ABSTRAK

Keamanan informasi pada saat ini menjadi lebih mudah untuk disalahgunakan oleh pihak lain ketika informasi itu dikirim dan disimpan. Untuk menanggulangi masalah tersebut maka dilakukan penelitian yang menciptakan suatu aplikasi yang menggunakan metode hybrid cryptosystem dan digital signature. Metode hybrid cryptosystem dilakukan dengan menggabungkan algoritma RC4 dan RSA.Metode digital signature dilakukan dengan menggunakan fungsi hash SHA-512 dengan pendekatan algoritma RSA. Aplikasi yang dibangun dapat melakukan enkripsi dan dekripsi pada file serta meningkatkan keamanan dalam mengirim data dengan hybrid cryptosystem dan digital signature. Berdasarkan hasil penelitian maka semua tipe file yang diuji berhasil dienkripsi dan didekripsi.

Kata kunci : Hybrid Cryptosystem, RC4, RSA, SHA-512, Digital Signature.

ABSTRAK

Information security is currently easier to abuse by other parties when the information is sent and stored. To overcome this problem, research is conducted that creates an application that uses the hybrid cryptosystem and digital signature method. The hybrid cryptosystem method is carried out by combining the algorithm RC4 and RSA. The digital signature method is done by using the SHA-512 hash function with the RSA algorithm approach. Applications that are built can encrypt and decrypt files and increase security in sending data with hybrid cryptosystem and digital signatures. Based on the results of the study, all file types tested were encrypted and decrypted and the larger the file size, the longer the encryption and decryption process.

Keywords: Hybrid Cryptosystem, RC4, RSA, SHA-512, Digital Signature.

.