

BAB II

LANDASAN TEORITIS

2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu “*cryptos*” artinya “*secret*” (rahasia), sedangkan “*graphein*” artinya “*writing*” (tulisan). Jadi, kriptografi berarti “*secret writing*” (tulisan rahasia). Ada beberapa defenisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Defenisi yang dipakai di dalam buku-buku yang menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan atau informasi dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Defenisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi dikalangan militer, diplomat, dan mata-mata[3].

Dalam kriptografi sering menemukan berbagai istilah atau terminology. Beberapa istilah kriptografi yaitu[3] :

1. *Plaintext, chipertext, key, algoritma*

Plaintext adalah pesan yang dapat dibaca. *Ciphertext* adalah pesan sandi atau pesan acak yang tidak dapat dibaca. *Key* yaitu untuk melakukan teknik kriptografi. *Algoritma* adalah metode untuk melakukan enkripsi dan deskripsi[2].