

Kenzley Alphonse
 CSE 508
 10/19/09

Topics: Miller-Rabin primality test, RSA Signatures

Def $(\mathbb{Z}/N\mathbb{Z})^* = \{ 0 \leq x \leq N \mid \gcd(x, N) = 1 \}$

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

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

$$\varphi(P) = P - 1 \text{ where } P \text{ is prime}$$

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

$$\gcd(a, b) = 1 \rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$$\text{If } p \text{ \& } q \text{ are prime } \varphi(p \cdot q) = (p - 1)(q - 1)$$

If $\gcd(a, b) = 1 \rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

By CRT

$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ so invertible elements of $\mathbb{Z}/ab\mathbb{Z}$ equals the invertible elements of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

$$\varphi(21) = \varphi(3) \cdot \varphi(7) = (3 - 1)(7 - 1) = 2 \cdot 6 = 12$$

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

Theorem $\gcd(a, N) = 1$ then $a^{\varphi(N)} \equiv 1 \pmod N$

Proof If $b \neq c$ then $ab \neq ac \Rightarrow b \neq c \pmod N$ then $ab \neq ac \pmod N$ since otherwise we would have $b = a^{-1}ab = a^{-1}ac = c$

■

If $b \in (\mathbb{Z}/N\mathbb{Z})^*$, then so is ab

So multiply by a , permutes the elements of $(\mathbb{Z}/N\mathbb{Z})^*$

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

Thus $a^{\varphi(N)} \equiv 1 \pmod N$

Now sub $(p-1)(q-1)$ to $\varphi(N)$

$$ed \equiv 1 \pmod{\varphi(N)}$$

$$ed = b\varphi(N) + 1$$

$$b\varphi(N) = ed - 1$$

$$\varphi(N) \mid ed - 1$$

$$(m^e)^d = m^{ed} = m^{b\varphi(N)+1} = (m^{\varphi(N)})^b m = 1^b \cdot m = m \pmod N$$

$e = 3$ Public key: (e, N)

$d \equiv 3^{-1} \pmod{\varphi(N)}$ Public key: (d, N)

Encryption is fast but decryption is slow

Miller-Rabin Primality Test

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

Pick a randomly $\pmod N$ and compute $b_0 = a^q, b_1 = a^{2q}, b_2 = a^{4q}, \dots, b_{r-1} = a^{2^{r-1}q}$.

If $b_r \neq 1$, output Composite

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

If $b_i \neq -1$, output Composite

Else output "Probably Prime"

Fact $\Pr[\text{Miller-Rabin say prime when composite}] \leq \frac{1}{4}$

If we repeat the test l times, then $\Pr[\text{error}] \leq \left(\frac{1}{4}\right)^l \leq \frac{1}{2^{2l}}$ i.e. $l = 256$

Example

$N = 17$ & $a = 3$

$N - 1 = 2^4 q \Rightarrow 16 = 2^4 q \Rightarrow q = 1$

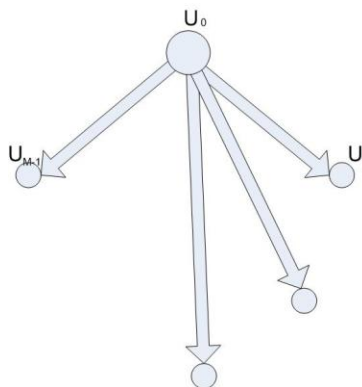
$b_0 = 3, b_1 = 9, b_2 = 13, b_3 = -1, b_4 = 1$

$N = 15$ & $a = 2$

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

$b_0 = 8, b_1 = 4$

Using RSA for signatures also



Symmetric key: $m(m - 1)$ key pairs

Public key: m keypairs

You can also use RSA as a MAC

Alice
 $S_A = (d, N)$
 $P_B = (e, N)$

$$m \parallel m^d \bmod N$$



$$m \parallel h(m)^d \bmod N$$



$$c \equiv m^{e_B} \bmod N_b$$
$$t \equiv h(c)^{d_A} \bmod N$$

Bob

$$P_A = (e, N)$$
$$S_A = (d, N)$$
$$m \parallel t \rightarrow m \equiv t^e \bmod N$$

$$m \parallel t \rightarrow h(m) \equiv t^e \bmod N$$

$$h(c) \equiv t^{e_A} \bmod N_A$$
$$m \equiv C^{d_B} \bmod N_B$$