ABSTRACT

Data security is very important at this moment, because many hackers or spywares want to know the important information from a message which is usable for personal purpose. To send data on personal computer networking or telecommunication system, a software which can protect information on a message is needed.

Encryption and decryption using SEAL stream cipher is a software which is made to randomize a message and can transform random message into original message, with RSA algorithm for digital signature and CRC algorithm for checking the difference between the message with the original one.

A plaintext which is converted to ciphertext with SEAL encryption and ciphertext which is sent to other people. If one want to read the original message from ciphertext then SEAL decryption software is needed and must put the right password.

ABSTRAK

Keamanan data saat ini merupakan suatu hal yang sangat penting, karena banyaknya penyusup atau *spyware* yang menginginkan informasi dari suatu pesan yang dapat dimanfaatkan untuk kepentingan pribadi. Untuk mengirimkan suatu data pada jaringan komputer atau sistem telekomunikasi diperlukan program yang dapat melindungi isi dari pesan tersebut.

Enkripsi dan dekripsi *stream cipher* dengan metoda SEAL adalah software yang dirancang untuk mengacak isi dari suatu pesan dan mengubah pesan acak tersebut menjadi pesan asli, disertai dengan algoritma RSA sebagai digital signature dan algoritma CRC check untuk memeriksa perbedaan dari suatu pesan dengan pesan aslinya.

Suatu pesan plaintext diolah kedalam enkripsi SEAL kemudian didapatkan keluaran sebuah file ciphertext yang siap dikirimkan kepada orang lain. Jika ingin membaca pesan asli dari ciphertext maka diperlukan software dekripsi SEAL dan harus memasukkan password yang sesuai.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL