BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi komputer dan telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Salah satu perkembangan yang sangat signifikan adalah penggunaan e-mail untuk pertukaran informasi atau pesan melalui jaringan internet. Namun demikian perlu diperhatikan tingkat keamanan informasi tersebut, karena e-mail menggunakan jaringan internet yang merupakan infrastruktur telekomunikasi dengan standar terbuka yang dapat dipergunakan oleh banyak pihak. Penyadapan informasi merupakan hal yang sangat merugikan bagi pengguna jaringan komunikasi saat ini. Dengan adanya kemungkinan penyadapan informasi tersebut, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting. Hal ini akan membuat para pengguna jaringan komunikasi merasa aman dan nyaman.

Kriptografi merupakan salah satu teknik yang dapat memberikan beberapa layanan yang mendukung untuk meningkatkan keamanan informasi antara lain otentikasi (*authentication*), nirpenyangkalan (*non-repudiation*) dan kerahasiaan (*confidentiality*). Otentikasi merupakan layanan yang berhubungan dengan identifikasi kebenaran sumber pesan. Nirpenyangkalan merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan yaitu pengirim pesan menyangkal melakukan pengiriman pesan.

Sedangkan kerahasiaan adalah layanan yang ditujukan untuk menjaga agar informasi atau pesan tidak dapat dibaca oleh pihak yang tidak berhak yaitu melalui proses enkripsi dan dekripsi.

Proses enkripsi yaitu mengubah pesan asli (*plaintext*) menjadi pesan dalam bentuk tersandi (*ciphertext*). Proses enkripsi akan menghasilkan data tersandi dan hanya dapat dibuka atau dibaca oleh pihak penerima yang memilki kunci (*key*) sedangkan proses dekripsi adalah mengembalikan data tersandi menjadi bentuk data asli. Proses enkripsi dan dekripsi yang dilakukan dengan menggunakan kunci yang sama dikenal dengan istilah kriptografi algoritma kunci simetri. Pada algoritma jenis ini, kunci bersifat rahasia dan hanya boleh diketahui oleh pihak pengirim dan penerima saja. Selain kriptografi algoritma kunci simetri telah dikembangkan juga kriptografi algoritma kunci asimetri, yaitu proses enkripsi dan dekripsi yang dilakukan dengan menggunakan kunci yang berbeda. Terdapat sepasang kunci yaitu kunci publik (*public key*) yang digunakan untuk proses enkripsi dan kunci privat (*privat key*) yang digunakan untuk proses dekripsi. Kunci publik tidak bersifat rahasia dan harus diketahui oleh pengirim pada saat akan mengenkripsi data. Sebaliknya untuk kunci privat adalah bersifat rahasia dan hanya diketahui oleh penerima data.

Penelitian ini adalah merancang perangkat lunak yang dapat digunakan untuk keamanan informasi yang akan dikirimkan menggunakan e-mail. Kriptografi algoritma kunci simetri AES (*Advanced Encryption Standard*) dipilih untuk proses enkripsi dan dekripsi informasi, sedangkan

kriptografi algoritma kunci asimetri RSA (*Rivest-Shamir-Adlemen*) digunakan untuk proses enkripsi dan dekripsi kunci rahasia dari algoritma AES serta untuk pemberian tanda tangan digital.

Informasi yang dikirim melalui e-mail menjadi lebih aman setelah diubah ke dalam bentuk data tersandi dan pemberian tanda tangan digital. Karena informasi (pesan) hanya dapat dibaca oleh pihak yang berhak dan penerima informasi dapat mengidentifikasi kebenaran sumber pengirim pesan. Hasil dari penelitian ini dapat digunakan untuk meningkatkan keamanan informasi yang dikirimkan melalui e-mail, sehingga pengirim dan penerima informasi merasa lebih aman terhadap informasi yang telah dikirim atau diterimanya.

1.2 Perumusan Masalah

Perumusan masalah dalam penelitian ini adalah:

a. Bagaimana merancang perangkat lunak yang dapat mengimplementasikan kriptografi algoritma AES dan RSA untuk keamanan informasi (pesan) pada e-mail yang meliputi kerahasiaan (*confidentiality*), otentikasi (a*uthenticatio*n) dan nirpenyangkalan (*non-repudiation***).**
b. Bagaimana menerapkan penggunaan kriptografi algoritma AES dan RSA
c. Bagaimana memberikan tanda tangan digital pada informasi (pesan) dengan menggunakan kriptografi algoritma RSA.

1.3 Batasan Masalah

Penulis menyadari bahwa untuk melakukan penelitian seperti yang telah dijelaskan pada rumusan masalah merupakan masalah yang masih cukup luas. Oleh sebab itu maka penulis membatasi penelitian ini sebagai berikut:

a. Algoritma yang digunakan adalah algoritma hybrid yang merupakan kombinasi dari algoritma AES dan RSA.
b. Informasi (*plaintext*) yang akan diproses oleh algoritma AES berbentuk teks dan dokumen.
c. Besarnya informasi maksimum adalah 500 Kilo Byte.
d. Algoritma RSA disusun menggunakan bilangan prima dengan panjang digit maksimum 400 digit.
e. Perangkat lunak yang digunakan adalah Matlab.
f. Pada perancangan sistem dengan metode Waterfall dibatasi hanya sampai tahap pengujian (testing).
g. Melakukan pengujian hasil proses enkripsi dan dekripsi agar data dapat disandikan dan dikembalikan ke bentuk aslinya dengan benar.
h. Melakukan pengujian terhadap ukuran data rahasia dan kunci rahasia yang dihasilkan.
i. Melakukan pengujian terhadap waktu yang diperlukan untuk mengerjakan proses enkripsi dan dekripsi.
j. Pemberian tanda tangan digital menggunakan algoritma RSA

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah merancang perangkat lunak yang dapat digunakan untuk keamanan informasi yang dikirimkan melalui e-mail dengan menggunakan algoritma AES dan RSA.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat antara lain

a. Bagi para pengguna jaringan komunikasi terutama pada saat pertukaran informasi melalui e-mail dapat dilakukan secara aman.

b. Menjadi referensi bagi kegiatan penelitian yang berhubungan dengan:

    1. Penerapan kriptografi menggunakan algoritma AES untuk meningkatkan keamanan data.
    2. Penerapan kriptografi menggunakan algoritma RSA untuk meningkatkan keamanan dan memudahkan pendistribusian kunci.
    3. Proses komputasi yang dilakukan pada algoritma AES dan RSA.
    4. Alokasi waktu dan ruang penyimpan yang dibutuhkan oleh proses enkripsi dan dekripsi pada algoritma AES dan RSA.
    5. Pemberian tanda tangan digital pada e-mail.
    6. Pengembangan perangkat lunak yang mengimplementasikan algoritma AES dan RSA.

1.6 Keaslian Penelitian

Beberapa penelitian dengan topik sejenis adalah sebagai berikut :

1. Levi Albert and Ozcan Mahmut, 2004, “Practical and Secure E-mail System (PractiSES)” Sabanci University Faculty of Engineering and Natural Sciences, Orhanli,Tuzla, TR-34956 Istanbul, Turkey.

   Penelitian ini mengusulkan sistem pengamanan e-mail yaitu pada proses distribusi dan mengelola kunci. Sistem ini dikembangkan menggunakan JCE 1.2.2 (Java Cryptographic Environment) untuk pemakaian beberapa algoritma berikut: RSA 2048 bit dan SHA-1 (keperluan pertukaran kunci), Triple DES (keperluan enkripsi dan dekripsi), dan Hash-Based MAC (HMAC) (keperluan integritas dan autentikasi pesan).

2. Khurana Himanshu, Slagell Adam , dan Bonilla Rafael, 2005, “SELS: A Secure E-mail List Service”, The 20th ACM Symposium on Applied Computing, 13-17 March 2005, Santa Fe, New Mexico, USA.

   Penelitian ini mengusulkan sistem pengamanan e-mail di dalam hal: *integrity*, *confidentiality*, *authentication*, dan *anti-spamming*. Pada pengamanan yang berhubungan dengan *confidentiality*, proses enkripsi dan dekripsi pesan menggunakan algoritma triple-DES dan ElGamal. Sistem SELS dikembangkan menggunakan bahasa pemrograman Java dan dapat diintegrasikan dengan program e-mail client Eudora melalui *eudora’s command-line interface and filters.*

Penelitian yang akan kami kembangkan berjudul “Perancangan Perangkat Lunak Untuk Keamanan Informasi Pada E-mail Dengan Menggunakan Algoritma AES dan RSA”. Pada penelitian ini, algoritma AES digunakan untuk proses

enkripsi dan dekripsi file lampiran pada e-mail sedangkan algoritma RSA digunakan untuk proses enkripsi dan dekripsi kunci dari algoritma AES serta pemberian tanda tangan digital. Media e-mail dipilih untuk mengirimkan informasi dikarenakan pada saat ini pemanfaatan e-mail telah umum digunakan untuk bertukar informasi.

Kelebihan dari penelitian yang akan kami kembangkan meliputi pemilihan algoritma AES dan RSA serta implementasi penelitian berupa perangkat lunak yang bermanfaat dan mudah digunakan. Algoritma AES memiliki beberapa kelebihan yaitu (Song , 2004, h.92; Stinson, 2002, h.102).

a. Security

   Setiap putaran pada algoritma AES akan menghasilkan kunci (subkey) yang berbeda sehingga memiliki tingkat keamanan yang baik.

b. Performance

   Kecepatan melakukan proses enkripsi dan dekripsi informasi (pesan)

c. Efficiency

   Penggunaan memori yang efisien

d. Implementability

   Algoritma AES dapat diimplementasikan dalam hardware dan software.

Disamping itu akan dikaji bahwa algoritma RSA akan menjamin keamanannya didasarkan pada kesulitan untuk memfaktorkan bilangan besar modulus n menjadi faktor-faktor primanya (Joye 1997, h.77; Robinson , 2003, h.3).