Abstract. In this lecture we continue our analysis of RSA and introduce the Elgamal public key cryptosystem. Readings from Chapter 5 and 6 of D. Stinson.

1 ElGamal Public Key Cryptosystem

1.1 Basic Idea of ElGamal Scheme

Encryption of a message is done by taking the message $m$ and multiplying with a random number $R$ to get $mR$. To then do decryption, if Bob has a way to remove the effect of $R$, then $m$ can be obtained.

1.2 Discrete Logarithm Problem

Definition 1. Define the order of an element $g \in G$ of a finite multiplicative group $G$ to be the smallest positive number such that $g^m = 1$.

Theorem 1. Lagrange theorem: Suppose $G$ is a multiplicative group of order $n$ (the order of a group refers to its cardinality). The order of any element $g \in G$ divides $n$.

If $p$ is a prime number, then the multiplicative group $\mathbb{Z}_p^*$ is a group of order $(p-1)$, and any element in $\mathbb{Z}_p^*$ has an order that divides $(p-1)$. In fact for $p$ prime, every element in $\mathbb{Z}_p^*$ is a cyclic group.

Definition 2. A multiplicative group $G$ is called cyclic if there exists an element $g \in G$ such as the order of $g$ is equal to the order of $G$.

An element $g$ of order $(p-1)$ modulo $p$ is called a primitive element modulo $p$. An element $g$ is a primitive element modulo $p$ if and only if:

$$\{g^i : 0 \leq i \leq p-2\} = \mathbb{Z}_p^*$$

(1)

Assume that $a$ is a primitive element modulo $p$, then any element of $b \in \mathbb{Z}_p^*$ can be written in the form $b = a^i$ with $0 \leq i \leq p-2$. It can be proven that the order of $b$ is

$$ord(b) = \frac{p-1}{gcd(p-1, i)}.$$  

(2)

The element $b$ is itself primitive if $gcd(p-1, i) = 1$. Hence, the number of primitive elements modulo $p$ are $\phi(p-1)$.

Example Consider $p = 13$. First verify that 2 is a primitive element modulo 13. Then compute the $gcd(i, p-1)$ to find the rest of the primitive elements.
Back to the discrete logarithm problem

Let \((G, \cdot)\) denote a finite multiplicative group. For an element of \(a \in G\) of order \(n\) we define

\[
<a> = \{a^i : 0 \leq i \leq (n - 1)\}.
\]

The group \(<a>\) is cyclic with order \(n\). We can easily construct such group from \(\mathbb{Z}_p^*\). The Discrete logarithm problem is defined as follows.

**Definition 3. Discrete Logarithm Problem:** Consider a multiplicative group \((G, \cdot)\), an element \(a \in G\) having an order \(n\) and an element \(b \in <a>\). Find the unique integer \(i, 0 \leq i \leq n - 1\) such that \(a^i = b\). We denote the integer \(i\) by \(\log_a b\) and it is called the discrete logarithm of \(b\).

The discrete logarithm problem is believed to be difficult in an appropriate group \(G\).

1.3 ElGamal Algorithm

1. Choose a large prime \(p\), and a number \(\alpha \in \mathbb{Z}_p^*\) to be a primitive element.
2. Choose a secret \(i, 1 \leq i \leq p - 1\).
3. Set \(\beta = \alpha^i \mod p\).
4. The public key is \((\alpha, \beta, p)\), and the private key is \(i\). ElGamal uses the property that finding \(i = \log_{\alpha} \beta \mod p\) is difficult.
5. For encryption, pick a secret random number \(k, 1 \leq k \leq p - 2\).
6. Given message \(m\), encryption is: \(E_K(m, k) = (y_1, y_2)\), \(y_1 = \alpha^k \mod p\), \(y_2 = m \beta^k \mod p\).
7. The decryption is done as: \(D_K(y_1, y_2) = y_2(y_1^i)^{-1} \mod p\).

General Idea of Elgamal: mask the plaintext \(m\) by multiplying it with \(\beta^k\) and generate \(y_2\). The value \(\alpha^k\) also becomes part of the ciphertext (Bob will use \(\alpha^k\) to compute \(\beta^k\) and recover \(m\) by using its private key \(i\)). Note that if Eve can compute \(\log_{\alpha} \beta = i\), then she can decrypt the message.

**Question** Does Elgamal encryption of a plaintext yield the same ciphertext? If not, how many are the possible ciphertexts?

1.4 Example

As example from the textbook (example 6.1, Stinson). Alice performs encryption as follows.

Let \(p = 2579\), \(\alpha = 2\). Choose \(i = 765\).

1. \(\beta = \alpha^{765} = 2^{765} \mod 2579 \equiv 949 \mod 2579\).
2. Message \(m = 1299\). Pick random number \(k = 853\).
3. \(y_1 = \alpha^k \mod p = 2^{853} \mod 2579 \equiv 435 \mod 2579\).
4. \(y_2 = m \beta^k \mod p = 1299 \times 435^{853} \mod 2579 \equiv 2396 \mod 2579\).

Therefore \(E_K(1299, 853) = (435, 2396)\).

The decryption by Bob is as follows.

\(D_K(y_1, y_2) = y_2(y_1^i)^{-1} \mod 2579 = 2396(435^{765})^{-1} \mod 2579 \equiv 1299 \mod 2579 = m\).

For Elgamal to be secure, \(p\) should have at least 300 digits, and \(p - 1\) must have at least one large prime factor.