ElGamal Public-Key Encryption and Decryption

ElGamal Cryptosystem

- Taher ElGamal, originally from Egypt, was a graduate student at Stanford University, and earned a PhD degree in 1984, Martin Hellman as his dissertation advisor
- He published a paper in 1985 titled "A public key cryptosystem and a signature scheme based on discrete logarithms" in which he proposed the ElGamal discrete log cryptosystem and the signature scheme
- The ElGamal cryptosystem essentially turns the Diffie-Hellman key exchange method into an encryption algorithm

ElGamal Key Setup

- **Domain Parameters:** The prime p and the generator g of $\mathcal{Z}_p^*$
- **Keys:** The private key is the integer $x \in \mathcal{Z}_p^*$ and the public key y is computed as $y = g^x \pmod{p}$
- Example: Given the prime $p = 2579$ and the generator $g = 2$, we select the private key $x = 765$, and compute the public key y as

$$\begin{aligned} y &= g^x \pmod{p} \\ &= 2^{765} \pmod{2579} \\ &= 949 \pmod{2579} \end{aligned}$$

Therefore, the private key $x = 765$ and the public key $y = 949$

ElGamal Public-Key Encryption

- **Encryption:** The User B forms a message $m \in \mathcal{Z}_p^*$, generates a random number r and computes the ciphertext pair (c_1, c_2)

$$\begin{aligned} c_1 &= g^r \pmod{p} \\ c_2 &= m \cdot y^r \pmod{p} \end{aligned}$$

- Example: Assume $m = 1299$, compute $E(m) = (c_1, c_2)$ using the public key $y = 949$ and the random number $r = 853$

$$\begin{aligned} c_1 &= g^r \pmod{p} \\ &= 2^{853} = 435 \pmod{2579} \\ c_2 &= m \cdot y^r \pmod{p} \\ &= 1299 \cdot 949^{853} = 2396 \pmod{2579} \end{aligned}$$

Therefore, $E(1299) = (c_1, c_2) = (435, 2396)$

ElGamal Public-Key Decryption

- **Decryption:** The User A decrypts the ciphertext pair (c_1, c_2) to obtain the message m by computing

$$\begin{aligned} u_1 &= c_1^x = (g^r)^x = (g^x)^r = y^r \pmod p \\ u_2 &= c_2 \cdot u_1^{-1} = y^r \cdot m \cdot y^{-r} = m \pmod p \end{aligned}$$

- Given $E(m) = (c_1, c_2) = (435, 2396)$, the User A finds the plaintext:

$$\begin{aligned} u_1 &= c_1^x \pmod p \\ &= 435^{765} = 2424 \pmod{2579} \\ u_2 &= c_2 \cdot u_1^{-1} \pmod p \\ &= 2396 \cdot 2424^{-1} = 1299 \pmod{2579} \end{aligned}$$

Therefore, $D(c_1, c_2) = D(435, 2396) = 1299$

ElGamal Cryptosystem Properties

- The ElGamal cryptosystem is a randomized algorithm: Every encryption requires the generation and use of a random number r
- The random number r should not be guessable
- The same random number r should not be used for another encryption, otherwise, the knowledge of one message allows the adversary to compute the other message
- The random number r is not needed for decryption
- The ElGamal cryptosystem produces a ciphertext pair, which is of twice length as the message
- Its security depends on the difficulty of the DLP in $\mathcal{Z}_p^*$
- Breaking Diffie-Hellman also implies breaking ElGamal