PENGGABUNGAN ALGORITMA DIFFIE-HELLMAN, RC4, DAN LSB UNTUK KEAMANAN PESAN

FATIMAH ZAHRA
(Pembimbing : Ricardus Anggi Pramunendar, MCS)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201207265@mhs.dinus.ac.id

ABSTRAK

Keamanan pesan sudah menjadi prioritas bagi setiap individu untuk mendapatkan suatu informasi. Bukan hanya pesan biasa, saat ini data perusahaan yang bersifat rahasia juga dikirimkan dalam bentuk digital maupun secara langsung melalui internet. Oleh sebab itu keamanan data rahasia sangat penting, pesan yang berupa data rahasia dapat dibajak oleh pihak yang tidak bertanggung jawab dan juga disalahgunakan fungsinya. Penggabungan algoritma dalam pengamanan pesan menjadi hal yang perlu dilakukan. Algoritma RC4 merupakan algoritma yang menggunakan kunci publik sebagai enkripsinya, maka diperlukan keamanan kunci dengan menggunakan algoritma pertukaran kunci Diffie-Hellman. Selain itu, penerapan penyisipan pesan kedalam gambar juga dilakukan dengan menggunakan metode LSB. Hasil dari penggabungan algoritma tersebut adalah sebuah citra yang telah disisipi pesan enkripsi dengan baik yang menghasilkan rata-rata nilai PSNR 70,1111 dB.

Kata Kunci : Penggabungan Algoritma, Pertukaran Kunci, Diffie-Hellman, RC4, LSB

INTEGRATION OF DIFFIE-HELLMAN ALGORITHM, RC4 AND LSB FOR MESSAGE SECURITY

FATIMAH ZAHRA
(Lecturer : Ricardus Anggi Pramunendar, MCS)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201207265@mhs.dinus.ac.id

ABSTRACT

Messaging security has become a priority for every individual to obtain information. Not just the usual message, this time confidential company data is also transmitted in digital form as well as directly through the internet. Therefore, the security of confidential data is very important, the message in the form of confidential data can be hijacked by parties who are not responsible and also abused its function. Merging algorithms in message security had to be done. The RC4 algorithm is an algorithm which uses a public key encryption, the necessary security key using the algorithm Diffie-Hellman key exchange. In addition, the implementation of inserting a message into images are also performed using the LSB. The result of the merger of the algorithm is an image that has been inserted properly encrypted messages that generate an average of 70.1111 dB PSNR.

Keyword : Integration of Algorithm, Key-Exchange, Diffie-Hellman, RC4, LSB