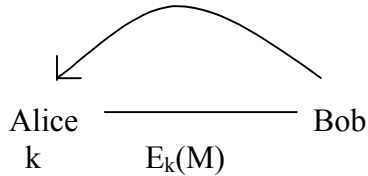


Network Security (CSE 508)

Lecture Oct 12, 2009

Public key cryptography

- has an encryption key and a decryption key



- Bob sends message (safe) to Alice and Alice, which has a public key, encrypts it and send back to Bob. Bob then uses its private key to decrypt it. Hence anybody who sends the safe, could have it encrypted by Alice & could be a recipient.

Safe crypt

- Only ensures that safe sender is the recipient
- Does not authenticate Alice

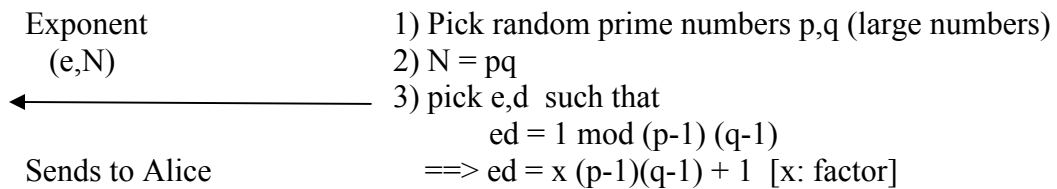
Key agreement

- Secrecy
- Integrity
- Availability

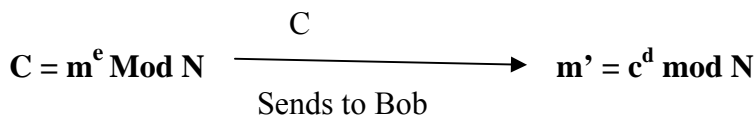
RSA

Alice

Bob



Where $1 < m < N$



Fact $m' = m$

Fact $c^d \equiv (m^e)^d \pmod N$ [since $c = m^e$]

$\equiv m^{ed} \pmod N$

$\equiv m^{x(p-1)(q-1) + 1} \pmod N \quad \text{-----} \rightarrow I$

Fact1: $m^{(p-1)(q-1)} = 1 \pmod N$ (Euler's Theorem)

Using Fact1 in I, we get,

$$\begin{aligned}c^d &= m^1 \pmod{N} \\ &= m \pmod{N}\end{aligned}$$

To break it, factor N

==> we will get p,q

==> get p-1, q-1

As we have 'e', 'p', and 'q', we can compute 'd' now and then compute m'.

And by doing so, any sender could become a recipient like Bob.

Attacks:

Factor N

Best factoring algorithm:

If N is 'n' bits long, Then Generalized NFS runs in $O(e^{2n^{1/3}} (\log n)^{2/3})$ time.

Finding Large primes:-

Fact (prime number theorem):-

The number of primes $\leq X$ is $\approx (X / \ln X)$

Example: There are about $2^{1024} / \ln(2^{1024})$ primes $\leq 2^{1024}$

By theoretically, $\ln(2^{1024}) < 1024$

On calculation, $\ln(2^{1024}) \cong 700$

To find large primes:-

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

How to test for prime?

- Euler's theorem
- Binary exponentiation

Factoring \Leftrightarrow find $(p-1)(q-1) \Leftrightarrow$ find d.

Chosen cipher text attacks (CCA)

Step 1:

Mallory: Given cipher text 'c', for message 'm'

$c' = 2^e c \pmod{N}$ (disguise 'c' as 'c'' and send it to Bob such a way that he decrypts it)

Step 2:

From Bob: we get

$$\begin{aligned}m' &= (c')^d \pmod{N} \\ &= 2^{ed} c^d \pmod{N}\end{aligned}$$

As decryption of $2^{ed} = 2$,

$$m' = 2m \cdot \text{mod } N \rightarrow (\text{Since, } m' = c^d \text{ mod } N \text{ and fact: } m' = m \text{ mod } N)$$

Step 3:

Mallory: $2^{-1} 2m \equiv \text{mod } N$

So here we are having an Integrity problem as Mallory can change the text.

Basic Number Theory:-

$Z \text{ mod } N \text{ } Z \rightarrow$ denoted as $Z/NZ = \{ 0, \dots N-1 \}$

$$a, b \in Z / NZ$$

then, $a + b = (a + b) \text{ mod } N$ and $a * b = (a * b) \text{ mod } N$

Fact:-

These,

- are commutative
- are distributive
- are associative
- 0 exists [for '+' ,since $a + 0 = a \text{ mod } N$]
- 1 exists [for '*' ,since $a * 1 = a \text{ mod } N$]
- negative exists .

$$\text{Since, } (a + (-a) = 0)$$

here (-a) is (N - a)

$$a + (N - a) = N \text{ mod } = 0$$

- Inverses sometimes exist (**a, 1/a**)

- Also exponent works (i.e.,) $(x^d)^c = x^{cd}$
 $= (x^c)^d \text{ mod } N$
 Also, $x^{a+b} = x^a x^b \text{ mod } N$

All rules mentioned work as long as there is no division.

Greatest Common Divisor:

Definition:-

$\text{gcd} (a, b)$ = the largest common divisor. [If the gcd of 2 numbers is 1, we call it relatively prime. Example: $\text{gcd} (21,10)$, $\text{gcd} (17,19)$]

Fact:- $\text{gcd} (a, b) = x$, when x is the smallest positive integer of the form $sa+tb$ where s, t belongs to Z.

Proof:-

Suppose $d|a$ and $d|b$

($\Rightarrow d$ is a divisor of 'a')

Then d divides $sa + tb$

$$(a/d \Rightarrow sa/d , b/d \Rightarrow tb/d)$$

$$\Rightarrow (sa + tb)/d$$

So, $\text{gcd} (a, b)$ divides $sa + tb$

Hence, $\text{gcd} (a, b)$ divides X

$\Rightarrow \text{gcd} (a, b) \leq X$ (where $X = sa + tb$).