CESS (Journal Of Computer Engineering System And Science) **p-ISSN :2502-7131**
Vol 1, No 1, Januari 2016 **e-ISSN :2502-714x**

MODEL KEAMANAN INFORMASI BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA RSA

Mohamad Ihwani
Universitas Negeri Medan
Jl. Willem Iskandar Pasar v Medan Estate, Medan 20221
mohamadihwani@unimed.ac.id

Abstrak — Kerahasiaan dan keamanan data yang merupakan hal yang sangat penting, sehingga untuk menjaga kerahasiaan dan keamanan data perusahaan tersebut dapat dilakukan salah satunya dengan menggunakan teknik kriptografi. Digital Signature Algorithm (DSA) merupakan salah satu kriptografi yang digunakan untuk nirpenyangkalan. DSA merupakan suatu tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital, namun DSA dengan fungsi hash tidak mengenkripsi plainteks asli sehingga, dikombinasikan dengan RSA.

Keywords : **Kriptografi, DSA, RSA.**

I. PENDAHULUAN

Salah satu algoritma kriptografi untuk keamanan informasi adalah algoritma digital signature (DSA). DSA atau Digital Signature Algorithm merupakan salah satu algoritma kriptografi kunci publik yang paling banyak digunakan saat ini. Penerapan tanda tangan digital antara lain: sertifikat digital untuk keamanan e-commerce, untuk penandatanganan kontrak yang sah dan untuk mengamankan pembaruan perangkat lunak (Mollin, 2007).

DSA merupakan suatu tanda tangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim dari suatu pesan atau penandatangan dari suatu dokumen digital. Tanda tangan digital ini memastikan isi pesan atau dokumen digital yang dikirim tidak mengalami perubahan sampai ke tangan penerima. Dengan demikian penerima yakin bahwa pesan yang diterimanya benar-benar asli dari pihak pengirim.

Selain kriptografi DSA juga membutuhkan fungsi hash, fungsi hash merupakan fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (fixed), umumnya berukuran jauh lebih kecil daripada ukuran string semula, hasil konversi pesan tersebut akan disamakan dengan hasil dekripsi dari proses kriptografi DSA untuk otentikasi dan integritas dari keaslian pesan.

DSA banyak diaplikasikan untuk keamanan informasi berupa file digital, hal tersebut dilakukan untuk mencegah pemalsuan pengiriman suatu file atau pesan digital. Teknologi informasi yang semakin berkembang saat ini menuntut perusahaan untuk dapat menjaga keamanan dan kerahasiaan data perusahaan termasuk harus melakukan otentikasi pengirim dan kepercayaan pada file atau pesan digital yang akan dikirimkan.

II. TINJAUAN PUSTAKA

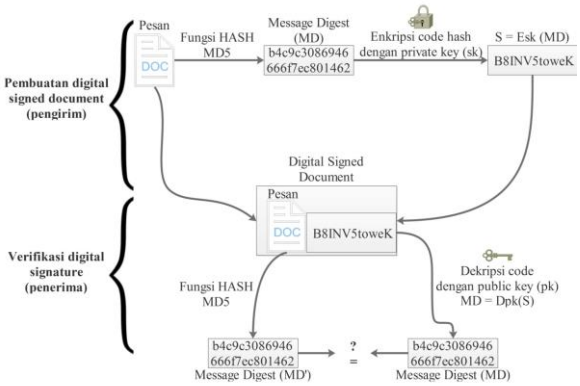
A. Digital Signature Algorithm (DSA)

Tanda tangan digital (digital signature) adalah suatu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas (Munir, 2006). Tanda tangan pesan dapat dilakukan dengan dua cara yaitu:

1. Enkripsi pesan

   Mengenkripsi pesan dengan sendirinya serta menyediakan ukuran otentikasi, pesan yang terenkripsi sudah menytakan pesan tersebut telah ditandatangani
2. Tanda tangan digital dengan fungsi hash (hash function)

   Tanda tangan digital dibangkitkan dari hash terhadap pesan. Nilai hash adalah kode ringkas dari pesan. Tanda tangan digital berlaku seperti tanda tangan dokumen kertas, tanda tangan digital ditambahkan (append) pada pesan.



Gambar 1. Proses DSA dengan fungsi HASH

Pada Gambar tersebut apabila pesan yang diterima sudah berubah, maka MD' yang dihasilkan dari fungsi hash berbeda dari MD semula yang berarti

pesan tersebut sudah tidak asli lagi. Apabila pesan M tidak berasal dari orang yang sebenarnya, maka message digest (MD) yang dihasilkan berbeda dengan message digest (MD') yang dihasilkan pada proses verifikasi karena kunci public yang digunakan oleh penerima pesan tidak berkoresponden dengan kunci privat pengirim. Bila MD = MD' maka pesan yang diterima adalah pesan asli (message authentication) dan orang yang mengirim merupakan orang yang sebenarnya (user authentication).

Proses pemberian tanda tangan digital (signing) dimulai dari menghitung message digest (MD) dari pesan yang diperoleh dengan mentransformasikan pesan M dengan menggunakan fungsi hash satu arah H.

$$MD = H(M)$$

Message Digest (MD) dienkripsi dengan algoritma kunci-publik dan menggunakan kunci privat (SK), hasil enkripsi ini dinamakan dengan tanda-tangan digital S.

$$S = Esk(MD)$$

Tanda-tangan digital S dilekatkan ke pesan M dengan cara append S, dan dikirin melalui media komunikasi, dalam hal ini dapat dikatakan bahwa pesan M sudah ditandatangani oleh pengirim dengan tanda-tangan digital S.

Untuk membuktikan keontetikannya maka sipenerima melakukan verifikasi, dimana tanda-tangan digital S di dekripsi dengan menggunakan kunci publik (pk) sehingga menghasilkan message digest (MD).

$$MD = Dpk(S)$$

Penerima kemudian merubah pesan M menjadi message digest MD' menggunakan fungsi hash satu-arah yang sama dengan fungsi hash yang digunakan pengirim, jika MD' = MD berarti tanda-tangan yang diterima otentik dan berasal dari pengirim yang benar.

```
--
*Best Regards*,
Mohamad Ihwani
ICT Coordinator
State University of Medan
email : ihwani@unimed.in; mohamadihwani@unimed.ac.id; goprax@gmail.com
laman Unimed : http://www.unimed.ac.id <http://sm-3t.unimed.ac.id/>

--089e0160d258df460c05183e1b47
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
```

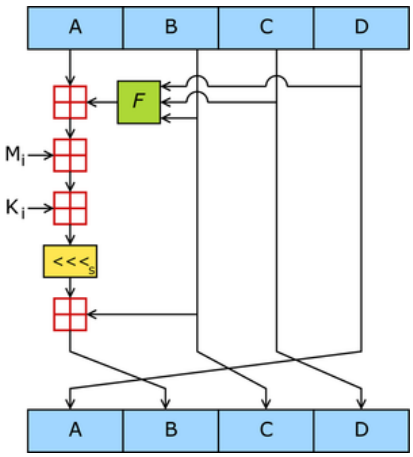
Gambar 2. Contoh tanda tangan digital

B. Fungsi HASH (MD5)

Fungsi hash satu-arah atau dikenal dengan nama lain one-way hash merupakan fungsi hash yang bekerja dalam satu arah, fungsi ini biasanya diperlukan untuk pengambilan sidik jari suatu pesan (Kurniawan, 2004). Pesan yang sudah menjadi message digest tidak dapat dikembalikan menjadi pesan semula, setiap pesan yang berbeda akan menghasilkan nilai hash yang berbeda.

Algoritma MD5 Fungsi hash satu arah yang dibuat oleh Ronald Rivest ditahun 1991. MD5 merupakan perbaikan dari MD4, algoritma ini menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.

Langkah-langkah pembuatan message digest secara garis besar adalah sebagai berikut:
- Penambahan bit-bit pengganjal (padding bits)
- Penambahan nilai panjang pesan semula
- Inisialisasi penyangga (buffer) MD
- Pengolahan pesan dalam blok berukuran 512bit



Gambar 3. Operasi dasar MD5

C. Algoritma RSA

Algoritma RSA, ditemukan oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. RSA merupakan salah satu dari public key cryptosystem yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar (Mollin, 2007).

Algoritma Pembentukan Kunci:

1. Tentukan p dan q bernilai dua bilangan Prima besar, acak dan dirahasiakan.

$p \neq q$, p dan q memiliki ukuran sama.

2. Hitung $n = pq$

Dan hitung $\imath(n) = (p-1)(q-1)$.

Bilangan integer n disebut (RSA) modulus.

3. Tentukan e bilangan Prima acak, yang memiliki syarat:

$1 < e < \imath(n)$

$GCD(e, \imath(n)) = 1$, disebut e relatif prima terhadap $\imath(n)$, Bilangan integer e disebut (RSA) enciphering exponent.

4. Memakai algoritma Euclid yang diperluas (Extended Eucledian Algorithm).

Menghitung bilangan khusus d,

syarat $1 < d < \imath(n)$

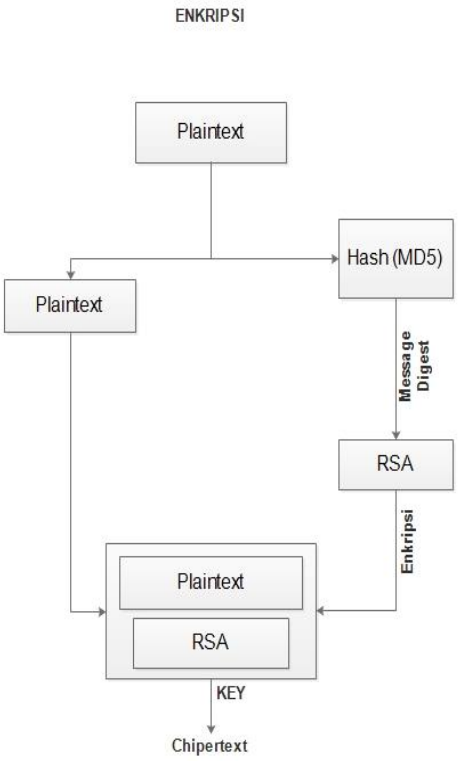
$d \equiv e\text{-}1 \bmod \imath(n)$

ed ≡ 1 (mod ı(n))
ed ≡ 1 + k.ı(n) untuk nilai k integer.
Bilangan integer d disebut (RSA) deciphering exponent.
5. Nilai (n,e) adalah nilai yang boleh dipublikasi.
Nilai d, p, q, ı(n) adalah nilai yang harus dirahasiakan.
Pasangan (n,e) merupakan kunci publik.
Pasangan (n,d) merupakan kunci rahasia.

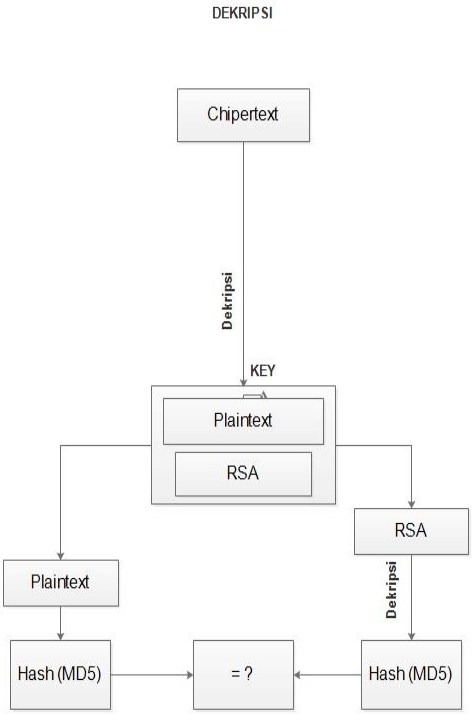
III. METODE PENELITIAN

Teknik pengembangan pada penelitian ini adalah teknik pengamanan digital signature algorithm (DSA) dengan penambahan algoritma dan RSA.

Adapun skema alur pengembangan teknik algortima Digital Signature dapat di lihat pada gambar dibawah ini:



Gambar 4. Rancangan enkripsi DSA

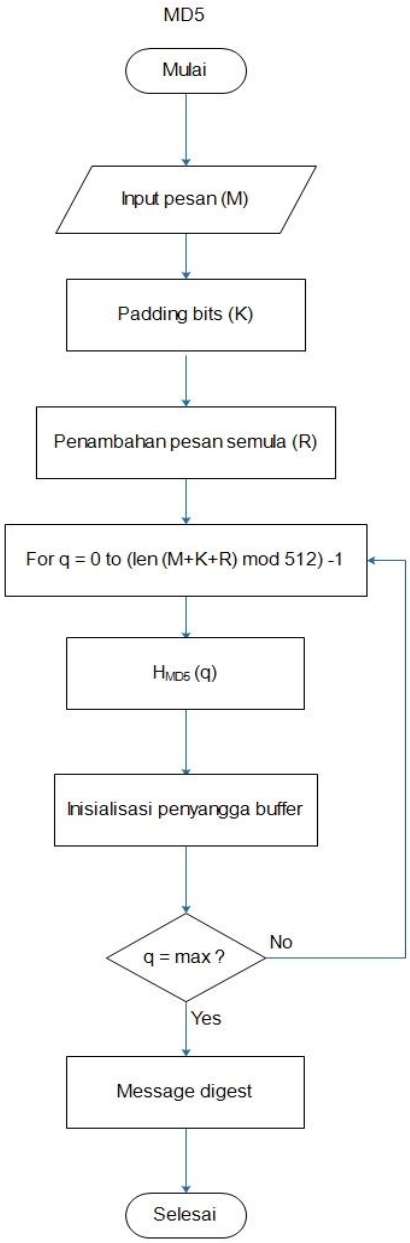


Gambar 5. Rancangan Dekripsi DSA

Untuk memudahkan dalam hal pembahasan, gambar diatas dapat dibagi menjadi beberapa bagian, diantaranya adalah:

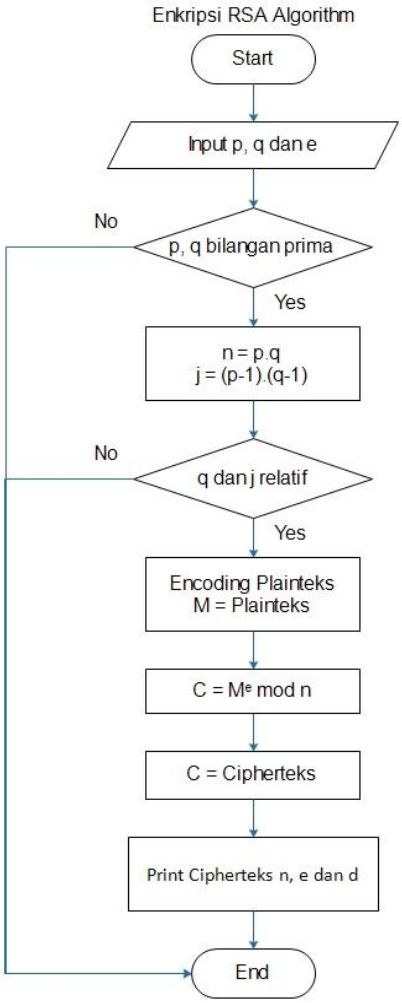
Proses enkripsi
a. Plainteks yang di bagi menjadi 2 bagian yaitu bagian plainteks asli dan bagian plainteks yang diubah menjadi message digest dengan menggunakan hashing MD5.
b. Proses enkripsi message digest dengan menggunakan RSA.
Proses dekripsi
a. Cipherteks RSA didekripsikan sehingga menghasilkan message digest yang diperoleh dari hasil hashing MD5.
b. Plainteks asli akan di jadikan message digest dengan MD5 dan akan dicocokkan dengan hasil message digest dari dekripsi RSA.

A. Fungsi peubah MD5

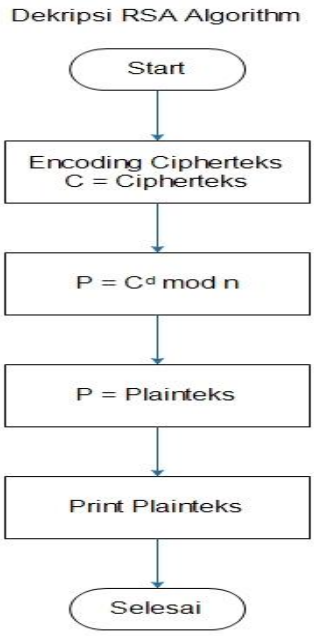


Gambar 6. Alur fungsi MD5

B. Alur enkripsi dan dekripsi RSA algorithm



Gambar 7. Alur enkripsi RSA



Gambar 8. Alur dekripsi RSA

Gambar 9. Proses validasi

Jika hasil ternyata cocok (sama) maka file/pesan terbukti keasliannya dan file dapat diunduh, namun jika terjadi ketidak cocokan, maka file/pesan tersebut sudah tidak asli dan file tidak dapat diunduh.

IV. HASIL DAN PEMBAHASAN

Penelitian ini merupakan model dari digital signature algorithm dengan fungsi hash, yang mana ditambahkan kombinasi dari algortma RSA. Algoritma digital signature dengan fungsi hash yaitu tanda tangan digital yang dibangkitkan dari hash terhadap pesan. Nilai hash adalah kode ringkas dari pesan. Tanda tangan digital berlaku sepertu tanda-tangan pada dokumen kertas. DSA model ini memiliki fungsi nir-penyangkalan, namun memiliki kelemahan dari sisi plainteks, algoritma DSA dengan fungsi hash akan tetap menampilkan plainteks yang dikirim tersebut , sehingga apabila teks tersebut dikirim ke penerima tetap akan menampilkan plainteks yang memungkinkan orang lain dapat melihatnya namun jika plainteks tersebut dirubah maka si penerima akan tau bahwa pesan tidak asli (nir-penyangkalan). Algoritma RSA merupakan sebuah algoritma simetris, dimana tingkat keamanannya tergantung dari perpangkatan bilangan prima yang menjadi kuncinya, algoritma RSA ini akan melakukan proses enkripsi pada hashing MD5 sehingga message digest terjaga dan terenkripsi, hal ini dilakukan untuk kemanan disisi MD5 yang akan dikirim bersamaan dengan plainteks.

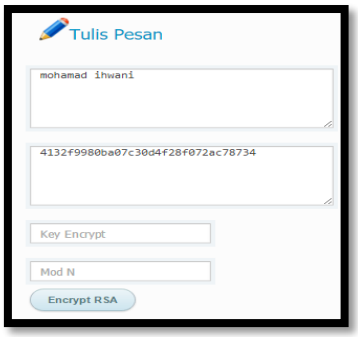
A. Uji Coba

Program yang dibangun untuk mendukung penelitian ini menggunakan PHP yang berjalan secara local host dan online pada system operasi windows 10, adapun tampilan program uji coba ini ditunjukkan pada gambar 10 dan 11. Gambar 10 menunjukkan form login dari aplikasi DSA system dan gambar 11 adalah tampilan menu utama setelah login.

Gambar 10. Login DSA

Gambar 11. Form enkripsi file dan teks

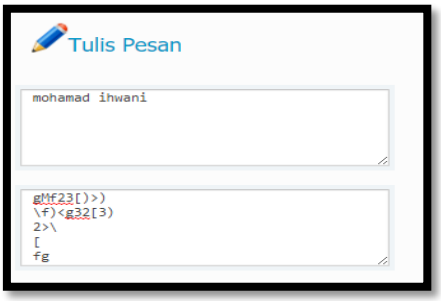
Percobaan akan dilakukan proses enkripsi terhadap pesan atau teks, input teks mohamad ihwani dan lakukan proses hashing.



Gambar 12. Proses hashing MD5

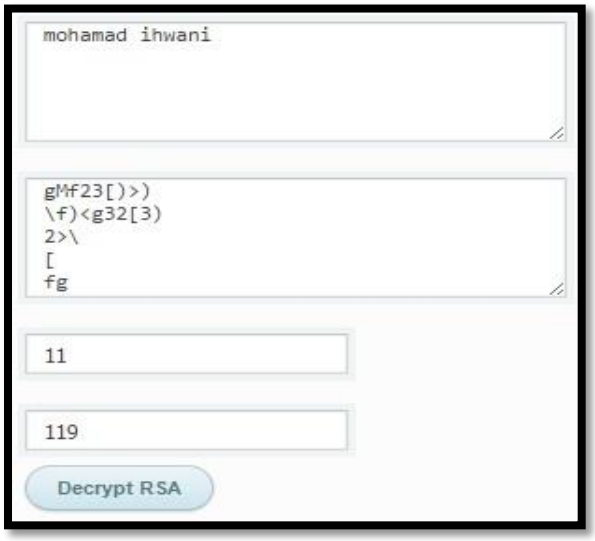
Hasil dari hashing teks mohamad ihwani dengan menggunakna MD5 adalah 4132f9980ba07c30d4f28f072ac78734 .Message digest ini kemudian akan dienkripsi menggunakan RSA algorithm, seperti berikut:

N = p x q dimana p dan q bilangan prima
J = (p-1) x (q-1)
Ambil 1 < e < j sehingga ditemukan d x e mod j = 1
E=M^(e) mod n
Bilangan prima yang digunakan pada contoh ini adalah p=7 dan q=17
N = 119
J = 96
Ambil 1 < e = 11 < 96 sehingga d = 35 supaya 35 * 11 mod 96 = 1
Pembangkit kunci untuk enkripsi adalah 35 sehingga
E = M35 mod 119



Gambar 13. Proses enkripsi RSA

Plainteks dan cipherteks dari RSA akan dikirimkan ke penerima.
Si penerima akan dekripsi hasil tersebut seperti berikut.



Gambar 14. Dekripsi pesan

Proses selanjutnya adalah dekripsi RSA menggunakan
N = pxq dimana p dan q bilangan prima
J = (p-1)x(q-1)
Ambil 1 < e < J sehingga ditemukan d x e mod J = 1
Decrypt
M = E^(d) mod n
Bilangan prima yang digunakan pada contoh ini adalah p=7 dan q=17
n=119
j=96
ambil 1<e=11<96 sehingga d=35 supaya 35*11 mod 96=1
decrypt
M=E^(11) mod 119

Hasil dari dekripsi RSA merupakan hashing dari plainteks awal, untuk pengujian DSA akan dilakukan dengan cara mencocokkan hashing dari plainteks dan hashing dekripsi RSA, apakah valid atau tidak, lakukan uji hash untuk menguji kecocokan dari pesan tersebut.

Gambar 15. Signature valid

Hash merupakan tanda tangan digital, dalam kasus ini hash yang dihasilkan dari dekripsi RSA sesuai dengan hash plainteks, kecocokan antar hash ini dapat dipastikan bahwasannya pesan benar-benar asli tidak ada perubahan. Apabila tidak sesuai maka dignature tidak akan valid.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan pembahasan dan evaluasi, maka dapat ditarik kesimpulan sebagai berikut:

1. Model algoritma Digital Signature Algorithm (DSA) yang digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan sebagai nirpenyangkalan membutuhkan algoritma kriptografi RSA untuk menjaga keamanan dan kerahasiaan file dan pesan.
2. Proses validasi pesan yang dikirimkan perusahaan menggunakan model algoritma DSA dengan fungsi hash dari proses dekripsi RSA dan fungsi hash dari plainteks, apabila hash tidak sesuai maka file tidak akan bisa diunduh.
3. Waktu yang dibutuhkan dalam proses hash dan enkripsi serta dekripsi beberapa file dengan kapasitas dan ekstensi yang berbeda-beda memiliki rata-rata kurang dari 1 detik, menunjukkan bahwa model algoritma Digital Signature Algorithm (DSA) sangat tepat digunakan dalam proses pengiriman file dan pesan berbasis arsitektur perusahaan.

B. Saran

Berikut adalah saran-saran untuk pengembangan lebih lanjut

1. Untuk pengembangan lebih lanjut, perlu diteliti model algoritma lain yang dapat melakukan proses pengiriman dan pengamanan file yang berukuran lebih besar (kapasitas Giga Byte) dari yang sudah dilakukan oleh peneliti.
2. Pada proses DSA plainteks dan hashing dipisah, plainteks hanya dienkripsi oleh algoritma RSA, sedangkan hashing telah dienkripsi sebelumnya dengan algoritma RSA, ada baiknya plainteks juga sudah terenkripsi.

REFERENSI

[1] Kurniawan, Yusuf. 2004, Kriptografi Keamanan Internet dan Jaringan Komunikasi, Bandung: Informatika.
[2] Mollin, R.A, 2007. "An introduction to cryptography", second edition, by Taylor & Francis Group, London, Newyork.
[3] Munir, R, 2006. "Belajar Ilmu Kriptografi" Penerbit Andi, Yogyakarta.
[4] Paramitasari, A.D., Cahyani, N.D. & Wirayuda, T.A.B. 2009. Implementasi Digital Signature Untuk Verifikasi Data Menggunakan Digital Signature Algorithm (DSA), Telkom-U (2009).