ElGamal Public-Key Cryptosystem

1 The Order of an Element. Primitive Roots

$\mathbf{Z}_m$ denotes the set $\{0, 1, \ldots, m-1\}$, $\mathbf{Z}_m^*$ stands for the set $\{a \in \mathbf{Z}_m | (a, m) = 1\}$. In case that $a \in \mathbf{Z}_m^*$, for some $m \geq 2$, there is an unique element $b \in \mathbf{Z}_m^*$ such that $a \cdot b \equiv 1 \ mod \ m$. The element b is denoted by $a^{-1} \ (mod \ m)$ and is referred to as the *multiplicative inverse* of a *modulo* m.

Euler's totient function is given by $\phi(m) = |\mathbf{Z}_m^*|$, for all $m \geq 1$, and $\phi(0) = 0$. In case that m and m' are coprime then $\phi(m \cdot m') = \phi(m) \cdot \phi(m')$. Moreover, if q is a *prime power*, i.e., there is a prime p and a positive integer l such that $q = p^l$, then $\phi(q) = \phi(p^l) = p^l - p^{l-1}$. As a particular case, if p is prime then $\phi(p) = p - 1$.

An important result is Euler's theorem, presented next.

Theorem 1 *(Euler's theorem)*
Let $m \geq 2$ *and* $a \in \mathbf{Z}_m^*$. *Then*

$$a^{\phi(m)} \equiv 1 \ mod \ m.$$

Definition 1 Let $m \geq 2$ and $a \in \mathbf{Z}_m^*$. The *order* of a modulo m, denoted by $ord_m(a)$ is defined as

$$ord_m(a) = min(\{l \in \mathbf{N}^* | a^l \ \equiv \ 1 \ mod \ m\})$$

The most important properties of the order of an element are summarized in Proposition 1.

Proposition 1 Let $m \geq 2$, $a \in \mathbf{Z}_m^*$, and k, l some positive integers.

1. If $a^k \equiv 1 \ mod \ m$ then $ord_m(a) | k$. As a particular case we obtain $ord_m(a) | \phi(m)$;
2. The relation $a^k \equiv a^l \ mod \ m$ is equivalent with $k \equiv l \ mod \ ord_m(a)$;
3. The elements $a^1 \ mod \ m$, $a^2 \ mod \ m$,$\ldots$,$a^{ord_m(a)} \ mod \ m$ are pairwise distinct;
4. The next relation holds true

$$ord_m(a^k \ mod \ m) = \frac{ord_m(a)}{(ord_m(a), k)}.$$

Definition 2 Let $m \geq 2$ and $\alpha \in \mathbf{Z}_m^*$. The element a is called *primitive root modulo* m if $ord_m(\alpha) = \phi(m)$.

Remark 1 In case that α is a primitive root modulo m, every element β from the set $\mathbf{Z}_m^*$ can be uniquely expressed as $\beta = \alpha^i \ mod \ m$ for $i \in \mathbf{Z}_{\phi(m)}$. The value i will be referred to as the *discrete logarithm (modulo m) to the base* α *of* β and we will write $i = log_\alpha \beta$. While an expression of form $\beta = \alpha^i \ mod \ m$ can be efficiently computed given α, i, m, the problem of finding the discrete logarithm modulo m to the base α of β, given α, β, m is intractable.

The most important properties of the primitive roots are summarized in Proposition 2.

Proposition 2 Let $m \geq 2$, $\alpha \in \mathbf{Z}_m^*$.

1. $\mathbf{Z}_m^*$ has primitive roots if and only if $m \in \{2, 4, p^k, 2p^k\}$, where p is an odd prime and $k \geq 1$ (Gauss' Theorem);

2. If $\mathbf{Z}_m^*$ has primitive roots, there are exactly $\phi(\phi(m))$ primitives roots modulo m;

3. If $\mathbf{Z}_m^*$ has primitive roots, α is a primitive root modulo m if and only if the next relation holds:

$$\alpha^{\frac{\phi(m)}{r}} \not\equiv 1 \ mod \ m,$$

for any prime divisor r of $\phi(m)$.

Proposition 2(3) does not always allow to efficiently generate primitive roots because computing $\phi(m)$ and factoring $\phi(m)$ are intractable for large integers m. In practice, m is chosen such that computing $\phi(m)$ and factoring $\phi(m)$ are easy. For example, m be chosen as a safe prime, i.e., m of form $m = 2q + 1$, where q is also a prime number. In this case α is a primitive root modulo m if and only if $\alpha^2 \not\equiv 1 \ mod \ m$ and $\alpha^q \not\equiv 1 \ mod \ m$.

Elements of order q may be generated via primitive roots. More exactly, if p and q are odd primes such that $q|(p-1)$, α is a primitive root modulo p, and $\beta = \alpha^{\frac{p-1}{q}} \ \texttt{mod} \ p$, then $ord_p(\beta) = q$. Indeed, by the Proposition 1(4), $ord_p(\alpha^{\frac{p-1}{q}} \ \texttt{mod} \ p) = \frac{ord_p(\alpha)}{(ord_p(\alpha), \frac{p-1}{q})} = \frac{p-1}{(p-1, \frac{p-1}{q})} = q$.

2 ElGamal Public-Key Cryptosystem

- `private key`: $a \in \mathbf{Z}_q^*$;
- `public key`: (p, q, α, β) where p is a large prime, such that $p-1$ has a large prime divisor q, α is an element of order q, and $\beta = \alpha^a \ \texttt{mod} \ p$;

- `encryption`: a plaintext $x \in \mathbf{Z}_p$ is encrypted as a pair (γ, δ) where
  - $\gamma = \alpha^r \bmod p$
  - $\delta = x \cdot \beta^r \bmod p$

  where $r \in \mathbf{Z}_q^*$ is a parameter chosen by the sender;
- `decryption`: the cryptotext $(\gamma, \delta) \in \mathbf{Z}_p \times \mathbf{Z}_p$ is decrypted as

$$(\gamma^a)^{-1} \cdot \delta \bmod p.$$

The correctness of the cryptosystem can be easily justified as follows:

$$\gamma^{-a} \cdot \delta \bmod p = \alpha^{-ar} \cdot (x \cdot (\alpha^a)^r) \bmod p = x.$$

The security of the ElGamal cryptosystem relies on the intractability of computing discrete logarithms.

2.1 Homomorphic Properties of the ElGamal Encryption

ElGamal encryption method, $e_r(x) = (\gamma, \delta)$ where $\gamma = \alpha^r \bmod p$ and $\delta = x \cdot \beta^r \bmod p$, for some $r \in \mathbf{Z}_q^*$, has homomorphic properties:

- $e_{r_1}(x_1) \cdot e_{r_2}(x_2) = e_{r_1+r_2}(x_1 \cdot x_2)$;
- $e_{r_1}(\overline{\alpha}^{v_1} \bmod p) \cdot e_{r_2}(\overline{\alpha}^{v_2} \bmod p) = e_{r_1+r_2}(\overline{\alpha}^{v_1+v_2 \bmod q} \bmod p)$.

2.2 Do Not Use the Same r!

It is very important that different random numbers r be used to encrypt different plaintexts. If two plaintexts x_1 and x_2 are encrypted using the same r, the knowledge of the corresponding cryptotexts (γ_1, δ_1), (γ_2, δ_2) and of the first plaintext leads to the second one. Indeed, because $\delta_1^{-1} = x_1^{-1} \cdot \beta^{-r} \bmod p$ and $\delta_2 = x_2 \cdot \beta^r \bmod p$, we obtain that $\delta_1^{-1}\delta_2 = x_1^{-1}x_2 \bmod p$, and, thus,

$$x_2 = x_1\delta_1^{-1}\delta_2 \bmod p.$$