ElGamal Cryptosystem and Signature Algorithm

ElGamal Signature Scheme

- 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
- The ElGamal signature scheme is the basis for Digital Signature Algorithm (DSA) adopted by the NIST

ElGamal Signature Scheme

- **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 $y = g^x \pmod{p}$
- **Signing:** The User A forms a message $m \in \mathcal{Z}_p^*$, generates a random number r and computes the signature pair (s_1, s_2)

$$\begin{aligned} s_1 &= g^r \pmod{p} \\ s_2 &= (m - x \cdot s_1) \cdot r^{-1} \pmod{p-1} \end{aligned}$$

- The message and signature consists of $[m, s_1, s_2]$
- Similar to the encryption case, the size of the signature is twice the size of the message

ElGamal Cryptosystem Signature Scheme

- **Verifying:** The verifier receives the triple $[m, s_1, s_2]$ and also has access to the public key y, and computes u_1 and u_2 as

$$\begin{aligned} u_1 &= g^m \pmod{p} \\ u_2 &= y^{s_1} \cdot s_1^{s_2} \pmod{p} \end{aligned}$$

If $u_1 = u_2$, then, the signature is valid

Proof.

The equality $u_1 = u_2$

$$g^m = y^{s_1} \cdot s_1^{s_2} = (g^x)^{s_1} \cdot (g^r)^{s_2} \pmod{p}$$

implies

$$m = x \cdot s_1 + r \cdot s_2 \pmod{p-1}$$

according to the Fermat's theorem □

ElGamal Cryptosystem Signature Example

- The parameters: the prime $p = 2579$ and the generator $g = 2$, the private key $x = 765$, and the public key $y = 949$
- We compute the signature pair on the message $m = 2013$ using the random number $r = 999$ as

$$
\begin{aligned}
s_1 &= g^r \pmod{p} \\
&= 2^{999} = 1833 \pmod{2579} \\
s_2 &= (m - x \cdot s_1) \cdot r^{-1} \pmod{p-1} \\
&= (2013 - 765 \cdot 1833) \cdot 999^{-1} \pmod{2578} \\
&= 2200 \cdot 1329 = 348 \pmod{2578}
\end{aligned}
$$

The message and signature triple is $[m, s_1, s_2] = [2013, 1833, 348]$

ElGamal Cryptosystem Signature Example

- The verifier has access to $(p, g, y) = (2579, 2, 949)$
- The verifier receives $[m, s_1, s_2] = [2013, 1833, 348]$ and computes

$$\begin{aligned}
u_1 &= g^m \pmod{p} \\
&= 2^{2013} \pmod{2579} \\
&= 713 \\
u_2 &= y^{s_1} \cdot s_1^{s_2} \pmod{p} \\
&= 949^{1833} \cdot 1833^{348} \pmod{2579} \\
&= 385 \cdot 2333 \pmod{2579} \\
&= 713
\end{aligned}$$

Since $u_1 = u_2$, the signature is valid