PENGKODEAN PESAN MENGGUNAKAN PERPADUAN CAESAR CIPHER DAN RSA PADA KRIPTOGRAFI HIBRIDA

SKRIPSI SARJANA MATEMATIKA

OLEH :

SILVIA ANNELIS
05134045

JURUSAN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS ANDALAS

PADANG

2010

ABSTRAK

Kriptografi Hibrida adalah suatu algoritma yang memadukan kriptografi klasik dengan kriptografi kunci-publik. Kriptografi Hibrida ini memanfaatkan dua tingkatan kunci yaitu kunci simetri untuk enkripsi dan dekripsi pesan dan pasangan kunci privat dengan kunci publik untuk melindungi kunci simetri. Dalam skripsi ini pembahasan difokuskan pada perpaduan Caesar Cipher dan RSA.

Kata kunci : *Kriptografi Hibrida, Algoritma, Kunci Simetri, Enkripsi, Dekripsi, Kunci Privat, Kunci Publik.*

BAB I

PENDAHULUAN

1.1. Latar Belakang

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu informasi rahasia. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia ini. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan sulit untuk mengetahui isi informasi yang sebenarnya. Ilmu yang membahas tentang metode penyandian ini disebut dengan kriptografi. Kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Cipherteks inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai pada penerima, cipherteks tersebut ditranformasikan kembali ke dalam bentuk plainteks agar dapat dikenali. Pengamanan informasi tersebut selain bertujuan untuk melindungi informasi agar tidak dapat diakses oleh orang-orang yang tidak berhak juga berfungsi untuk mencegah terjadinya penyisipan atau penghapusan informasi oleh pihak yang tidak bertanggung-jawab.

Kriptografi klasik merupakan kriptografi yang menggunakan satu kunci untuk mengamankan pesan sehingga kerahasiaan pesan tidak terjamin, namun dalam proses pengerjaannya membutuhkan waktu komputasi relatif lebih singkat. Sedangkan kriptografi kunci-publik menggunakan dua tingkatan kunci yaitu kunci privat dan kunci publik sehingga kerahasiaan pesan lebih terjamin, namun proses

pengerjaannya memakan waktu komputasi yang lebih lama dibandingkan kriptografi klasik. Masing-masing algoritma di atas memiliki kekurangan dan kelebihan. Berdasarkan hal itu dibuatlah suatu sistem yang memanfaatkan kedua algoritma di atas yaitu sistem hibrida atau disebut juga kriptografi hibrida. Salah satunya dengan menggabungkan Caesar Cipher dengan RSA (*Rivest Shamir Adleman*).

1.2. Perumusan Masalah

Berdasarkan hal di atas diperoleh suatu perumusan masalah penulisan tugas akhir ini yaitu "Bagaimana mekanisme kerja enkripsi dan dekripsi pesan dengan menggunakan Caesar Cipher, RSA, dan kriptografi Hibrida ?" serta "Bagaimana penerapannya pada contoh soal ?".

1.3. Pembatasan Masalah

Penulisan tugas akhir ini hanya membahas perpaduan antara Caesar Cipher dan RSA dalam sebuah sistem kriptografi hibrida.

1.4. Tujuan Penulisan

Adapun tujuan dari penulisan tugas akhir ini adalah untuk mempelajari enkripsi dan dekripsi pesan menggunakan Caesar Cipher, RSA dan kriptografi hibrida serta menerapkannya pada contoh soal.

1.5. Sistematika Penulisan

Pada Bab I, diuraikan tentang latar belakang, permasalahan, pembatasan masalah, tujuan, dan sistematika penulisan tugas akhir ini. Konsep dasar yang berhubungan dengan kriptografi seperti definisi kriptografi, algoritma kriptografi, teori bilangan, aritmetika modulo serta beberapa teori pendukung yang digunakan

BAB IV

KESIMPULAN

Adapun kesimpulan yang dapat diambil dari pembahasan skripsi ini adalah memadukan Caesar Cipher dengan RSA pada kriptografi Hibrida untuk menjamin kerahasiaan pesan serta dapat mengurangi waktu komputasi yang terlalu lama dalam proses enkripsi dan dekripsi pesan. Kriptografi ini menggunakan dua tingkatan kunci yaitu kunci simetri dan pasangan kunci privat dengan pasangan kunci publik. Dalam hal ini. Plainteks $\mathbb{M}$ dienkripsi menggunakan kunci *Caesar Cipher* menjadi cipherteks $\mathbb{C}_1$ selanjutnya kunci *Caesar Cipher* tersebut dienkripsi menjadi cipherteks $\mathbb{C}_2$ menggunakan pasangan kunci publik *RSA*. Selanjutnya dekripsi cipherteks $\mathbb{C}_2$ menjadi kunci *Caesar Cipher* menggunakan pasangan kunci privat *RSA*. Setelah diperoleh kunci *Caesar Cipher* hasil dekripsi tersebut maka selanjutnya dekripsi $\mathbb{C}_1$ menjadi plainteks $\mathbb{M}$ semula dengan kunci tersebut.

DAFTAR PUSTAKA

[1] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*. ANDI, Yogyakarta.

[2] Durbin, J. R. 2000. *Modern Algebra An Introduction*. New York. John Wiley and Sons, Inc.

[3] Hoffstein, J, Hill Pipher dan Joseph. H. S. 2008. *An Introduction to Mathematical Cryptography*. Springer Science+Bussines Media. LLC.

[4] Lipschutz, Seymour. 1989. *Teori Himpunan*. Erlangga, Jakarta.

[5] Menezes, A. V. O. dan S. Vanstone. 1997. *Handbook Of Applied Cryptography*. ISC Press.

[6] Munir, R. 2006. *Kriptografi*. Informatika, Bandung.

[7] Munir, R. 2005. *Matematika Diskrit*, edisi-3. Informatika, Bandung.

[8] Purcell, J. Edwin. 1987.*Kalkulus*. edisi-5, jilid 1.Erlangga, Jakarta.

[9] Rosen. K. H. 2007. *An Introduction to Cryptography*. Taylor & Francis Group. *LLC*.

ABSTRAK

Kriptografi Hibrida adalah suatu algoritma yang memadukan kriptografi klasik dengan kriptografi kunci-publik. Kriptografi Hibrida ini memanfaatkan dua tingkatan kunci yaitu kunci simetri untuk enkripsi dan dekripsi pesan dan pasangan kunci privat dengan kunci publik untuk melindungi kunci simetri. Dalam skripsi ini pembahasan difokuskan pada perpaduan Caesar Cipher dan RSA.

Kata kunci : *Kriptografi Hibrida, Algoritma, Kunci Simetri, Enkripsi, Dekripsi, Kunci Privat, Kunci Publik.*