

Network Security(CSE 508)

Date : 10/19/2009

Submitted by : Linet D'souza

Definition : $(\mathbb{Z}/N\mathbb{Z})^* = \{0 < x < n \mid \gcd(x, n) = 1\}$

Example : $(\mathbb{Z}/6\mathbb{Z})^* = \{0, 5\}$

$$\Phi(N) = |(\mathbb{Z}/N\mathbb{Z})^*|$$

Where $\Phi(N)$ are the numbers between 1 and N that are relatively prime to N.

If P is the prime number

$$\Phi(P) = P - 1$$

$$0 \quad p \quad 2p \quad 3p \quad \dots \quad p^2 \quad \dots \quad p^n$$

$$\begin{aligned}\Phi(P^n) &= p^n - p^{(n-1)} \\ &= (p-1) p^{(n-1)}\end{aligned}$$

$\gcd(a, b) = 1$ then $\Phi(a, b) = \Phi(a) \cdot \Phi(b)$

If p and q are distinct primes,

$$\Phi(p, q) = (p-1)(q-1)$$

If $\gcd(a, b) = 1$ then $\Phi(a, b) = \Phi(a) \cdot \Phi(b)$

By CRT

$$\mathbb{Z}/ab\mathbb{Z} \sim \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

So invertible elements of $\mathbb{Z}/ab\mathbb{Z} \sim$ invertible elements of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

$$\Phi(21) = \Phi(3) \cdot \Phi(7) = 2 \cdot 6 = 12$$

$$(\mathbb{Z}/21\mathbb{Z})^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

Theorem : If $\gcd(a, N) = 1$, Then $a^{\Phi(N)} = 1 \pmod N$

Proof : if $b \neq c \pmod N$

Then $ab \neq ac \pmod N$

Since otherwise, we would have $b = a^{-1} a \cdot b = a^{-1} a \cdot c = c$

If $b \in (\mathbb{Z}/N\mathbb{Z})^*$, then so is ab . so multiplying by 'a' just permutes the elements of $(\mathbb{Z}/N\mathbb{Z})^*$

$$\prod_{b \in (\mathbb{Z}/N\mathbb{Z})^*} b = \prod_{b \in (\mathbb{Z}/N\mathbb{Z})^*} ab$$

$$= a^{\phi(N)} \prod_{b \in (\mathbb{Z}/N\mathbb{Z})^*} b \pmod N$$

thus, $a^{\phi(N)} = 1 \pmod N$

$$ed = 1 \pmod{\phi(N)}$$

$$\begin{aligned} ((m^e)^d) &= m^{ed} \\ &= m^{b\phi(N)+1} \\ &= (m^{\phi(N)})^b \cdot m \\ &= m \pmod N \end{aligned}$$

RSA

1. Pick $p, q, N=pq$
2. Pick e, d such that $ed = 1 \pmod{\phi(N)}$

Public key : (e, N)

Private key : (d, N)

$$e = 3$$

$$d = 3^{-1} \pmod{\phi(N)}$$

Miller Rabin Primality test

Isprime(N)

Let $N-1 = 2^r q$ where q is odd

Pick a randomly mod N and compute

| | | | | |
|-------|----------|----------|------|-----------|
| a^q | a^{2q} | a^{4q} | | a^{2rq} |
| b_0 | b_1 | b_2 | | b_r |

If $b_r \neq 1$ output COMPOSITE

Say $b_i \neq 1, b_{i+1} \neq 1$

If $b_i \neq -1$ output composite
 Else output "probably prime".

Fact : Pr [Miller Rabin N is prime when N composite] $\leq \frac{1}{4}$

If we repeat the test l times
 $\text{Pr}[\text{error}] \leq (1/4)^l = (1/2)^{2l}$

Example : $N = 17$

$a = 3$

$b_0 = 3$

$b_1 = 9$

$b_2 = 13$

$b_3 = 16 = -1$

RSA can also be used as signatures

In a network of m nodes.

No. of keys required symmetric key = $m(m-1)/2$

Public key = m keypairs

So in public key encryption, key management is easy.

RSA signatures

Alice

$S_A = (d, N)$

$m \parallel m^d \pmod N$ \longrightarrow

$m \parallel h(m)^d \pmod N$ \longrightarrow

$SA = (d_A, N_A)$

$PB = (e_B, N_B)$

$C = m^{e_B} \pmod{N_B}$
 $t = h(c)^{d_A} \pmod{N_A}$

$c \parallel t$ \longrightarrow

Bob

$P_A = (e, N)$

$m \parallel t$
 $m = t^e \pmod N$

$m \parallel t$
 $h(m) = t^e \pmod N$

$PA = (e_A, N_A)$

$SA = (d_B, N_B)$

$h(c) = t^{e_A} \pmod{N_A}$
 $m = h(c)^{d_B} \pmod{N_B}$