Riset dan E-Jurnal Manajemen Informatika Komputer
Vol. 1 Nomor 2, April 2017
e-ISSN : 2541-1330
p-ISSN : 2541-1322

ANALISIS DAN PERANCANGAN APLIKASI KRIPTOGRAFI KEAMANAN FILE BERBASIS TEKS DENGAN MENGGUNAKAN METODE RSA

Leo Benny
STMIK ITMI Medan
Jl. Timah Putih Komplek Asia Mega Mas Blok G No. 16
Medan, Sumatera Utara
Leobenny87@yahoo.com

ABSTRAK--Telah diuji suatu model pengamanan dokumen yang dapat digunakan sebagai salah satu instrumen sistem pengamanan dokumen khususnya untuk dokumen teks. Adapun prinsip pengamanan dokumen ini adalah bagaimana sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen. Mula-mula dokumen dalam bentuk teks dienkripsi. Sehingga dokumen tidak dapat dibaca oleh siapapun. Karena teks telah berubah menjadi susunan huruf yang teracak. Dokumen yang susunan hurufnya telah teracak tersebut jika ingin dibaca oleh pemilik dokumen, maka dokumen tersebut harus dibuka dengan dekripsi. Dalam penelitian ini, metode yang digunakan adalah metode RSA, dimana metode tersebut menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal (dengan private key maupun dengan public key) sehingga amat sulit untuk ditembus oleh orang yang tidak berkepentingan. Sistem ini dibangun dengan perangkat lunak vb 6.0 . Hasil pengujian ini menunjukkan bahwa sistem dapat menyimpan dan mengirimkan dokumen baik pengiriman melalui internet maupun intranet dalam bentuk susunan huruf yang terenkripsi dan mengembalikan ke bentuk dokumen semula dengan cara dekripsi.

Kata Kunci--Pengujian, Dokumen, Enkripsi, Dekripsi, RSA, Waktu proses.

I. PENDAHULUAN

1. Latar Belakang

Dewasa ini, Semakin pesatnya perkembangan teknologi informasi (TI) tidak akan pernah lepas dari permasalahan keamanan komputer *(Computer Security).* Keamanan Komputer sebagai isu yang tidak akan pernah habis dibicarakan para pelaku bidang TI selalu menuntut adanya *update* setiap saat dan berkala. Namun hal yang tidak kalah penting dari permasalahan keamanan komputer dalam hal keabsahan pengiriman maupun penerimaan File Dokumen.

Seperti pada kasus pengiriman file, pengiriman file via internet, Email maupun via Offline antar sesama perusahaan merupakan cara yang paling praktis di era teknologi informasi dewasa ini. Karena bisa dilakukan dengan mudah, maka aspek-aspek keamanan dalam proses pengirimannya perlu diperhatikan. Padahal dalam pengiriman File Dokumen di dalam sistem pengelola perusahaan memakai keamanan data akses menggunakan password, Namun aspek-aspek keamanan tersebut tetap saja belum mampu untuk menghentikan para *pengakses yang iseng* untuk melakukan teknik *deception (man in the middle),* yaitu suatu teknik untuk mendapatkan data dengan cara melakukan pengelabuan seakan-akan dia adalah orang yang dituju dalam pengiriman data. Bila teknik ini berhasil dilakukan, maka sudah bisa dipastikan bahwa data akan jatuh ke tangan *orang yang tidak berkepentingan* dan dengan mudah dapat dibaca.

Dalam dunia TI integritas suatu data yang dikirim terkadang juga menjadi pertanyaan, apakah data tersebut benar-benar

e-ISSN : 2541-1330
p-ISSN : 2541-1322

dikirim oleh orang yang bersangkutan atau tidak, dan apakah isi dari data benar-benar otentik seperti sebelum dikirim. Hal ini merupakan masalah serius karena bisa saja sesorang mengirimkan data palsu.

2. Tinjauan Pustaka

Beberapa penelitian yang menjadi referensi penelitian ini adalah :

[1]. Penelitian yang di lakukan oleh Nugraha, Ary Reza dengan judul *Penyembunyian pesan rahasia yang terenkripsi menggunakan algoritma RSA pada media kompresi*. Jurnal Teknik POMITS Vol2, No.1, (2013), IISN: 2337-3539 (2301-9271). Saat ini banyak sekali penerimaan dan pengiriman pesan yang beredar tetapi bias di lacak oleh orang yang tidak berkepentingan, Untuk itu diperlukan suatu cara untuk mengamankan pesan rahasia tadi agar tidak diketahui oleh orang yang tidak berkepentingan. Penyembunyian pesan rahasia yang berupa file dalam arsip ZIP dapat menjadi salah satu solusi untuk keamanan data yang bersifat rahasia jika data tersebut ingin dikirimkan. Arsip ZIP merupakan kumpulan dari beberapa file yang terkompresi dimana ukuran dari file-file tersebut beragam. Biasanya orang tidak memperhatikan ukuran file dari arsip ZIP karena ukuran dari file-file di dalam arsip ZIP tersebut terkompresi. Dari hasil uji coba yang dilakukan, file yang berisi pesan rahasia berhasil disembunyikan pada arsip ZIP serta tidak akan terbaca pada aplikasi pembaca arsip ZIP.

[2]. Penelitian yang di lakukan oleh Aditya Permana dengan judul "*Kriptografi pada file Dokumen Microsoft office menggunakan metode RSA"***.** jurnal komputer Program Studi Ilmu Komputer Universitas Brawijaya Malang, 2005. Dalam penelitian ini algoritma yang digunakan dalam proses enkripsi dan dekripsi adalah algoritma RSA dimana algoritma ini termasuk algoritma asimetris atau penggunaan dua kunci dalam proses dekripsi dan enkripsinya.

[3]. Penelitian yang di lakukan oleh Rian arifin dengan judul "*Implementasi Kriptografi dan Steganografi menggunakan Algoritma Rsa dan Metode LSB"*. Jurnal computer univesitas Negri Malang, 2004. Penelitian ini menggunakan metode RSA dan LSB Salah satu cara untuk menjaga keamanan pesan adalah menggunakan teknik steganografi. Metode steganografi yang digunakan adalah metode penyisipan pesan LSB (*Least Significant Bit*). Pesan rahasia disandikan sebelum disisipkan menggunakan teknik kriptografi. Algoritma kriptografi yang digunakan adalah algoritma RSA. Algoritma RSA terdiri dari algoritma enkripsi dan algoritma dekripsi. Pesan rahasia disandikan menggunakan algoritma enkripsi RSA dan disisipkan menggunakan metode penyisipan LSB. Membaca pesan dengan menggunakan metode LSB dan algoritma dekripsi RSA.

[4]. Penelitian yang di lakukan oleh Tumpal pandiangan, Suwoto, dengan judul *Aplikasi Kriptografi untuk Sistem Keamanan Penyimpanan Data Atau Informasi Hasil-Hasil Penelitian Yang Bersifat Rahasia.* Risalah Lokakarya komputasi dalam Sains dan Teknologi Nuklir XVI, Agustus 2005 (97-116). Aplikasi Kriptografi Salah

e-ISSN : 2541-1330
p-ISSN : 2541-1322

satu cara yang digunakan untuk pengamanan data dan atau informasi adalah menggunakan sistem kriptografi. Aplikasi ini, menggunakan algoritma MARS dengan modus ECB (Electronic Code Book). MARS sebagai salah satu kandidat AES(Advanced Encrypted Standard), memiliki kelebihan yaitu mempunyai tingkat keamanan dan proses kecepatan yang tinggi. Hal ini menjadikan algoritma MARS sebagai pilihan terbaik untuk proses enkripsi yang diperlukan oleh dunia informasi menuju abad berikutnya. Algoritma MARS menggunakan kunci 128 bit dan proses enkripsinya terdiri dari 32 ronde. Program ini dirancang dengan menyediakan unit sarana pengiriman file, baik untuk file yang telah dienkripsi maupun jenis file biasa. Hasil pengujian menunjukkan bahwa program ini dapat berjalan sesuai dengan spesifikasi rancangannya.

[5]. Penelitian yang di lakukan oleh Febrian Budi Utama dengan judul "*Studi dan Implementasi Algoritma RSA untuk pengamanan data Akademik Mahasiswa".* RSA adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Data transkrip akademik mahasiswa merupakan salah satu data yang harus dijaga keamanannya sehingga perlu diterapkan suatu teknik pengamanan dalam penyimpanannya. Pada makalah ini akan dibahas proses enkripsi (penyandian data) nilai transkrip akademik mahasiswa menggunakan algoritma Berdasarkan pengujian diperoleh waktu komputasi algoritma RSA adalah sebesar 15625 mikrodetik. Sedangkan kompleksitas memori yang dibutuhkan algoritma RSA sebesar 3908 bytes.

[6]. Penelitian yang di lakukan oleh Putra, satya andika dengan judul *Verifikasi Kepemilikan Citra Medis dengan Kriptografi RSA dan LSB Watermaking*. Jurnal Sains dan Matematika vol 19 (3): 75-81 (2001). Metode yang digunakan adalah dengan menyisipkan pesan teks kedalam sebuah data citra medis.perlindungan data citra medis perlu dilakukan agar tidak terjadi kesalahaninformasi kepemilikan data medis pasien satu dengan lainnya. Informasi yang di sembunyikan di dalam citra medis berupa teks yang sebelumnya dilakukan enkripsi atau pengacakan pesan.

[7]. Penelitian yang dilakukan oleh Supriyono dengan judul *Pengujian Sistem Enkripsi-Deskripsi Dengan Metode RSA Untuk Pengamanan Dokumen*. Jurnal Sekolah Tinggi Teknologi Nuklir Batan (2001). Telah diuji suatu model pengamanan dokumen yang dapat digunakan sebagai salah satu instrumen sistem pengamanan dokumen khususnya untuk dokumen teks. Adapun prinsip pengamanan dokumen ini adalah bagaimana sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen. Mula-mula dokumen dalam bentuk teks dienkripsi. Sehingga dokumen tidak dapat dibaca oleh siapapun. Karena teks telah berubah menjadi susunan huruf yang teracak. Dokumen yang susunan hurufnya telah teracak

e-ISSN : 2541-1330
p-ISSN : 2541-1322

tersebut jika ingin dibaca oleh pemilik dokumen, maka dokumen tersebut harus dibuka dengan dekripsi. Dalam penelitian ini, metode yang digunakan adalah metode RSA, dimana metode tersebut menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal (dengan private key maupun dengan public key) sehingga amat sulit untuk ditembus oleh hacker. Sistem ini dibangun dengan perangkat lunak Borland Delphi 7. Hasil pengujian ini menunjukkan bahwa sistem dapat menyimpan dan mengirimkan dokumen baik pengiriman melalui internet maupun intranet dalam bentuk susunan huruf yang terenkripsi dan mengembalikan ke bentuk dokumen semula dengan cara dekripsi. Dilakukan pula pengujian proses enkripsi dan dekripsi untuk dokumen dengan ukuran memori yang bermacam-macam.

[8]. Penelitian yang di lakukan oleh Muhammad, arif dengan judul *Kriptografi RSA pada Aplikasi File Client-Server Based*. Jurnal komputasi Universitas Telkom (2002). Perkembangan teknologi membuat kemudahan dalam berkomunikasi. Kemudahan ini juga membuat mudahnya tersebar data-data privat seseorang. Dibutuhkan suatu pengamanan data. Algoritma RSA merupakan algoritma kriptografi yang memiliki tingkat keamanan tinggi. Kunci RSA dengan panjang 1024 bit dapat memakan waktu ratusan tahun untuk dibobol jika menggunakan metode *brute force*. Dalam penelitian ini, enkripsi RSA pada file akan diimplementasikan dalam sebuah aplikasi FTP *client*. Saat proses *upload*, *file* akan dienkripsi sehingga *file* tersebut tidak bisa dibaca sembarang orang. Hanya yang memiliki kunci yang dapat membacanya. Dengan ini dihasilkan mekanisme berbagi *file* yang lebih aman walaupun menggunakan sebuah jaringan publik. Dari beberapa percobaan, dihasilkan bahwa algoritma RSA dapat digunakan untuk enkripsi dan dekripsi sebuah *file* untuk meningkatkan keamanan pada suatu jaringan publik. Namun dikarenakan penggunaan JVM yang terbatas, ukuran *file* yang dapat dienkripsi juga terbatas.

[9]. Penelitian yang di lakukan oleh Maharani, septya dengan judul *Implementasi Perangkat Lunak Penyadian Pesan Menggunakan Algoritma RSA*. Jurnal Informatika Mulawarman Vol.4 No.1 Feb 2010. Perkembangan teknologi telekomunikasi dan penyimpanan data dengan menggunakan computer memungkinkan pengiriman data jarak jauh menjadi relatife cepat dan murah. Kemajuan dan perkembangan kriptografi turut mempengaruhi perkembangan aplikasi pengirimian pesan yang disandikan. Kriptografi menjaga kerahasiaan informasi yang terkandung dalam pesan sehingga informasi tersebut tidak dapat diketahui oleh pihak yan tidak sah. Penelitian ini bertujuan untuk mengimplementasikan rancangan sistem penyandian pesan untuk menjadi perangkat lunak bantu yang sesungguhnya.. Tulisan kali ini memuat hasil implementasi sistem dalam bentuk algoritma pembangkitan

e-ISSN : 2541-1330
p-ISSN : 2541-1322

kunci, algoritma engkripsi dan dekripsi, integrasi dengan aplikasi pengiriman mail, serta tampilan antar muka perangkat lunak tersebut.

3. Landasan Teori

1. KRIPTOGRAFI

Kriptografi berasal dari akar kata Yunani kryptos dan gráphō, yang mempunyai arti "tulisan tersembunyi". Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman.

Kriptografi dapat memenuhi kebutuhan umum suatu transaksi, yaitu:

a. Kerahasiaan (*confidentiality*) dijamin dengan melakukan enkripsi (penyandian).

b. Keutuhan (*integrity*) atas data dilakukan dengan fungsi *hash* satu arah.

c. Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat *digital*. Sedangkan keotentikan data transaksi dapat dilakukan dengan tandatangan digital.

d. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non- repudiation*) dengan memanfaatkan tandatangan *digital* dan sertifikat *digital*.

2. RSA

Pada algoritma RSA terdapat tiga proses yaitu, pembangkitan kunci, proses enkripsi dan proses dekripsi. Letak kesulitan algoritma ini adalah bagaimana menemukan dua faktor bilangan prima yang besar yang akan digunakan sebagai kunci publik dan kunci privat. Dua bilangan prima besar tersebut p dan q dimana $p \neq q$.

Konsep utama keamanan dari RSA adalah susah pemfaktoran bilangan-bilangan besar menjadi faktor- faktor primanya. Terdapat besaran-besaran yang penting di algoritma RSA yakni :

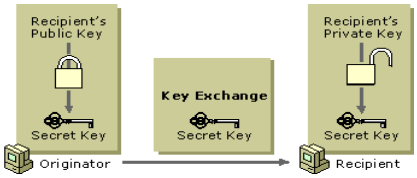
1. p dan q bilangan prima (rahasia)
2. n = p . q (tidak rahasia)
3. φ (n) = (p - 1) (q - 1) (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)
6. m (plainteks) (rahasia)
7. chiperteks (tidak rahasia)

Teknik operasi pembangkitan kunci pada RSA adalah sebagai berikut

1. Memilih dua bilangan prima berbeda p dan q.
   - Untuk alasan keamanan, bilangan bulat p dan q dipilih secara random.
2. Compute $n = pq$. Hitung n = p . q
   - n digunakan sebagai modulus dari kunci publik dan kunci privat.
3. Hitung $\varphi(n) = (p-1)(q-1)$, di mana φ is fungsi Euler tosien.
4. Pilih sebuah bilangan bulat e sehingga $1 < e < \varphi(n)$ dan faktor pembagi terbesar dari $(e, \varphi(n)) = 1$; i.e., e dan $\varphi(n)$ are relatif prima.
   - e digunakan sebagai eksponen kunci publik.
   - e mempunyai panjang bit yang pendek dan berat Hamming yang ringan menghasilkan hasil yang lebih efisien dalam enkripsi - umumnya 0x10001 = 65,537. Namun demikian, semakin kecil nilai e (such as 3) semakin kecil pula tingkat keamanan di hal– hal tertentu.
5. Berdasar technet.microsoft.com, penerapan RSA di dalam pertukaran kunci adalah dengan cara

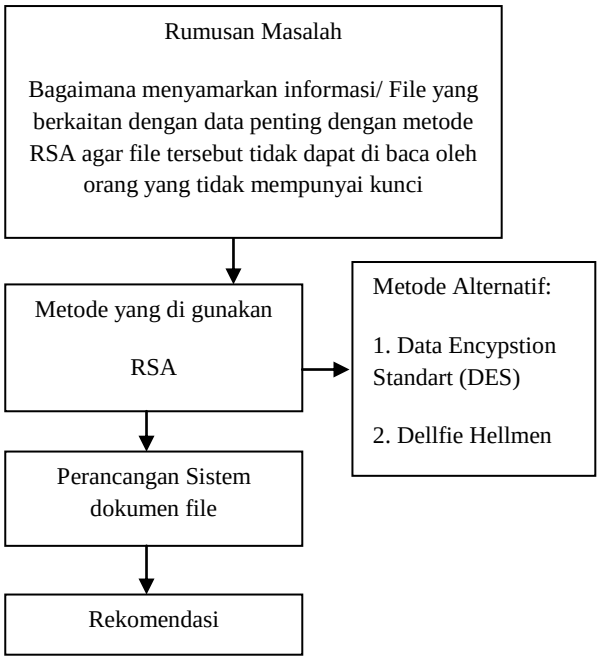
e-ISSN : 2541-1330
p-ISSN : 2541-1322

mengenkripsi kunci privat dari pesan dengan menggunakan kunci publik hasil pembangkitan dari RSA dan pesan berisi kunci itu dapat dibuka hanya dengan kunci privat hasil pembangkitan RSA yang dimiliki oleh penerima pesan. Berikut kurang lebih skema dari pertukaran kunci tersebut:



1. Gambar 2.2 Skema pertukaran kunci dengan RSA

II. KERANGKA PEMIKIRAN



Gambar 2. Kerangka Pemikiran

III. METODOLOGI PENELITIAN

Objek yang diteliti dalam penelitian tentang pengamanan e-dokumen dengan menggunakan metode *hybrid.* biometrik tandatangan dan DSA yaitu biometrik tandatangan *offline* dan e-dokumen. Tandatangan *offline* adalah *scan* tandatangan manual atau tandatangan beserta keterangan, misalnya nomer dokumen, tempat, tanggal, nama atau keterangan lainnya. Jenis file e-dokumen yang digunakan dalam penelitian ini berupa file dengan ekstensi : php, mp3, pptx, ppt, html, pdf, txt, bmp, sys, docx, doc, xlsx, xls, zip, exe, jpg. Sedangkan tandatangan *offline* yang digunakan dalam penelitian ini berupa *scan* tandatangan manual dalam file dengan ekstensi jpg.

Metode pengumpulan data dalam penelitian ini adalah sebagai berikut :

1. Observasi--Merupakan metode pengumpulan data dengan cara melakukan pengamatan secara langsung pada obyek yang diteliti yaitu biometrik tandatangan *offline* dan e-dokumen yang perlu diberi tandatangan *digital.*
2. Studi Pustaka--Merupakan metode pengumpulan data dengan cara mengumpulkan data-data dari berbagai sumber yang mendukung penelitian baik itu dari buku, jurnal ilmiah, makalah prosiding maupun artikel lainnya yang mendukung penelitian.

Alat penelitian yang digunakan dalam proses penelitian ini sebagai berikut :

1.
2.

Metode Alternatif:

1. Data Encyption Standart (DES)

2. Deffile Helman

IV. HASIL DAN PEMBAHASAN

Enkripsi menggunakan algoritma RSA terhadap *plaintext M = FISIKA*. Pertama-tama

e-ISSN : 2541-1330
p-ISSN : 2541-1322

plaintext tersebut diubah menjadi format ASCII sebagai beri-kut:

TEXT (Karakter)	F	I	S	I	K	A
ASCII (Hexa)	46	49	53	49	4B	41
ASCII (Decimal)	70	73	83	73	75	65

Tabel 1 Text karakter to Decimal

Plaintext dalam format ASCII desimal terse-but kemudian dipecah menjadi blok-blok tiga digit berikut :

mi = 707 *m3 = 737*

m2 = 383 *m4 = 565*

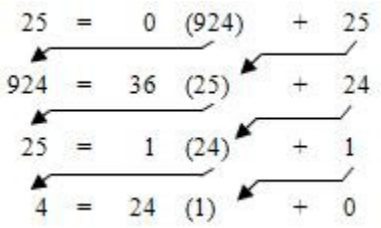
Dalam membuat kunci RSA, perlu dirancang agar nilai *mi* masih terletak di dalam ren-tang antara 0 sampai *n – 1*. Maka ditentu-kan bahwa nilai *n* minimal adalah 909. Nilai ini diambil berdasarkan pertimbangan bahwa karakter huruf kapital dengan nilai terbesar adalah Z dengan nilai ASCII yaitu 5Ah atau 90. Kombinasi ZZ akan dapat dipecah menjadi blok 909 atau 090.

Misalkan dipilih *p = 23* dan *q = 43* (keduanya prima), maka dapat dihitung

n = p x q = 989

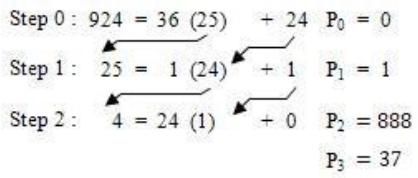
m = (p – 1) x (q – 1) = 924

Dipilih kunci publik *e = 25* (yang relatif prima dengan 924 karena pembagi ber-sama terbesarnya adalah 1). Bahwa 25 relatif prima terhadap 924 dapat dibuktikan dengan mencari nilai gcd (25,924) melalui algoritma Euclid seperti berikut.



Hasil gcd pada algoritma ini adalah hasil sisa bagi terakhir sebelum 0. Maka pada perhitungan diatas terlihat bahwa sisa bagi sebelum nol adalah 1. Maka gcd (25, 924) = 1.

Selanjutnya untuk menghitung kunci privat *d* algoritma Extended Euclid sebagai berikut.



P2 dan P3 dihitung melalui persamaan berikut

P2 = *(pi-2 – pi-1qi-2) mod n*

(0 – 1(36)) mod 924 = 888

P3 = (1 – 888(1)) mod 924 = 37

Maka diperoleh kunci publik adalah 25 dan 989. Sedangkan kunci privat adalah 37 dan 989. Enkripsi setiap blok diperoleh meng-gunakan kunci public 25 dan 989 dengan cara sebagai berikut :

c1 = 70725 mod 989

Untuk menghitung 70725 mod 989 dapat menggunakan teknik *divide and conquer* untuk membagi pemangkatnya sampai berukuran kecil. Ilustarinya adalah sebagai berikut

e-ISSN : 2541-1330
p-ISSN : 2541-1322

$$707^{25} = 707^{16} \cdot 707^{8} \cdot 707^{1}$$

$$707^{2} \bmod 989 = 499849 \bmod 989 = 404$$

$$\begin{aligned} 707^{4} \bmod 989 &= (707^{2} \cdot 707^{2}) \bmod 989 \\ &= [(707^{2} \bmod 989)(707^{2} \bmod 989)] \bmod 989 \\ &= (404 \cdot 404) \bmod 989 \\ &= 163216 \bmod 989 = 31 \end{aligned}$$

$$\begin{aligned} 707^{8} \bmod 989 &= (707^{4} \cdot 707^{4}) \bmod 989 \\ &= [(707^{4} \bmod 989)(707^{4} \bmod 989)] \bmod 989 \\ &= (31 \cdot 31) \bmod 989 \\ &= 961 \bmod 989 = 961 \end{aligned}$$

$$\begin{aligned} 707^{16} \bmod 989 &= (707^{8} \cdot 707^{8}) \bmod 989 \\ &= [(707^{8} \bmod 989)(707^{8} \bmod 989)] \bmod 989 \\ &= (961 \cdot 961) \bmod 989 \\ &= 923521 \bmod 989 = 784 \end{aligned}$$

$$\begin{aligned} 707^{25} \bmod 989 &= 707^{16} \cdot 707^{8} \cdot 707^{1} \bmod 989 \\ &= ((707^{16} \bmod 989 \cdot 707^{8} \bmod 989) \bmod 989 \cdot 707^{1} \bmod 989) \bmod 989 \\ &= ((784 \cdot 961) \bmod 989 \cdot 707) \bmod 989 \\ &= ((753424) \bmod 989 \cdot 707) \bmod 989 \\ &= (795 \cdot 707) \bmod 989 = 313 \end{aligned}$$

Jadi c1 = 70725 mod 989 = 313.

Dengan cara yang sama dapat diperoleh :

c2 = 38325 mod 989 = 776

c3 = 73725 mod 989 = 737

c4 = 56525 mod 989 = 909

Maka *ciphertext* adalah C = 313 776 737 909

Perlu diingat, bahwa *ciphertext* ini dalam format ASCII desimal. Jika diubah kembalimenjadi format karakter maka dapat diperoleh:

TEXT (Karakter)	-	%	L	1	0	-
ASCII (Hexa)	1F	24	4C	49	4F	09
ASCII (Decimal)	31	37	76	73	79	09

Tabel 2 Tabel Text karakter to Hexa

Untuk melakukan dekripsi (mengubah *ci-phertext* menjadi *plaintext*) maka digunakan kunci privat 37 dan 989 dengan cara seba-gai berikut :

m1 = 31337 mod 989 = 707

m2 = 77637 mod 989 = 383

m3 = 73737 mod 989 = 737

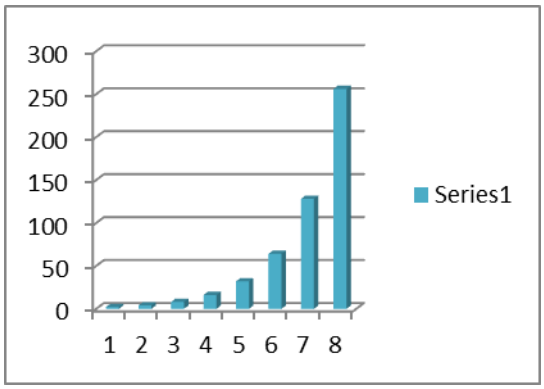
m4 = 90937 mod 989 = 565

Maka diperoleh *plaintext* 707 383 737 565

VARIABEL	DIPANGKATKAN	HASIL
(i) a = 1	2	2
(ii) a = 2	2 x 2	4
(iii) a = 3	2 x 4	8
(iv) a = 4	2 x 8	16
(v) a = 5	2 x 16	32
(vi) a = 6	2 x 32	64
(vii) a = 7	2 x 64	128
(viii) a = 8	2 x 128	256

Tabel 3 Tabel variable Komplesitas Metode Deffie dan RSA

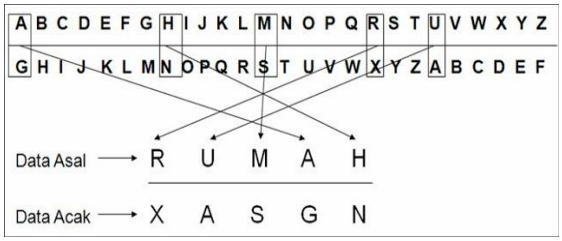
Apabila angka 2, 4, 8, 16, 32, 64, 128, 256 tersebut digambarkan dalam bentuk kurva maka bentuknya akan menaik secara eksponensial seperti di bawah ini.



Gambar 3 Grafik Hasil Kompleksitas perbandigan metode Deffie dan RSA

e-ISSN : 2541-1330
p-ISSN : 2541-1322

Gambar tabeldi atas merupakan perbandingan yang di lakukan dengan menggunakan metode RSA danDeffie Hellman, di dapat untuk jarak ke titik 8 metode RSA lebi unggul. Ini maksudnya untuak jarak yang lama dalam waktu RSA lebih unggul dan lebih susah untuk di tembus.



Gambar 4. Gambar hitungan kata Rumah

V. KESIMPULAN DAN SARAN

Kesimpulan yang dapat diambil dari studi pemakaian RSA adalah:

- Cara penyamaran isi file dari segi teknis penghitungan, sistem RSA mempunyai cara enkripsi yang mudah, tetapi jika sudah dienkripsi, data yang terenkripsi sulit untuk dibobol jika hanya mempunyai kunci publiknya saja, Belum ada teknik pembobolan lain yang lebih efektif daripada *brute force attack*, jadi untuk ukuran kunci yang panjang, sistem penyandian dengan RSA masih baik dan sulit untuk dibobol
- File dari pengiriman yang mana dalam proses pembuatan kunci actor dan kunci privat, terdapat beberapa actor yang menjadi pertimbangan, yaitu ukuran dari kunci, penentuan nilai *p* dan *q* agar sulit untuk dibobol, dan kemungkinan-kemungkinan
  kelemahan yang dapat diketahui saat data selesai dienkripsi

Untuk menyempurnakan hasil penelitian ini, beberapa hal yang disarankan untuk dilakukan adalah:

- Agar Metode ini dapat terus di kembangkan, karena metode ini tidak begitu rumit bila di bandingkan dengan metode lain seperti deffie hellman, End of file, dll. Maka metode ini tetap dapat diketahui cara untuk membobolnya.

REFERENSI

[1]. Ary Reza Nugraha, Ary Mazharuddin S, *Penyembunyian pesan rahasia yang terenkripsi menggunakan algoritma RSA pada media kompresi*. Jurusan Teknik Informatika Fakultas Teknologi Informasi, Institut teknologi Sepuluh Nopember (ITS), Surabaya. Jurnal Teknik PomITS Vol2, No.1, (2013), ISSN 2337-3539 (2301-9271)
Ary.shiddiqi@cs.its.ac.id.

[2]. Aditya Permana, Edy Santoso, Dian Eka Ratnawati, *Kriptografi Pada File Dokumen Microsoft Office Menggunakan Metode RSA*. Program Studi Ilmu Komputer Fakultas Teknologi Informasi Universitas Brawijaya Malang.
0810963028@mail.uba.ac.id,
edy144@uba.ac.id,
dianilkom@uba.ac.id.

[3]. Rian arifin. Lucky Tri Oktoviana, *judul Implementasi Kriptografi dan Steganografi menggunakan Algoritma Rsa dan Metode LSB*. Program Studi Matematika Universitas Negri Malang. arifin199@gmail.com,

[4]. Tumpal Pandiangan, Suwoto, Zuhair, Ferhat Aziz, *Aplikasi Kriptografi Untuk Sistem Keamanan Penyimpanan Data atau Informasi Hasil-Hasil Penelitian yang bersifat Rahasia*. Jurnal Lokakarya Komputasi dalam Sains dan Teknologi Nuklir XVI, Agustus 2005 (97-116).

[5]. Tri Raharjonngroem, Muhammad Aria, *Studi dan Implementasi*

e-ISSN : 2541-1330
p-ISSN : 2541-1322

Algoritma RSA Untuk Pengaman DataTranskip Akademik Mahasiswa, Jurnal Ilmiah Unikom Vol 08, 01 Hal 77-90.

[6]. Satya Sandika Putra, Priyo Sidik Sasongko, Nurdin Bahtiar, *Verifikasi Kepemilikan Citra Medis dengan Kriptografi RSA dan LSB Watermaking*, Jurnal Sains Dan Matimatika Vol 19 (3): 75-81 (2011).

[7]. Supriyono, *Pengujian Sistem Enkripsi-Deskripsi dengan Metode RSA untuk Pengaman Dokumen*, Jurnal JFN Vol 2 No.2 Nov 2008.

[8]. Muhammad Arief, Fitriyani, Nurul Ikhsan, *Kriptografi RSA Pada Aplikasi File Transfer Client-Server Based*, Prodi Ilmu Komputasi Universitas Telkom bandung, Ariefmuhammad08@gmail.com, Fitriyani.y@gmail.com.

[9]. Septya Maharani, Fahrul Agus, *Implementasi Perangkat Lunak Penyandian PesanMenggunakan Algoritma RSA*, Jurnal Informatika Mulawarman Vol 04, No.1 Feb 2009.

Leo Benny, lahir di Tebing Tinggi, tanggal 09 October 1987 jenis kelamin laki-laki. Memperoleh gelar Sarjana Komputer (S.Kom) dibidang Teknik Informatika dari STMIK IBBI Medan, saat ini sedang kuliah dalam penyusunan tesis di STMIK Eresha Program studi Teknik Informatika jenjang Strata 2 (S2) Magister Komputer. Bekerja sebagai Dosen pada STMIK ITMI Medan.