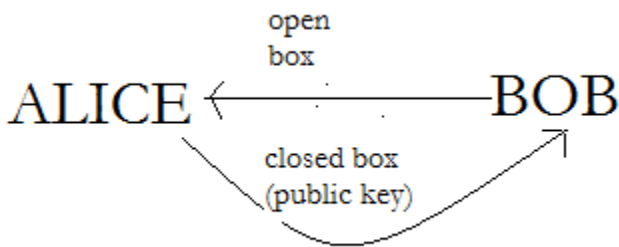


Public Key Cryptography

General Idea



Alice and Bob share a public key which ensures Integrity and Availability.

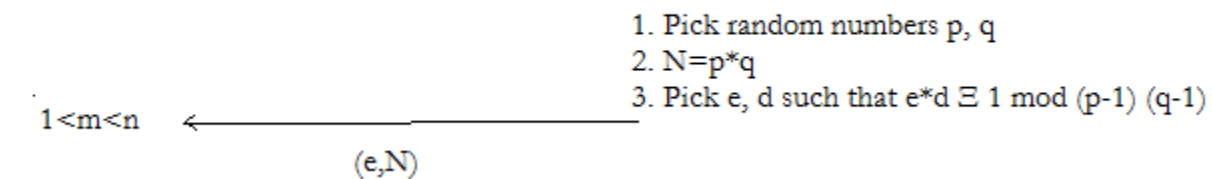
Note that in public key cryptography secrecy not needed between both parties.

RSA Algorithm:

It works as follows

Alice

Bob



$$C = m^e \pmod n \xrightarrow{c}$$

$$M^1 = c^d \pmod n$$

Fact $m = m^1$

Proof:

$$\begin{aligned}
 C^d &= (m^e)^d \pmod n \\
 &= m^{ed} \pmod n \\
 &= m^{x(p-1)(q-1)+1} \pmod n \\
 &= 1^x m^1 \pmod n \quad \text{[Euler's theorem]} \\
 &= m \pmod n
 \end{aligned}$$

Attacks:

Factoring of N: If N is n bits long then algorithm runs in $O(e^{2(n)^{1/3}(\log n)^{2/3}})$

In practice if n=640 then N can be factorized in 8 months using 80 aprons.

if n=2048 then it will be 8 million times harder to break N.

Finding Large Primes:

For a number $\leq X$, number of primes are $\leq X/\ln X$.

For example if $X \leq 2^{1024}$ there are about $2^{1024} / \ln(2^{1024})$ prime number cases.

To find a large prime number $1 < m < N$

- Pick a random $X \leq 2^{1024}$
- Test if it is prime
- Repeat until success

Other things to be learned:

How to test for primes

Euler's theorem

Binary exponentiation

Key recovery attack: Factoring \leftrightarrow find (p-1) (q-1) \leftrightarrow find d

Since (p-1)(q-1) is divisible by 4 and trails $p*q$ by $p+q-1$ one might assume we can do it quickly but for 1024 bit long operation it is still not feasible in given time.

Chosen Cipher Text Attack:

Adversary: Given cipher text c,

$$C^1 = 2^e C \text{ mod } N$$

$$\begin{aligned}
 \text{Bob: } m^1 &= (c^1)^d \pmod N \\
 &= 2^{ed} c^d \pmod N \\
 &= 2 m \pmod N
 \end{aligned}$$

$$\text{Adversary: } 2^{-1} 2 m = m \pmod N$$

Attacker changes CTXT and understands how it modifies PTXT

Basic Number Theory:

Consider $Z/NZ = \{0, 1 \dots n\}$;

If $a, b \in Z/NZ$

$$\text{Then } a+b = (a+b) \pmod n$$

$$\text{And } a*b = (a*b) \pmod n$$

Facts: The above Z/NZ follows following properties.

- Commutative
- Distributive
- Associative
- 0 exists
- 1 exists
- Negative/ additive inverse exists
- Multiplicative inverse exists sometimes
- We can delay taking mod till the end

The GCD of two numbers is 1 then they are relatively prime numbers.

Definition: $\text{GCD}(a, b) = X$ where X is the smallest possible integer of the form $s.a+t.b$ where $s, t \in Z/NZ$

Proof: Suppose $d|a, d|b$ then $d|s.a+t.b$

$$\text{So } \text{GCD}(a, b) | s.a+t.b; \quad \text{Hence } \text{GCD}(a, b) | X;$$

Remaining proof will be done in next class.