ABSTRAK

Tujuan dari Tugas Akhir ini adalah untuk membuat aplikasi dalam mengenkripsi dan mendekripsikan suatu data dalam entuk pesan atau gambar. Teknik-teknik yang digunakan adalah McEliece, Elgamal, dan Rabin. Aplikasi berjudul “John’s Encryption-Decryption”

Pengguna dapat menyandikan pesan maupun gambar dengan teknik – teknik kunci-publik tertentu, yakni : Elgamal, McEliece, dan Rabin. Setelah disandikan maka pengguna dapat menyimpan hasil kodenya tersebut di dalam bentuk *file*. Untuk mengembalikannya ke pesan asli, pengguna hanya cukup mengambil *file* yang sebelumnya pernah di simpan agar dapat melakukan dekripsi.

Pengguna dapat melihat hasil perbandingan dari tiap teknik. Efesiensi yang dimaksud terdiri dari waktu, ukuran file, dan banyaknya karakter di setiap file. Pengguna juga dapat melihat diagram batang dari perbandingan efesiensi setiap teknik.

kata kunci : McEliece, Elgamal, Rabin, Enkripsi, Dekripsi, Sandi, Kunci-Publik, Efesiensi

ABSTRACT

The aim of this last task is to be capable of making the application in encrypting and decrypting to encode data to form a message or picture, using McEliece's, ElGamal's, and Rabin's technique. The application is John's Encryption-Decryption.

Users are able to encode either message or picture using the certain public technique key which are ElGamal, McEliece and Rabin. After Encoding, the user are able to save the code in the file form. And turning back the original message is just to take the files which have been saved before to make decryption.

User can be able to know and see the result of comparison from every technique. With the efficiency of time, size of file and the character in every file. Either see the comparison efficiency from the rectangle diagram from every technique.

keyword : McEliece, Elgamal, Rabin, Encrypting, Decrypting, Encoding, Public-Key, Efficiency.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR CUPLIKAN KODE PROGRAM

DAFTAR LAMPIRAN