ABSTRAK

Pertukaran informasi merupakan kebutuhan yang sangat penting dalam kehidupan manusia sebagai makhluk sosial. Salah satu cara untuk melakukan pertukaran informasi yang paling popular sekarang ini adalah menggunakan e-mail atau *electronic mail.* E-mail menyediakan komunikasi dengan biaya murah, mudah dan dan cepat ke seluruh daerah di muka bumi. Tetapi E-mail yang dikirim melalui jaringan publik akan memiliki resiko ancaman keamanan yang besar seperti penyadapan, pengubahan pesan informasi, pemalsuan pesan, dan lain sebagainya oleh pihak yang tidak berwenang terhadap informasi tersebut. Oleh karena itu diperlukan pengamanan pada e-mail. Salah satu pengamanan pada e-mail yaitu dengan metode penyandian. Di dalam penelitian ini akan dibahas mengenai implementasi algoritma penyandian AES (*Advance Encryption Standard*) dan RSA (Rivest, Shamir, Adleman) pada aplikasi *end-to-end user* yang menggunakan e-mail yang sudah terdaftar pada Pop Mail Server yang menyediakan *free mail service.* Dalam implementasinya algoritma AES digunakan untuk menghasilkan rangkaian kunci dan menyandi pesan tertulis pada e-mail maupun *file attachment.* Sedangkan algoritma RSA digunakan untuk menghasilkan pasangan kunci publik dan privat dan menyandi rangkaian kunci yang dihasilkan oleh algoritma AES. Rangkaian kunci yang sudah disandi disimpan pada dongle, kemudian dongle ini akan didistibusikan ke setiap pengguna yang berhak. Penelitian ini bertujuan untuk menerapkan penyandian (enkripsi) e-mail untuk *end-to-end user* yang sudah terdaftar pada Pop Mail Server atau Imap Mail Server yang menyediakan *free mail service* dengan menggunakan algoritma enkripsi serta algoritma penghasil pasangan kunci publik dan privat. Hasil penelitian menunjukkan bahwa sistem pengamanan pada e-mail yang dibangun menggunakan pemrograman bahasa Java sudah memenuhi uji fungsionalitas, uji kemampuan sistem, uji kesesuaian sistem dengan tema, dan uji performance dengan tingkat keberhasilan 100 %.

Kata kunci : enkripsi e-mail, *dongle*, algoritma AES, algoritma RSA

ABSTRACT

Exchange of information is an important necessity in a human life as social beings. Currently, the most popular way to exchange information is utilizing e-mail or electronic mail. E-mail provides a low cost, easy and fast media for communication to any area on the earth. However, e-mail that is sent over a public network may have a big security risk such as eavesdropping, alteration of information messages, message forgery, and so forth. Therefore, the security of e-mail address is required, and one of them is e-mail security using encoding method.

This paper discusses the implementation of AES (Advance Encryption Standard) and RSA (Rivest, Shamir, Adleman) encryption algorithm on the application of end-to-end users who use e-mail that has been registered in the Pop Mail Server which provides a free mail service by using the encryption algorithm and the algorithm generating public and private key pair. In the implementation, AES algorithm is utilized to generate the key sequence and encodes a message written on the e-mail and file attachments. The RSA algorithm is utilized to generate pairs of public and private keys and encode the key sequence generated by the AES algorithm. The key sequence that has been encoded is stored in the dongle. This dongle will then be delivered to every user who has the authorization. Experimental testing results showed that the security system on the e-mail that was built using Java programming language already passed the functionality testing, system capabilities testing, system suitability testing under the theme, and performance testing with 100% success rate.

Keywords: e-mail encryption, dongle, AES algorithm, RSA algorithm