12 ELGAMAL CRYPTOSYSTEM

The structure of the ElGamal cryptosystem is shown in Figure.

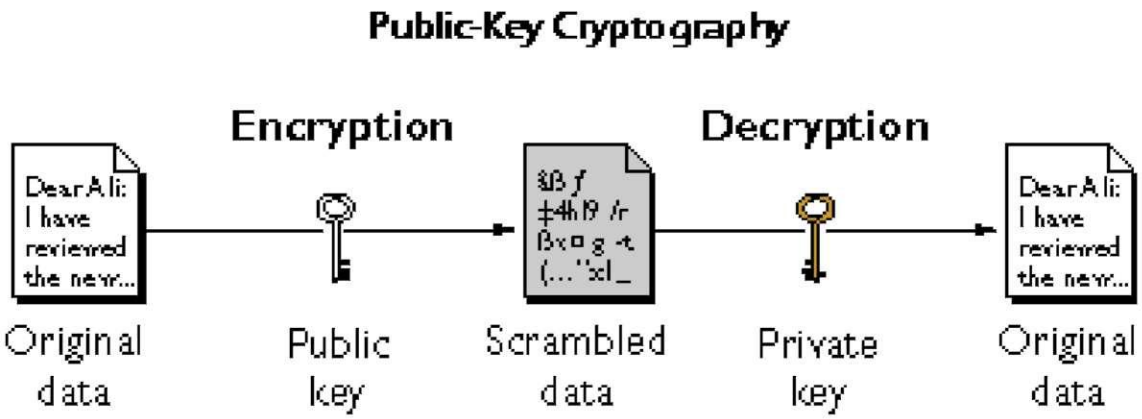

Figure Block diagram of the ElGamal cryptosystem

Encryption can be expressed by the equations:

$$\begin{aligned} a &= G^K \bmod P, \\ b &= Y^K M \bmod P. \end{aligned} \tag{1}$$

Decryption can be expressed by the equations:

$$M = b\left(a^X\right)^{-1} \bmod P. \tag{2}$$