

Public Key Cryptography – Part 3

Notes for : 19 Oct 2009

Notes by : Manoj Harpalani

Professor : Rob Johnson

Topics Covered:

1. More RSA
2. Euler's Theorem
3. Miller Rabin's Primality Test Algo
4. Advantage of Public Key over Symmetric.
5. RSA Signatures

Def.

$(\mathbb{Z}/n\mathbb{Z})^* = \{0 < x < N \mid \gcd(x, N) = 1\}$ -- Set of all integers less than N which are relatively prime to N

Ex. $(\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\}$

$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ -- Number of elements in $(\mathbb{Z}/n\mathbb{Z})^*$

$\phi(6) = 2$

For prime number p:

$\phi(p) = p - 1$

$\phi(p^n) = p^n - p^{n-1}$

If $\gcd(a, b) = 1$; $\phi(ab) = \phi(a)\phi(b)$

If p and q are prime $\phi(pq) = (p - 1)(q - 1)$

Ex. $\phi(21) = \phi(3)\phi(7) = 2 \times 6 = 12$

$(\mathbb{Z}/12\mathbb{Z})^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

Euler's Theorem:

If $\gcd(a, N) = 1$ then $a^{\phi(N)} = 1 \pmod N$

Proof:

$\gcd(a, N) = 1$, then a has an inverse

If $b \equiv c \pmod N$

Then $ab \neq ac \pmod N$

Since otherwise we would have

$b = a^{-1}ab = a^{-1}ac = c$, which is contradicting.

Now $\gcd(a,N)=1, \gcd(b,N)=1 \rightarrow \gcd(ab,N)=1$

If $b \in (Z/nZ)^*$ then so does ab .

Thus multiplying by a just permutes the elements of $(Z/nZ)^*$

Now Imagine:

$$\prod_{b \in (Z/nZ)^*} b = \prod_{b \in (Z/nZ)^*} ab = a^{\phi(n)} \prod_{b \in (Z/nZ)^*} b$$

$$\text{Thus } a^{\phi(n)} = 1 \pmod N$$

This result is used in RSA for decryption:

$$ed \cong 1 \pmod{(p-1)(q-1)}$$

$$ed \cong 1 \pmod{\phi(n)}$$

$$\text{Since } \phi(n) \mid ed - 1 \rightarrow b \phi(n) = ed - 1 \rightarrow ed = b \phi(n) + 1$$

$$c^d = M^{b \phi(n) + 1} \pmod N$$

$$c^d = M \pmod N$$

Note: When $\gcd(m,N)$ is not 1 usually, but if one finds it to be close to 1, then discard the public and private key as $\gcd(m,N)$ has to be either p or q .

Terminology \rightarrow Non Trivial GCD \rightarrow which is not 1.

In RSA if encryption key e is small, then encryption is fast whereas decryption key is large hence decryption becomes slow. Hence one should chose these keys carefully.

Miller Rabin's Primality Test:

$\text{Is_Prime}(N)$

Let $N - 1 = 2^r \cdot q$ where q is odd. \rightarrow { Pulling out powers of 2 }

Pick a random value for 'a' mod N. {0, -1 etc are not good choices}

Compute $a^q, a^{2q}, a^{4q}, \dots, a^r$ and Name them as $b_0, b_1, b_2, b_3, \dots, b_r$

If $b_r \neq 1$

Output "Composite"

Else

Say $b_i \neq 1 \Rightarrow b_{i+1} = 1$

If $b_i \neq -1$ then Output "Composite"

Else Output "Probably Prime"

Probability $P[\text{Miller Rabin says prime for composite } N] \leq \frac{1}{4}$

Hence to increase the accuracy of the test, usually its run 256 times on a number that is output as Prime.

If Miller Rabin finds a number to be composite there is no need to check for a second time. It has to be composite.

Ex.

$N = 17$

$N-1 = 16 = 2^4 \cdot 1$

So we have $r=4$ and $q=1$.

Choose $a = 3$.

$b_0 = 3, b_1 = 9, b_2 = 81 \bmod 17 = 13, b_3 = 169 \bmod 17 = 16 = -1, b_4 = 1$

Output \rightarrow Probably Prime

Ex. $N = 15$

$N-1 = 14 = 2 \cdot 7$

So we have $r=1$ and $q=7$.

$$b_0 = 8, b_1 = 4$$

Since $b_r \neq 1$, hence Output Composite

Advantage of Public Key over Symmetric Key Crypto:

In a Network of m users :

No. of keys required to communicate securely using Public key Crypto – m pairs.

No. of keys required to communicate securely using Symmetric key Crypto – $m(m-1)//2$

Hence public key crypto has a simpler key management process.

RSA Signatures:

Public key crypto can be used as an authentication MAC.

Alice ----- Bob

C||T

Private Key – (d_A, N_A)

Private Key – (d_B, N_B)

Public Key – (e_A, N_A)

Public Key – (e_B, N_B)

1. $C = (M^{e_B} \bmod N_B)$
2. $T = H(C)^{d_A} \bmod N_A$
3. Send C||T

4. Check if $H(C) == (T)^{e_A} \bmod N_A$
5. If yes then $M = (C)^{d_B} \bmod N_B$

In this way Public Key Crypto – RSA can be used for authenticating the message sender.