ElGamal Cryptosystem :-

To send a message P to the user A, we choose an integer k at random and then send P to A in the following pair (g^k, Pg^{ak}) modulo p.

Here g is a generator mod p.
And a is the randomly chosen integer in the range $0 < a < p-1$.

"a" → selected by the user A and kept secret. (Secret key of A).

g^a → public key.
(Made public by A, computing g^a)

Encryption :- The message P is multiplied with $(g^a)^k$ to get Pg^{ak}.

Cipher text : (g^k, Pg^{ak}).

(i.e., message P is wearing mask g^{ak} and a remover g^k)

Decryption:- 'a' is kept secret by A.

A computes $(g^k)^a = g^{ak} \cdot \text{mod } p$.

Thus $(Pg^{ak}) \cdot g^{-ak} \equiv P \pmod p$.

Equivalently, $(g^k)^{p-1-a} \cdot (Pg^{ak})$

$\equiv (g^{-ak})(Pg^{ak})$.

$\equiv P \pmod p$

Ex:- User selects secret key $a = 15$, $g = 3$ and $p = 43$.

$g^a = 3^{15} \equiv 22 \pmod{43}$.

Public key $\equiv (p, g, g^a) = (43, 3, 22)$.

To send message "SELL" to the person with public key $K_E = (43, 3, 22)$, we have to select integer 'k' and compute g^k and Pg^{ak} and send it the user.

Let $k = 23 \Rightarrow g^k = 3^{23} \equiv 34 \pmod{43}$

Now: $\left.\begin{matrix} S: 18 \\ E: 4 \\ L: 11 \\ L: 11 \end{matrix}\right\} \Rightarrow Pg^{ak} \pmod p \Rightarrow \left\{\begin{matrix} 17 \\ 42 \\ 8 \\ 8 \end{matrix}\right.$

We have to send (g^k, Pg^{ak}) to the user as pairs:

$(34,17), (34,42), (34,8), (34,8)$.

Decryption:- $(g^k)^{p-1-a} (Pg^{ak})$

$= (34)^{43-1-15} (Pg^{ak})$

$= (34)^{27} (Pg^{ak})$

$\equiv 39 (Pg^{ak}) \pmod{43}$

$\Rightarrow 39 \times 17 \equiv 18 \pmod{43} \Rightarrow S$

$39 \times 42 \equiv 4 \pmod{43} \Rightarrow E$

$39 \times 8 \equiv 11 \pmod{43} \Rightarrow L$

$39 \times 8 \equiv 11 \pmod{43} \Rightarrow L.$

Ex:- The message "REPLY TODAY" must encrypted in the ElGamal Crypto-

system and forwarded to the user with public key $K_E = (p, q, g^a) = (47, 5, 10)$.

Select a random number $k = 13$ and Encrypt the message. Also decipher the message to verify, if the secret key of the user is $a = 19$.