BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan dan privasi sangat dibutuhkan saat melakukan pertukaran informasi penting pada era teknologi informasi dan komunikasi saat ini.Pada seiring perkembangan teknologi yang semakin pesat maka semakin besar pula penyadapan informasi penting yang bersifat privasi dengan melalui berbagai macam perantara media sosial.Tingkat keamanan dan privasi juga semakin diperlukan untuk menghindari penyadapan informasi yang mungkin bisa kapan pun terjadi, terutama pada era sekarang. Salah satu cara yang bisa digunakan untuk menjadikan suatu informasi yang bersifat privasi dapat tidak diketahui oleh orang yang tidak berhak adalah menyandikan (mengenkripsikan) informasi tersebut sehingga informasi sulit dan bahkan tidak dapat dipahami oleh orang lain.

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan[1]. Kriptografi dapat menyandikan (mengenkripsikan) informasi yang bersifat privasi menjadi informasi yang tidak dapat dipahami oleh orang yang tidak berhak.Enkripsi pada kriptografi digunakan untuk merubah informasi menjadi sandi-sandi dengan menggunakan kunci (*key).*Dekripsi pada kriptografi digunakan untuk membuka sandi-sandi yang telah di enkripsikan sebelumnya dengan menggunakan kunci (*key)* yang sama[2]. Salah satu cara untuk