

ABSTRAK

Keamanan sebuah data dalam aplikasi sangatlah penting keberadaannya sehingga kita harus memberikan prioritas. Karena pada akhir jaman ini pencurian informasi atau pun data sudah banyak dilakukan, oleh karena itu berbagai cara dilakukan untuk memberikan keamanan. Salah satu cara yang dapat dilakukan untuk keamanan suatu data adalah melakukan enkripsi, baik dilakukan enkripsi untuk transfer data atau hanya untuk enkripsi data ketika dilakukan penyimpanan karena dengan melakukan enkripsi berarti mengubah suatu *plaintext* menjadi *chipertext*.

Dengan adanya enkripsi ketika melakukan pengiriman file ke tujuan, tidak setiap orang akan dapat membacanya dengan mudah karena untuk dapat membaca data yang lewat yang sudah terenkripsi, harus mengetahui *key* yang digunakan, setelah itu harus mengetahui algoritma seperti apa yang digunakan karena secara logika untuk mendekripsi data yang terenkripsi, berarti harus membalik algoritma enkripsi. Untuk melakukan hal ini dibutuhkan waktu yang lama, inilah yang membuat data yang terenkripsi sudah dikatakan aman. Enkripsi yang digunakan adalah menggunakan RSA (*Rivest-Shamir-Adleman*) dengan merandom dua bilangan prima secara acak untuk membangkitkan *key*, lalu mengenkrip *plaintext*, dengan tujuan mengamankan suatu *file*.

Kata kunci: enkripsi, *chipertext*, *plaintext*

ABSTRACT

Security data in an application is very important given that we must give priority. Because at the end of this era of information theft or data has been done, therefore, various methods are used to provide security. One way that can be done to the security of an encryption of data is done, well done encryption for data transfer or only for the storage of data encryption when done by performing the encryption means for converting plaintext to ciphertext.

With the encryption when sending files to the destination, not everyone will be able to read easily as to be able to read data through the already encrypted, we must know the key to be used, after which it must know what algorithm is used because it is logic to decrypt data is encrypted, we reverse the encryption algorithm. To do this it takes a long time, this is what makes the data terenkripsi been considered safe. Encryption used is using RSA (Rivest-Shamir-Adleman) with merandom two primes at random to generate the key, then encrypt the plaintext, with aim of securung the fi le.

Keyword: encryption, chipertext, plaintext