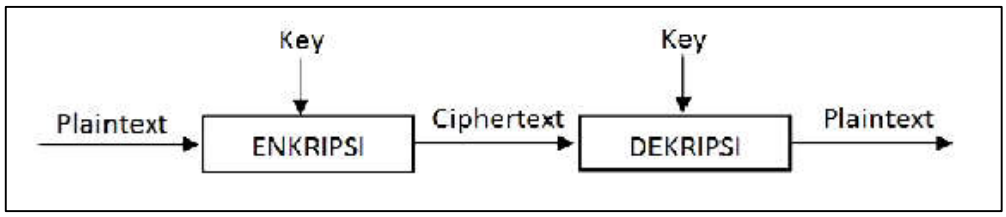
BAB II

LANDASAN TEORI

2.1 Kriptografi

Secara etimologis, kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphy*. *Crypto* artinya *secret* dan *graphy* artinya menulis. Maka, kriptografi berdasarkan dari bahasanya didefinisikan sebagai menulis secara rahasia. Kriptografi adalah sutau ilmu dan seni untuk mengamankan informasi yang berupa pesan yang terbaca (*plaintext*) menjadi pesan yang tidak bisa dibaca (*ciphertext*), sehingga hanya pengirim pesan dan penerima pesan yang dapat mengganti, menghapus dan membaca pesan tersebut. Ada dua proses pembentukkan kunci pada kriptografi, yaitu kunci simetris dan asimetris. Di mana kunci simetris memiliki kunci yang sama pada saat proses enkripsi dan dekripsi. Sedangkan, kunci asimetris memiliki kunci yang berbeda pada saat proses enkripsi dan dekripsi [1].



Gambar 2.1 Skema enkripsi dan deskripsi

Bentuk awal dari penulisan rahasia membutuhkan lebih sedikit dari implementasi penulisan sejak banyak orang tidak dapat membaca. lawan yang lebih terpelajar, membutuhkan kriptografi yang nyata. Tipe sandi klasik utama ialah *sandi transposisi*, di mana mengatur aturan huruf pada pesan (contoh 'hello