# Elgamal Cryptography

→ Asymmetric Key Cryptography

Steps

→ Key Generation

→ Encryption

→ Decryption

## Key Generation

1. Select large Prime number (P)
2. Select a decryption key also called Private key (d)
3. Select Second Part of encryption key ($e_1$)
4. Calculate ~~Select~~ third Part of encryption key ($e_2$)

$$e_2 = e_1^d \bmod P$$

5. Public Key = $(e_1, e_2, P)$ and Private Key = d.

## Encryption

1. Select Random Integer (R)
2. Calculate $C_1 = e^r \bmod P$
3. Calculate $C_2 = (PT \times e_2^R) \bmod P$

Assume PT

4. Cipher Text = $(C_1, C_2)$

## Decryption

$$PT = \left[ C_2 \times \left( (C_1)^d \right)^{-1} \right] \bmod P.$$

## Example

Select $P = 11$

Select $d = 3$

select $e_1 = 2$

Calculate $e_2 = e_1^d \bmod P$

$= 2^3 \bmod 11$

$= 8 \bmod 11$

$e_2 = 8$

Public key = $(e_1, e_2, p)$

Public key = (2, 8, 11)

Private key = d = 3

## Encryption

1. Select $r = 4$

2. Calculate $C_1 = e_1^r \bmod p$

$= 2^4 \bmod 11$

$= 16 \bmod 11$

$C_1 = 5$

3. Calculate $C_2 = (PT \times e_2^r) \bmod p$

Assume $PT = 7$

$= (7 \times 8^4) \bmod 11$

$= 28672 \bmod 11 = 6$

$C_2 = 6$

Cipher Text $C_1, C_2 = 5, 6$

## Decryption

$PT = [C_2 \times ((C_1)^d)^{-1}] \bmod p$

$= [6 \times ((5)^3)^{-1}] \bmod 11$

$= [6 \times (125)^{-1}] \bmod 11$

$ab \bmod n = (a \bmod n)(b \bmod n)$

$125x \bmod 11 = 1$ $\quad x = 1, 2, 3 \ldots$

$x = 1$

$125 \bmod 11 \neq 4$

$x = 2$

$250 \bmod 11 \neq 8$

$x = 3$

$375 \bmod 11 = 1$ ✓

$= (6 \bmod 11)(3 \bmod 11)$

$PT = (6 \times 3) \bmod 11$

$= 18 \bmod 11$

$PT = 7$