MA080G Cryptography Assignment Block 3

Viktor Rosvall

May 14, 2019

Question 3

c. Explain the discrete logarithm problem.

d. Explain the operation of the ElGamal public-key cryptosystem

Answer 3

c. The discrete logarithm problem is potential solution to the problem of finding the private exponent d, such that $x \equiv y^d \pmod{n}$ in the RSA cryptosystem.

> **Definition:** given x, y and a prime p such that:
>
> $$y \equiv x^e \pmod{p}$$
>
> find e.

This problem however is believed to be as hard as factorization and not yet proven to be NP-complete. The order or x should be as large as possible to avoid it being broken by a exhaustive search. So x should be chose as a primitive root mod p, which is an element of order $\lambda(p) = p - 1$

d. Let prime $p = 23$ and the primitive root $g = 5$.

The ElGamal cryptosystem works as: Bob chooses a prime p and a primitive root g mod p. He then chooses a *secret* exponent $a \in$

$\{1, ..., p-1\}$. Let $a = 3$ and compute

$$h = g^a \text{ MOD } p = 5^3 \text{ MOD } 23 = 23$$

This gives us the *public key* $(p, g, h) = (23, 5, 10)$ and the private component $a = 3$.

Say Alice want's to send a plaintext message x to Bob, where $x \in \{1, ..., p-1\}$. Let $x = 6$. Alice then choose a *secret* exponent $k \in \{1, ..., p-1\}$. Let $k = 8$ and compute

$$\begin{aligned} y_1 &= g^k \text{ MOD } p & y_2 &= xh^k \text{ MOD } p \\ &= 5^8 \text{ MOD } 23 & &= 6 * 10^8 \text{ MOD } 23 \\ &= 16 & &= 12 \end{aligned}$$

where p, g, h is Bob's *public key*. This gives Alice the ciphertext pair $(y_1, y_2) = (16, 12)$.

Bob receives the message $(y_1, y_2) = (g^k, xh^k) \bmod p$. Bob knows his secret number a such that $h = g^a \pmod p$, so he can thus compute

$$h^k \equiv (g^a)^k \equiv (g^k)^a \pmod p$$

Remember that Bob knows g^k from the ciphertext pair Alice sent. He also knows his secret a. He can thus easily compute

$$h^k \equiv (g^k)^a \pmod p = 16^3 \text{ MOD } 23 = 2$$

For Bob to extract x from xh^k he needs to compute the inverse of h^k, i.e., $(h^k)^{-1}$ with the EEA of h^k and p, which gives us

$$(h^k)^{-1} = \text{EEA(2,23)} = 12$$

Multiply the inverse of with xh^k

$$xh^k * (h^k)^{-1} \text{ MOD } p = x \text{ MOD } p = x$$

$$x = 12 * 12 \text{ MOD } 23 = 6$$

$$x \text{ MOD } 23 = 6$$

gives us $x = 6$.