

ABSTRAK

Perkembangan teknologi membuat kemudahan dalam berkomunikasi. Kemudahan ini juga membuat mudahnya tersebar data-data privat seseorang. Untuk itu diperlukannya sebuah pengamanan data dalam sebuah jaringan komunikasi. Salah satu solusinya adalah kriptografi.

Kriptografi adalah sebuah ilmu yang mempelajari tentang menyembunyikan huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dimengerti atau dibaca. Untuk saat ini, Algoritma RSA merupakan algoritma kriptografi yang memiliki tingkat keamanan tinggi. Kunci RSA dengan panjang 1024 bit dapat memakan waktu ratusan tahun untuk dibobol jika menggunakan metode *brute force*.

Dalam tugas akhir ini, algoritma RSA akan diterapkan pada sebuah aplikasi FTP *client*. Aplikasi ini melakukan proses enkripsi pada saat proses *upload* sehingga *file* tidak bisa dibaca sembarang orang. Hanya yang memiliki kunci yang dapat membacanya. Dengan ini dihasilkan mekanisme berbagi *file* yang lebih aman walaupun menggunakan sebuah jaringan publik

Kata Kunci : Kriptografi, RSA, FTP

ABSTRACT

Developments in technology make it easy to communicate. This easiness also makes it easy to spread someone's private data. It required a data security in a communication network. One of the solution is cryptography.

Cryptography is a study of concealment of writings or letters so as to make the text cannot be understood or read. For now, The RSA algorithm is a cryptographic algorithm that has a high security level. RSA key with a length of 1024 bits can take hundreds of years to be cracked if using a brute force method.

In this final project, the RSA algorithm will be applied to an FTP client application. This application will perform the encryption process during the upload process so that the file cannot be read by anyone. Only those who have a key that can read them. With the implementation of this application resulted a secure file sharing mechanism despite using a public network.

Keywords: Cryptography, RSA, FTP