dari SHA-0 dan dipublikasikan pada tahun 1995 di FIPS PUB 180-1.

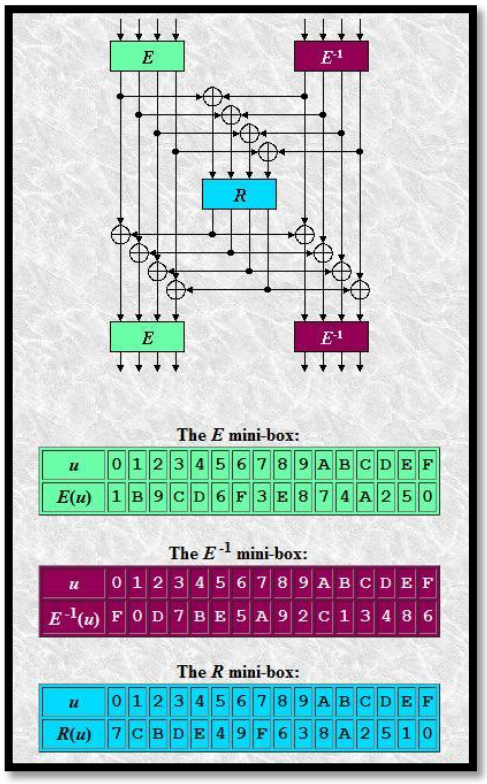
SHA-1 mampu menerima masukan data berukuran sampai dengan 2^{64}-1 bit dan menghasilkan nilai hash berukuran 160 bit. Masukan pada SHA-1 akan dipartisi dan diproses sebanyak 80 kali putaran dengan proses tiap putarannya seperti yang ditunjukkan pada gambar di bawah.



2.2.2 Algoritma WHIRLPOOL

WHIRLPOOL adalah fungsi hash yang dirancang oleh Vicent Rijmen, salah satu perancang algoritma Rijndael yang dijadikan sebagai AES (*Advanced Encryption Standard*), dan Paulo S. L. M. Barreto pada tahun 2000.

WHIRLPOOL mampu menerima masukan data berukuran sampai dengan 2^{256}-1 bit dan menghasilkan nilai hash berukuran 512 bit. Masukan pada WHIRLPOOL akan dipartisi dan diproses sebanyak 10 kali putaran. WHIRLPOOL juga memanfaatkan S-BOX yang disusun secara acak menurut struktur yang rekursif seperti gambar



2.3 Kriptografi Kunci-Publik

Kriptografi kunci-publik dikembangkan karena terdapat permasalahan pada kriptografi kunci-simetri yaitu kesulitan dalam mengirimkan kunci rahasia pada penerima. Saluran yang aman yang dapat digunakan untuk mengirimkan kunci rahasia tersebut biasanya lambat dan mahal. Untuk mengatasi masalah tersebut muncullah ide konsep dari kriptografi kunci-publik yang dibuat oleh Whitfield Diffie dan Martin Hellman pada tahun 1976.

Kriptografi kunci-publik didasarkan pada fakta bahwa komputasi untuk enkripsi dan dekripsi pesan sudah mudah untuk dilakukan dan hampir tidak mungkin mendapatkan kunci privat bila diketahui kunci publiknya.

Kelebihan dari kriptografi kunci-publik antara lain:
- Hanya kunci privat yang perlu dijaga kerahasiaannya.
- Pasangan kunci publik dan privat tidak perlu diubah.
- Dapat digunakan untuk pengiriman kunci simetri.

Kekurangan dari kriptografi kunci-publik antara lain:
- Enkripsi dan dekripsi data umumnya lebih lambat daripada yang menggunakan kunci simetri..
- Ukuran cipherteks lebih besar daripada plainteks.
- Ukuran kunci relatif lebih besar dari kunci simetri.

Contoh dari algoritma kriptografi kunci-publik antara lain:
- RSA
- Paillier
- DSA
- ElGamal

III. Perbandingan Algoritma Fungsi Hash dan Kriptografi Kunci-Publik

Tanda-tangan digital dapat diimplementasikan menggunakan kombinasi antara fungsi hash dengan kriptografi kunci-publik. Saat ini sudah banyak sekali algoritma dari fungsi hash dan kriptografi kunci-publik yang sudah dikembangkan. Setiap algoritma yang dikembangkan memiliki kelebihan, kekurangan, dan ciri khas masing-masing.

Pada kali ini akan dibandingkan dua algoritma fungsi hash, yaitu algoritma SHA-1 dan WHIRLPOOL, dan dua algoritma kriptografi kunci-publik, yaitu RSA dan Paillier.

3.1 Perbandingan Fungsi Hash

Algoritma	SHA-1	WHIRLPOOL
Ukuran Hasil (bit)	160	512
Ukuran Blok	512	512
Ukuran Maksimum (bit)	2^{64}-1	2^{256}-1
Jumlah Putaran	80	10
Kolisi	Teoritis	Belum

3.2 Perbandingan Kriptografi Kunci-Publik

Algoritma RSA dan Paillier memiliki beberapa variabel yang sifat kerahasiaannya publik atau privat.

Untuk algoritma RSA sifat-sifat dari variabelnya adalah:

Properti	Sifat Kerahasiaan
p (bilangan prima besar)	privat
q (bilangan prima besar)	privat
n = p . q (kunci)	publik
Φ(n) = (p - 1)(q - 1)	privat
e (kunci publik)	publik
d (kunci privat)	privat

Untuk algoritma Paillier sifat-sifat dari variabelnya adalah:

Properti	Sifat Kerahasiaan
p (bilangan prima besar)	privat
q (bilangan prima besar)	privat
n = p . q (kunci)	publik
λ = kpk(p - 1)(q - 1) (kunci privat)	privat
g (kunci publik)	publik
r	privat
μ	privat

IV. PENGUJIAN DAN ANALISIS

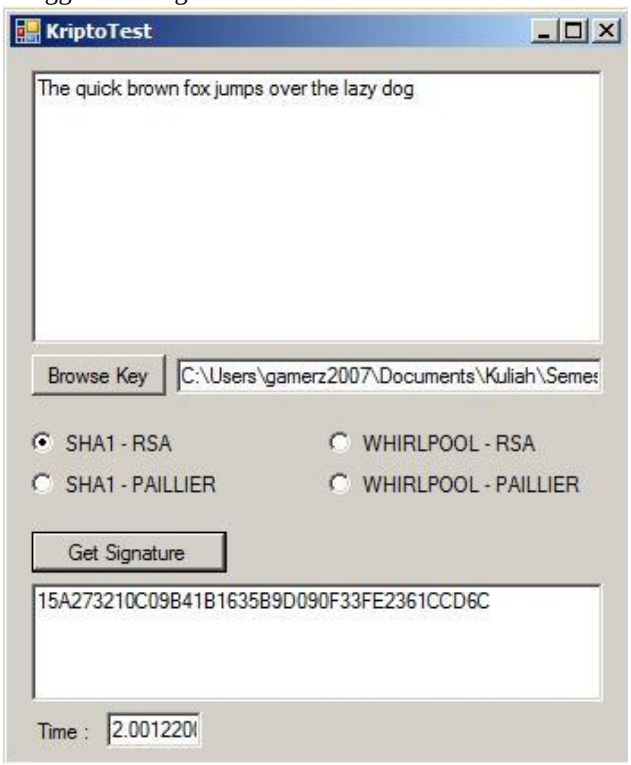
4.1 Pengujian

Pada bab ini akan diuji dan dibandingkan hasil dari implementasi kombinasi antara dua fungsi hash dan dua kriptografi kunci-publik, yaitu:

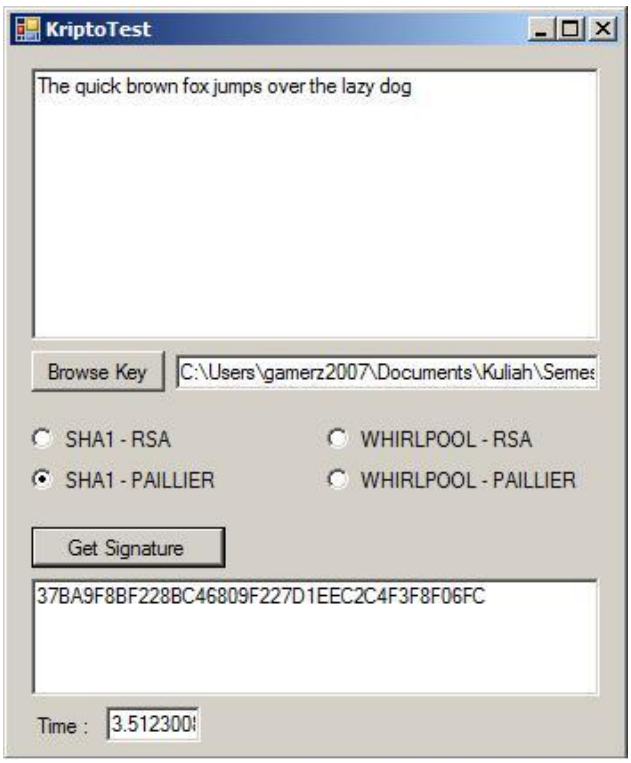
1. SHA-1 – RSA
2. SHA-1 – Paullier
3. WHIRLPOOL – RSA
4. WHIRLPOOL – Paullier

Pada pengujian ini diukur waktu yang dibutuhkan untuk melakukan proses pembuatan tanda-tangan digital sesuai dengan algoritma yang digunakan.

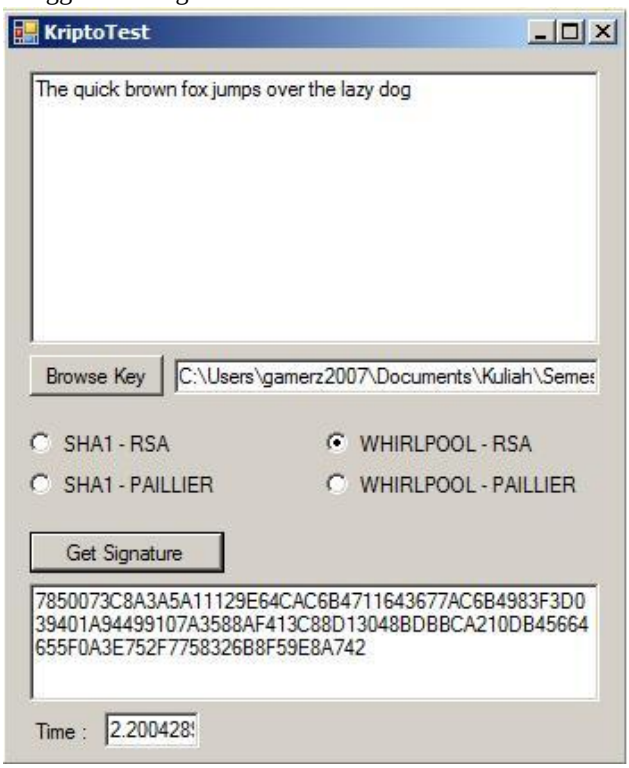
Hasil pengujian untuk implementasi tanda-tangan digital menggunakan algoritma SHA-1 dan RSA:



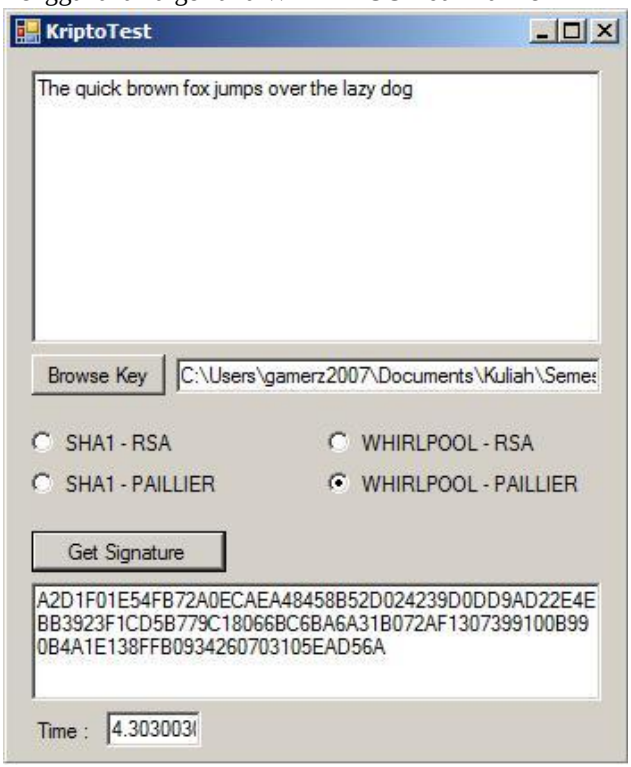
Hasil pengujian untuk implementasi tanda-tangan digital menggunakan algoritma SHA-1 dan Paillier:



Hasil pengujian untuk implementasi tanda-tangan digital menggunakan algoritma WHIRLPOOL dan RSA



Hasil pengujian untuk implementasi tanda-tangan digital menggunakan algoritma WHIRLPOOL dan Paillier



Hasil dari perbandingan waktu yang dibutuhkan antara kombinasi-kombinasi fungsi hash dan kriptografi kunci-publik tersebut adalah:

	SHA-1	WHIRLPOOL
RSA	**2.00**	**2.20**
Paillier	**3.51**	**4.30**

4.2 Analisis

4.2.1 Analisis Kecepatan Proses Tanda-Tangan Digital

Dari hasil pengujian jika waktu yang dibutuhkan untuk menyelesaikan proses penghitungan nilai tanda-tangan digital diurutkan dari yang paling cepat maka hasilnya adalah:

1. SHA-1 – RSA
2. WHIRLPOOL – RSA
3. SHA-1 – Paillier
4. WHIRLPOOL – Paillier

Dari hasil yang didapat tersebut dapat dilihat bahwa algoritma yang memberikan pengaruh yang cukup signifikan adalah algoritma kriptografi kunci-publiknya. Hal ini disebabkan oleh perbedaan proses yang cukup signifikan antara algoritma RSA dan Paillier dimana komputasi enkripsi yang terjadi pada Paillier lebih rumit jika dibandingkan dengan algoritma RSA. Pada proses enkripsi algoritma RSA yang terjadi adalah proses satu kali operasi perpangkatan dan satu kali operasi modulo. Sedangkan pada proses enkripsi algoritma Paillier yang terjadi adalah proses dua kali operasi perpangkatan, satu kali operasi perkalian, dan satu kali operasi modulo.

Dapat dilihat juga walaupun tidak signifikan terdapat perbedaan waktu yang dibutuhkan antara kombinasi yang menggunakan algoritma fungsi hash SHA-1 dan WHIRLPOOL. Algoritma SHA-1 relatif lebih cepat jika dibandingkan dengan algoritma WHIRLPOOL. Hal ini disebabkan karena walaupun putaran yang dilakukan oleh SHA-1 jauh lebih banyak jika dibandingkan dengan WHIRLPOOL (80 pada SHA-1 dan 10 pada WHIRLPOOL), proses yang terjadi pada fungsi SHA-1 jauh lebih sederhana jika dibandingkan dengan fungsi WHIRLPOOL. Pada fungsi hash SHA-1 proses yang terjadi adalah operasi rotasi dan penjumlahan (XOR) saja. Pada fungsi hash WHIRLPOOL proses yang terjadi adalah rotasi, penjumlahan, dan permutasi yang dilakukan dengan S-BOX yang pembuatannya pun membutuhkan waktu yang cukup banyak juga.

4.2.2 Analisis Keamanan Tanda-Tangan Digital

Untuk faktor keamanan pada tanda-tangan digital dilihat dari panjangnya tanda-tangan digital karena semakin panjang ukuran tanda-tangan digital maka semakin kecil pula kemungkinan terjadi kolisi. Dari asumsi tersebut maka dapat disimpulkan bahwa penerapan tanda-tangan digital yang menggunakan algoritma fungsi hash WHIRLPOOL lebih aman karena panjang *message digest* yang lebih panjang dari SHA-1, yaitu 512 bit.

V. KESIMPULAN

Berdasarkan pengujian dan analisis dari beberapa kombinasi fungsi hash dan kriptografi kunci-publik untuk mengimplementasikan tanda-tangan digital, penulis mendapatkan beberapa kesimpulan, yaitu:

1. Implementasi dari tanda-tangan digital bisa menggunakan kombinasi fungsi hash dan kriptografi kunci-publik.
2. Algoritma dari fFungsi hash dan kriptografi kunci-publik yang digunakan pada tanda-tangan digital bisa diubah sesuai kebutuhan.
3. Algoritma fungsi hash SHA-1 lebih cepat jika dibandingkan dengan algoritma fungsi hash WHIRLPOOL.
4. Algoritma kriptografi kunci-publik RSA lebih cepat jika dibandingkan dengan algoritma kriptografi kunci-publik Paillier.
5. Tanda-tangan digital yang menggunakan algoritma fungsi hash WHIRLPOOL lebih aman karena hasilnya yang lebih panjang.

DAFTAR PUSTAKA

[1] http://www.youdzone.com/signature.html
Tanggal akses: 5 Mei 2011

[2] http://williamstallings.com/Extras/Security-Notes/lectures/authent.html
Tanggal akses: 5 Mei 2011

[3] www.cgi.com/cgi/pdf/cgi_whpr_35_pki_e.pdf
Tanggal akses: 5 Mei 2011

[4] http://www.di-mgt.com.au/rsa_alg.html
Tanggal akses: 5 Mei 2011

[5] http://www.itl.nist.gov/fipspubs/fip180-1.htm
Tanggal akses: 5 Mei 2011

[6] http://www.gemplus.com/smart/rd/publications/pdf/Pai99pai.pdf
Tanggal akses: 5 Mei 2011

[7] http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html
Tanggal akses: 5 Mei 2011

[8] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung

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 Mei 2011

Aditya Pratama, 13507084