ABSTRAKSI

Kemajuan bidang jaringan komputer dengan konsep open system membuat pengguna lebih mudah dalam menyimpan dan saling bertukar data karena dapat dilakukan dimanapun dan kapanpun. Konsep open system ini juga memiliki kelemahan karena dimanfaatkan oleh para hacker untuk mencoba mengambil dan membuka data tersebut. Hal ini dikarenakan kurangnya keananan pada data sehingga mudah diakses oleh orang lain. Untuk mengatasi masalah tersebut salah satunya adalah dengan teknik penyandian data yang dikenal dengan teknik kriptografi. Ada banyak teknik kriptografi yang dapat digunakan dengan kelebihan dan kekurangannya masing-masing. Semakin banyak teknik yang digunakan dalam satu data maka semakin sulit data tersebut diakses oleh orang lain. Pada penelitian ini dibahas mengenai pengembangan salah satu algoritma pada kriptografi yaitu Caesar Cipher. Algoritma ini dikembangkan sehingga dapat digabungkan dengan Algoritma lain yaitu Affine Cipher. Proses enkripsi dan dekripsi pada Caesar Cipher dilakukan dengan melakukan pergeseran tiap huruf pada pesan asli sebanyak kunci yang ditentukan, sedangkan proses enkripsi dan dekripsi pada Affine Cipher membutuhkan dua buah kunci. Pesan asli akan di enkripsi dengan metode Caesar Cipher, kemudian hasilnya akan dienkripsi lagi dengan metode Affine Cipher. Dengan menggabungkan dua metode tersebut maka akan menambah tingkat keamanan data karena memerlukan dua tahap untuk melakukan enkripsi dan dekripsi.

Kata Kunci: Kriptografi, Enkripsi, Caesar Cipher, Affine Cipher

ABSTRACT

The development of computer networks with the concept of open system makes it easier for user to store data because it can be done anywhere and anytime. The concept of open system also has the disadvantage exploited by hackers to attempt to retrieve and open data. This is because the lack of security on the data so it is easily accessible by others. One solution for this problem is to provide password to that data. Techniques to provide passwords is called cryptography. There are many cryptographic techniques that can be used with the advantages and disadvantages of each. The more techniques used in the data, the more difficult the data accessed by others. In this study, discussed the development of one of the cryptographic algorithm that Caesar Cipher. This algorithm was developed so that it can be combined with other algorithms that Affine Cipher. Encryption and decryption process at the Caesar Cipher is done by shifting each letter in the original message as specified key, while the encryption and decryption process on Affine Cipher requires two keys. The original message will be encrypted with the Caesar Cipher, then the result will be encrypted again with Affine Cipher. By combining the two methods, it will increase the level of data security because it requires two stages to perform encryption and decryption.

Keywords : Cryptographic, Encryption, Caesar Cipher, Affine cipher