Lecture 8

Public-Key encryption

RSA Cryptosystem
[Rivest, Shamir, Adleman]

Its security is related to the difficulty of finding the factorization of a composite positive integer that is the product of two large primes.

The exchange of keys is an very important part of any symmetrical cryptosystem. Symmetrical systems are much faster than public-key encryption systems (such as RSA).

There are two RSA keys.

Bob generates randomly and independently two large prime number p and q and computes the product

$$n = pq.$$

Bob also chooses an integer e with

$$1 < e < \varphi(n) = (p-1)(q-1)$$

$$\gcd(e, (p-1)(q-1)) = 1.$$

Note, that e is always odd.

Bob computes an integer d with

$$de \equiv 1 \mod (p-1)(q-1)$$

Since $\gcd(e, (p-1)(q-1)) = 1$, such a number d exists. It can be computed by the extended euclidean algorithm.

Bob's public key is the pair (n, e).

n - is called the RSA modulus

e is called the encryption exponent.

d is Bob's ~~private~~ private key (it is a secret key and only Bob knows it) - decryption ~~to~~ exponent

The secret key should be secure: in fact it can be computed from the encryption exponent e, if prime factors p and q of n are known.

It is important to understand how the factors p and q have to be chosen in order to make the factorization of n infeasible.

Example 1. Choose the prime factors

$p = 11$ and $q = 23$.

Therefore $n = 11 \times 23 = 253$.

and $(p-1)(q-1) = 10 \times 22 = 220 = 4 \cdot 5 \cdot 11$

The smallest possible $e = 3$. $\gcd(3, 220) = 1$

Then $d = 147$ $(441 \equiv 1 \mod 220.)$

Encryption

The plaintext space consists of all integers m with

$$0 \leq m < n.$$

A plaintex is encrypted by computing

$$c = m^e \bmod n.$$

The cyphertext is c. In order to encrypt the message it is sufficient to know the public key (n, e).

Example 2. Let $n = 253$ and $e = 3$.
The plaintext space is $\{0, 1, \dots, 252\}$.
Encrypting the integer $m = 165$ we get

$$c = 165^3 \bmod 253 = 110.$$

Decryption

The decryption is based on the following theorem.

Th. Let (n, e) be a public RSA key and d the corresponding private RSA key. Then

$$(m^e)^d \bmod n = m$$

(i.e. $c^d \bmod n = m$)

for any integer m with $0 \le m < n$.

Example 3. Let $p = 3$, $q = 7$ (primes) then $n = 3 \cdot 7 = 21$.

We get $\varphi(21) = 2 \cdot 6 = 12$ $(= 4 \cdot 3)$

Select $e = 5$, such that $\gcd(5, 12) = 1$.

Solve equation

$$e\,d \equiv 1 \mod 12.$$

by using extended Euclidean algorithm

$d = 5$ (i.e. $5 \cdot 5 = 25 \equiv 1 \mod 12$)

Select $m = 14$ and calculate cyphertext

$$c = 14^5 \mod 21$$

$$14^2 = 196 \equiv 7 \mod 21$$

$$14^4 = 7 \cdot 7 = 49 \equiv 7 \mod 21.$$

$$c = 7 \cdot 14 = 98 \equiv 14 \mod 21.$$

Explain, why we expected to get $c = 14$.

$$c^d = 14^5 \equiv 14 \mod 21.$$

Proof. Since

$$ed \equiv 1 \mod (p-1)(q-1)$$

there is an integer l with

$$ed = 1 + l(p-1)(q-1)$$

Therefore

$$(m^e)^d = m^{ed} = m^{1+l(p-1)(q-1)}$$

$$= m\, m^{l(p-1)(q-1)} = m\left(m^{(p-1)(q-1)}\right)^l$$

Let formulate theorem of Fermat

T. (Fermat)
If $\gcd(a, b) = 1$, then
$a^{\varphi(b)} \equiv 1 \mod b$.

Ex. $a = 4$, $b = 3 \Rightarrow \gcd(4, 3) = 1$

$\varphi(3) = 2$ $\quad 4^2 = 16 \equiv 1 \mod 3$.

Let assume that p is not the divisor of m. (i.e. $\gcd(p, m) = 1$)
Then it follows from Fermat theorem that

$$m^{p-1} \equiv 1 \mod p$$

and

$$(m^e)^d = m\,(m^{p-1})^{(q-1)e} \equiv m \mod p$$

If is p divisor of m, then

$$(m^e)^d \equiv m \mod p$$, because both sides of the congruence $0 \mod p$.

Note, we obtained the equivalence equality only, but still we can't compute m by solving this equation (computing mod p).

Analogously we see that

$$(m^e)^d \equiv m \bmod q$$

Because p and q are distinct prime numbers we obtain

$$(m^e)^d \equiv m \bmod n.$$

The proof follows from the fact that $0 \leq m < n$.

$$(m^e)^d - m \equiv 0 \bmod p$$

$$(m^e)^d - m = \ell p$$

$$(m^e)^\ell - m = k q$$

$$\ell = sq$$

$$\Rightarrow \boxed{(m^e)^d - m = sqp = sn}$$