BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Berkat perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran informasi. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan informasi atau dikenal dengan istilah Kriptografi.

Kriptografi merupakan salah satu cara untuk mengamankan informasi, yaitu dengan menyandikan pesan asli (*plaintext*) ke dalam bentuk pesan rahasia (*ciphertext*). Proses pengamanan ini melibatkan algoritma dan kunci. Kunci enkripsi dapat dengan mudah mengembalikan *plaintext* dari *ciphertext* [1].

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkiripsi adalah proses mengubah pesan asli (*plaintext*) menjadi pesan yang disandikan (*ciphertext*) berdasarkan metode yang telah ditentukan yang mana