Elgamal Cryptosystem

The Elgamal Public Key Encryption Algorithm

Elgamal Cryptosystem

- The *ElGamal encryption system* is a public key encryption algorithm proposed by Taher Elgamal in 1985 that is based on the Diffie-Hellman key exchange

Elgamal Cryptosystem Steps

- Generate Keys
- Encryption
- Decryption

Generate Keys

Agent X chooses

I. A large prime p
II. A primitive element g modulo p
III. A (possibly random) integer d with $2 \leq d \leq p-2$.
IV. Computes $e = g^d \bmod p$
V. Posts public key (p, g, e).
VI. Private key is d.

Encryption

1. Agent Y encrypts a short message M (M < p) and sends it to Agent X like this:
2. Agent Y chooses a random integer k (which he keeps secret).
3. Agent Y computes **$Y1 = g^k \bmod p$** and **$Y2 = M * e^k \bmod p$**
4. Agent Y sends his encrypted message (Y1, Y2) to Agent X

Decryption

When Agent X receives the encrypted message (Y1, Y2), he decrypts (using the private key d) by computing

- **Plain text = $Y2 * (Y1^{d})^{-1} \bmod p$**

Example:

- Agent X chooses prime number p = 13,
- Generator g = 2, g is a primitive root of p, GCD(g,p)=1.
- Select d = 3, 2<=d<=p-2
- and then he computes e = g^d mod p.
  - e= 2^3 mod 13
  - e= 8 mod 13
  - e= 8
- His public key is (p, g, e) = (13,2,8), and his private key is d = 3.

Example:

- Agent Y wants to send the message “M=4" to Agent X. M should be less than p.
- He chooses a random integer k = 7.
- Now, he calculate, $Y1= g^k \bmod p$
  - $Y1= 2^7 \bmod 13$
  - $Y1= 11$
- And $Y2= M * e^k \bmod p$
  - $Y2= 4 * 8^7 \bmod 13$
  - $Y2=7$
- He sends the encrypted message (11, 7) to Agent X.

Example:

- Agent X receives the message (Y1, Y2) = (11, 7), and using his private key d = 3 he decrypts the plain text,
- PT= $Y2 * (Y1^{d})^{-1} \bmod p$
- PT= $7 * (11^{3})^{-1} \bmod 13$
- PT= $7 * 8 \bmod 13$
- PT= $56 \bmod 13$
- PT= 4