

ABSTRAK

Sejak lama penyandian pesan dilakukan dengan metode kriptografi. Jaman Romawi penyandian pesan telah dilakukan. Penyandian dengan metode kriptografi ini dikenal dengan nama *caesar cipher* yang merupakan algoritma kriptografi cipher substitusi. Adapun pengembangan dari caesar cipher adalah algoritma cipher substitusi homofonik dan poligram. Proses penyandian ini disebut enkripsi dan untuk membuka penyandiannya disebut dekripsi. Proses enkripsi merupakan proses perubah data asli (*plaintext*) menjadi data rahasia (*ciphertext*). Sehingga kerahasiaan data ketika dikirim diharapkan terjaga. Proses dekripsi adalah proses merubah data tersandian (*ciphertext*) menjadi data asli (*plaintext*) ketika data diterima oleh yang berhak.

Kata Kunci : Kriptografi, Caesar cipher, Cipher substitusi, Homofonik, Poligram.



ABSTRACT

Since long encoding messages by cryptographic methods. Roman era encoding the message has been conducted, the encoding method is known as cryptography caesar cipher which is a substitution cipher cryptographic algorithm. The development of caesar cipher is a homofonik substitution cipher algorithm and poligram. Encoding process is called encryption and to open the encryption is called decryption. The process of encryption is the process of changing the original data (plaintext) into secret data (ciphertext), so that the confidentiality of data while being shipped is expected to awake. Decryption process is the process of the change secret data (ciphertext) into original data (plaintext) when data is received by the authorized.

Keywords : Cryptography, Caesar cipher, Cipher Substitution, Homofonik, Polygram.

