IMPLEMENTASI DAN PERBANDINGAN KRIPTOGRAFI ALGORTIMA DES DAN RSA UNTUK PENYANDIAN DATA

Aziz Nofiyanto Nugroho[1], Andrian Rakhmatsyah[2], Endro Ariyanto[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Pengiriman data-data penting melalui akses internet pada masa sekarang sudah menjadi hal yang biasa. Hal ini menimbulkan semakin berkembangnya dunia kejahatan melalui jaringan internet, seperti penyadapan, pencurian, dan pemalsuan data informasi yang dikirim melalui internet terutama dalam sektor bisnis, perbankan, perdagangan, sampai sektor pemerintahan. Karena itulah kriptografi menjadi pilihan untuk melindungi data.

RSA(Rivers Shamir Adleman) merupakan algoritma kriptografi yang dianggap aman, karena RSA memiliki pemfaktoran bilangan prima yang sangat besar. Sedangkan DES(Data Encryption Standart) merupakan algoritma yang menjadi pilihan untuk menjaga keamanan data. Misalnya digunakan dalam kartu chip yang dimiliki oleh para nasabah bank. DES menggunakan kunci yang sama untuk menyandi (enkripsi) maupun untuk menterjemahan (dekripsi), sedangkan RSA menggunakan dua kunci yang berbeda. Istilahnya, DES disebut sistem sandi simetris sementara RSA disebut sistem sandi asimetris.

Pada Tugas Akhir ini dibuat perangkat lunak untuk menganalisis performansi kedua algoritma dengan parameter : waktu enkripsi, waktu dekripsi, penggunaan memori dan pembengkakan ukuran chipertext. Kesimpulan yang dapat diambil berdasarkan pengujian dan analisis yang dilakukan, didapatkan bahwa RSA dengan menggunakan kunci besar dianggap lebih baik dibandingkan dengan algoritma DES.

Kata Kunci : Kriptografi, DES, RSA

Abstract

Delivery of important data through accessing internet in this period have become commonplace. This matter generate progressively expand the badness through internet like increasing of badness taping, theft and forgery of information data sent through internet especially in business, banking, commerce, until the governance sector. For that, cryptography becomes a choice to pacify data.

RSA(Rivers Shamir Adleman) represent secure assumed cryptography algorithm, because of RSA have factoring that very big prime number. Others, DES is an algorithm that becoming choice to take care of data security. For example, DES is used in chip card owned by all bank clients. DES use same key to encode (encryption) and also for translation (description), while RSA use two different key. Equally, DES referred as symmetrical encode system whereas RSA referred as unsymmetrical encode system.

This Final Task made software to analyze performance both of the algorithms by parameters: encryption time, description time, using of memory, and increasing of chipertext size. After get the conclusion taken pursuant to examination and analysis from the software hence got that RSA algorithm by using big key is better than by DES algorithm.

Keywords : cryptography, DES, RSA.

1. Pendahuluan

1.1 Latar belakang

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikan. Ketika suatu pesan dikirim dari satu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat disadap oleh pihak lain. Untuk menjaga keamanan pesan, maka pesan tersebut dapat diacak atau diubah menjadi kode yang tidak dimengerti orang lain, namun dapat dikembalikan menjadi pesan semula. Perlindungan terhadap kerahasiaan datapun meningkat, salah satu caranya adalah dengan penyandian data atau enkripsi. Sebagai media komunikasi umum, Internet sangat rawan terhadap penyadapan, pencurian, dan pemalsuan informasi. Karena itu eksploitasi Internet oleh sektor-sektor strategis seperti bisnis, perbankan, atau pemerintahan sangat memerlukan teknologi penyandian Informasi.

Ada beberapa teknik yang dapat digunakan untuk menerapkan sistem kriptografi, yaitu konvensional dan kunci publik. Pada kriptografi konvensional, untuk mengubah *plaintext* ke bentuk chipertext dan proses kebalikannya menggunakan kunci yang sama atau disebut juga *symetric*, sedangkan pada kriptografi kunci publik atau disebut juga kriptografi *asymetrik*, diperlukan 2 buah kunci. Satu kunci yang disebut kunci publik (*publik key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Algoritma DES (Data Encryption Standard) sebagai salah satu algoritma kriptografi *symetric*, memiliki blok kunci 64 bit tetapi yang digunakan dalam eksekusi hanya 56 bit dan merupakan algoritma enkripsi yang paling banyak digunakan di dunia, karena secara teori blok kunci 56 bit termasuk algoritma enkripsi yang mudah yang kuat dan tidak mudah di terobos [8]. Algoritma DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk keluarga block *chiper*. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Algoritma DES sangat banyak digunakan untuk melindungi data dalam dunia elektronik khususnya di bidang perbankan, finansial, dan *e-commers*. Hingga kini algoritma DES masih kebal terhadap *cryptanalysis* baik yang berjenis *linier cryptoanalysis* maupun *differential cryptanalysis*, dua teknik yang dikenal sebagai cara yang paling ampuh untuk memecahkan sandi modern [4].

Algoritma kunci publik yang paling umum digunakan adalah RSA(Rivest Shamir Adleman). RSA dianggap aman karena sulitnya pemfaktoran bilangan yang sangat besar meskipun tidak pernah dibuktikan aman tidaknya [7]. Dilihat dari persamaan matematisnya, algoritma RSA sulit dipecahkan karena sulitnya pemfaktoran bilangan prima yang sangat besar. Jumlah bilangan prima yang tersedia pada bilangan 512 bit adalah sekitar 10 pangkat 151, jika terdapat mendapatkan 1000 bilangan prima, maka diperlukan hanya 1000 milyar (10 pangkat 12) bilangan prima yang berbeda untuk memenuhinya. Jumlah ini cukup

kecil jika dibandingkan bilangan prima yang tersedia pada 512 bit (sekitar 10 pangkat 151), apalagi jika menggunakan 1024 bit (tersedia sekitar 10 pangkat 305 bilangan prima) [9].

Pada kenyataanya RSA dianggap aman karena memiliki pemfaktoran bialangan prima yang besar, walaupun belum pernah ada yang membuktikan, sedangkan algoritma DES banyak diterapkan dalam dunia nyata terutama dalam dunia perbankan. Oleh karena itu diperlukan suatu pengujian terhadap algoritma DES sebagai algoritma *symetrik* dan membandingkannya dengan algoritma *asymetrik* yang umum digunakan yaitu algoritma RSA. Pengujian dilakukan terhadap file (*.txt) menggunakan perangkat lunak sebagai simulasi suatu sistem kriptografi yang menggunakan algoritma DES dan RSA.

1.2 Perumusan masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana membangun prangkat lunak berdasarkan algoritma kriptografi DES dan algoritma RSA.
2. Menganalisis performansi implementasi perangkat lunak kriptografi algortima DES dan RSA berdasarkan parameter tertentu.

Adapun batasan masalah tugas akhir ini adalah sebagai berikut :

1. Data atau pesan yang dienkripi atau didekripsi berupa text.
2. Perangkat lunak yang dihasilkan merupakan simulasi dari kedua algoritma.
3. Algoritma RSA yang digunakan memiliki kunci 8 bit, 16 bit, dan 24 bit.
4. Algoritma DES enkripsi data pada 64 bit

1.3 Tujuan

1. Mengimplementasikan Algoritma DES dan RSA dalam bentuk perangkat lunak
2. Menganalisis performansi algoritma RSA berdasarkan jumlah kunci, pembengkakan *chipertext*, dan pemakaian memori pada saat proses enkripsi dan dekripsi. Yang kemudian dibandingkan dengan algoritma DES

1.4 Metodologi penyelesaian masalah

Metode yang digunakan dalam penyelesaian tugas akhir ini adalah menggunakan metode studi pustaka atau studi literatur dan analisis dengan langkah kerja sebagai berikut:

1. Studi Literatur:
   a. Pencarian referensi
      Mencari referensi dan sumber-sumber lain yang layak yang berhubungan dengan materi kriptografi terutama mengenai algoritma DES dan algoritma RSA.

b. Pendalaman materi
   Mempelajari dan memahami materi yang berhubungan dengan tugas akhir ini.

2. Mempelajari konsep dasar dari kedua algoritma (algoritma DES dan RSA) secara detail yang digunakan sebagai langkah awal dalam mendesain perangkat lunak.
3. Melakukan perancangan dan implementasi perangkat lunak. Bertujuan merancang perangkat lunak yang dibuat, metode pengembangan perngkat lunak yang digunakan adalah model *waterfall* yang disebut juga *clasic life cycle*.
4. Pengujian dan analisis. Bertujuan menganalisis apakah perangkat lunak yang dibuat sesuai dengan spesifikasi yang diinginkan. Analisis dilakukan terhadap kedua algoritma setelah perangkat lunak selesai dibuat.
5. Pengambilan kesimpulan dan penyusunan laporan tugas akhir. Merupakan hasil analisis perbandingan dari kedua algoritma berdasarkan perangkat lunak yang telah dibuat.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan implementasi dan analisis data uji yang telah dilakukan, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Dari segi waktu, algoritma RSA 24 bit dinilai lebih cepat daripada algoritma DES
2. Dari segi kebutuhan memory pada saat proses enkripsi dan dekripsi, RSA 8 bit dan RSA 16 bit memerlukan banyak memori dibandingkan DES. Tetapi RSA 24 lebih sedikit memakan memori dibandingkan DES. Ini berarti RSA 24 bit lebih sedikit menggunakan memori dibandingkan dengan RSA 8 bit, RSA 16, dan DES 64.
3. Berdasarkan hasil uji coba yang telah dilakuakan, besar file berpengaruh kecepatan proses enkripsi/dekripsi, semakin besar file yang akan diproses semakin lama waktu proses file tersebut.
4. Ukuran *chipertext* pada Algoritma RSA yang dihasilkan 1 sampai 6 kali lipat ukuran *plaintext*nya, sedangkan pada DES pembengkakan ukuran chipertext yang terjadi 1 sampai 4 kali lipatnya.
5. Ukuran *plaintext* berpengaruh pada lamanya proses dan pembengkakan chipertext. Semakin besar ukuran *plaintext*, semakin lama proses enkripsi dan dekripsi

5.2 Saran

1. Untuk kelanjutan dari tugas akhir ini diharapkan dapat dilakukan analisis yang lebih mendalam seperti tentang tingkat ketahanan algoritma DES terhadap percobaan serangan dari luar.
2. Perangkat lunak yang digunakan sebaiknya dapat dijalankan tidak hanya dalam satu komputer saja, namun dapat diterapkan di dalam jaringan komputer.
3. Untuk kelanjutan dari tugas akhir ini diharapkan dapat dilakukan untuk berbagai macam tipe file, tidak hanya terbatas pada file tipe text (*.txt)
4. Cara pembuatan perangkat lunak pada masing-masing orang mungkin akan berbeda, ini akan sangat berpengaruh pada pemakaian memori dan waktu.
5. Penggunaan Kunci pada RSA akan lebih baik menggunakan bit yang lebih besar.

Daftar Pustaka

[1] Ariyus, Doni. 2006. *Computer Security*. Andi:Yogyakarta

[2] Brenton, Chris & Cameron Hunt. 2003. *Network Security*. Sybex :USA

[3] FIPS PUB 46-2, Data Encryption Standard (DES) http://www.itl.nist.gov/pspubs/p46-2.htm

[4] Hasan, Rusyd. 2003. Mengenal Algoritma DES. Copyright©2003-2006 IlmuKomputer.com, tanggal download : 7 Januari 2007

[5] Heru, Irman. 1996. *Studi dan Implementasi Algoritma Kriptografi Kunci Publik RSA dan LUC untuk Penyandian Data*

[6] ITHB. *Artikel Ilmiah:Ada Apa Dengan Kriptografi ?:* http: //www.ITHB e-Magazine Oktober 2004, tanggal download: 15 September 2005

[7] Kavita, Jajang. 2004. *Analisis Perbandingan Performansi RSA dan Elliptic Curve Cryptography (ECC) pada Protokol Secure Socket Layer*

[8] Komputer, Wahana. 2003. *Memahami Model Enkripsi dan Security Data*. Andi: Yogyakarta

[9] Kurniawan, Yusuf, MT. 2004. *Kriptografi Keamanan Internet dan Jaringan telekomunikasi*. Penerbit Informatika: Bandung

[10] Prasetya, ISWB. *Mengupas Rahasia Penyandian Informasi* : http://www. Infokom Edisi Internet - Cakrawala Edisi Juni 1998, tanggal download: 15 Januari 2007

[11] Riverst, R. L, Shamir, Adleman "*A Method for Obtaining Digital Signatures and Public Key Cryptosystems*", Communication of The ACM Vol 21, No. 2 February 1978

[12] Schafer, Gunter. 2003. *Securuty in Fixed and Wireless Networks: An Introduction to Securing Data Communications*. Willey: Inggris

[13] Schneier, B. *Applied Cryptography, 2nd*. Wiley: Kanada

[14] Stalling, William. 1999. *Cryptography And Network security*. Prentice Hall.