RSA cryptosystem

Lesson 2

DECENTRALIZED fit@hcmus.CRYPT

RSA theorem

- Let p, q be two different primes and $n = pq$ and $\varphi = \varphi(n) = (p-1)(q-1)$;
- Let e, d be to integers such that $ed \bmod \varphi = 1$.
- $\forall m \in \{0, 1, \ldots, n-1\}$, if $c = m^e \bmod n$ then $m = c^d \bmod n$, and vice versa.

Ring $\mathbb{Z}_n$

$(\mathbb{Z}_n, +, *)$: ring, where

- $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$
- $\forall a, b \in \mathbb{Z}_n, c = +(a, b) = (a + b) \; mod \; n.$
- $\forall a, b \in \mathbb{Z}_n, c = *(a, b) = (a * b) \; mod \; n.$

Definition (inverse element)

- $x \in \mathbb{Z}_n$ is invertible iff there exists $y \in \mathbb{Z}_n$: $(y * x) mod \; n = 1$. y is called the inverse of x, we write $y \equiv x^{-1} (mod \; n)$.
- $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : x \; is \; invertible\}$

Proposition. $x \in \mathbb{Z}_n^* \Leftrightarrow x, n : co - primes.$

RSA implementation:- (1) Big Integer

- $x \in \mathbb{Z}_N \;\equiv\; x_0 x_0 \ldots x_{n-1} \colon x_i \in \{0, 1\}, \forall 0 \leq i \leq n, n = \lceil log_2(N) \rceil - 1$
- Add_Mod(x, y, N) = (x + y) mod N.
- Mul_Mod(x, y, N) = (x * y) mod N.
- Power_Mod(x, p, N) = x^p mod N = (x*x mod N)…(x*x mod N).

RSA implementation:- (2) Euclid theorem

Euclid theorem:

- gcd(a, a) = a.
- gcd(a, b) = gcd(a/2, b) if a is even and b is odd.
- gcd(a, b) = gcd(a/2, b/2) if both a and b are even.
- gcd(a, b) = gcd(a, b-a) if both a and b are even and suppose that b > a.

Extended Euclid theorem (Bezout theorem)

- $\forall a, b \in \mathbb{N}, \exists x, y \in \mathbb{Z}: ax + by = \gcd(a, b)$.

RSA implementation:- (3) primes

- $\wp = \{p \ \in \mathbb{N}: \forall 2 \leq i \leq p - 1, \mathrm{gcd}(p, i) = 1 \equiv (p, i) = 1\}$
- Theorem (the little Fermat theorem)

$p \in \wp, \forall b: b \dagger p \ then \ b^{p-1} \ mod \ p = 1.$

- Definition (pseudo-prime)

$n \in \mathbb{N}^{+}, b: 1 \leq b \leq p - 1$, is called a pseudo-prime with base b iff $b^{n-1} \ mod \ n = 1.$

RSA protocol

Alice		Bob
(1) p, q ← PrimeGen(λ) n ← p*q φ ← (p-1)*(q-1) e, q ← KeyGen()		
(2) Publish (e, n)		
		(3) c ← PowerMod(m,e,n)
	←	
(4) m ← PowerMod(c,e,n)		

Prove RSA:- (1) Chiness Remainder Theorem

Chiness Remainder Theorem (CRT)

- n_1, ..., n_p be p intergers such that $(n_i,n_j)=1$, $\forall 1 \leq i, j \leq p$ and $i \neq j$.
- a_1,..., a_p be p integers such that $a_i \geq 0$, $\forall 1 \leq i \leq p$.

The congruent equations system

$$\begin{cases} x & \equiv & a_1 \ (mod\, n_1) \\ \ldots & \ldots & \ldots \\ x & \equiv & a_p \ (mod\, n_p) \end{cases}$$

has uniquement solution in $\mathbb{Z}_N$, where $N = n_1 \times \cdots \times n_p$.

RSA proving:- (2) Prove CRT

$$\begin{cases} x & \equiv & a_1\ (mod\ n_1) \\ \dots & \dots & \dots \\ x & \equiv & a_p\ (mod\ n_p) \end{cases}$$

- Let $N = n_1 \times \cdots \times n_p$ and $N_i = \frac{M}{n_i}, \forall 1 \leq i \leq p$. We have
- $(N_i, n_j) = 1, \forall 1 \leq i \leq p\ and\ i \neq j$, so there exists $N_i^{-1}(mod\ n_j)$,
- $N_i^{-1} = Bezout(N_i, n_j)$.
- Let $x = a_1 N_1 N_1^{-1}(mod\ n_1) + \cdots + a_p N_p^{-1}\left(mod\ n_p\right)$, then

$x\ mod\ n_1 = a_1 + 0 = a_1$

…

$x\ mod\ n_p = 0 + a_p = a_p$

- So x is solution

Prove RSA theorem

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

Fast decrypting

- Let $d_1 = d \bmod (p - 1) \Rightarrow \exists k_1: k_1(p - 1) + d_1 = d$
- Let $d_2 = d \bmod (q - 1) \Rightarrow \exists k_2: k_2(q - 1) + d_2 = d$
- $c^d \bmod p = c^{k_1(p-1) + d_1} = (c^{(p-1)})^{k_1} c^{d_1} = c^{d_1}$ (*)
- $c^d \bmod q = c^{k_2(q-1) + d_2} = (c^{(q-1)})^{k_2} c^{d_2} = c^{d_2}$ (**)

- $(p, q) = 1$, let $x = c^d$, by (*) and (**) we have a congruent equations system: $\begin{cases} x \equiv c^{d_1} (mod\ p) \\ x \equiv c^{d_2} (mod\ q) \end{cases}$ and $x = m$ is a unique solution of this system.