

Network Security

CSE 508

October 16, 2009

RSA

- Pick large primes
- Distinguishable primes
- Modular exponentiation
- Modular inverses
- Pick e, d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$

Theorem:

$\gcd(a, b) = x$ where x is smallest positive linear combination of a & b , is $x = sa + tb$

Proof:

1) $\gcd(a, b) \leq x$ (proven lot of time)

2) Goal,

$$x \leq \gcd(a, b)$$

goal,

$$x/a, x/b \text{ (i.e. } x \text{ divides } a \text{ and } b).$$

By division algorithm $\exists q, 0 \leq r < x$

such that $a = q.x + r$

$$r = (1 - q.s)a - q.t.b$$

Thus “ r ” is a linear combination of a & b & $r < x$.

Since “ x ” is the smallest positive linear combination of a & b , “ r ” must not be positive,

Hence $r = 0$, So x/a

similarly x/b

➔ $x \leq \gcd(a, b)$

Extended Euclidean Algorithm:

Pick 2 numbers say, 24 and 33

$$1 * 24 + 0 * 33 = 24 \quad \rightarrow \quad [1 \quad 0 \quad 24]$$

$$0 * 24 + 1 * 33 = 33 \quad [0 \quad 1 \quad 33]$$

$$[1 \quad -1 \quad 9]$$



(subtract 1st - 2nd)

mod 33/24

Now,

$$\begin{array}{l} -1 [0 \quad 1 \quad 24] \\ -2 [0 \quad -1 \quad 9] \\ -1 [-2 \quad 3 \quad 6] \\ -2 [3 \quad -4 \quad 3] \\ \quad [-8 \quad 11 \quad 0] \end{array} \quad \rightarrow \begin{array}{l} 3(33) + (-4)(24) = 3 \\ 99 \quad - 96 \quad = 3 \end{array}$$

RSA Step

Pick e, d such that $e \cdot d = 1 \pmod{(p-1)(q-1)}$

- 1) Pick “ e ” randomly such that
- 2) Use extended Euclidean algorithm

$$\gcd(e, (p-1)(q-1)) = 1$$

To find s, t such that

$$s \cdot e + t \cdot (p-1)(q-1) = 1$$

Definition: $a = b \pmod m$

$$\Leftrightarrow m/a - b$$

$$6 = 9 \pmod 3$$

$$s \cdot e - 1 = -t \cdot (p-1)(q-1)$$

$$s \cdot e = 1 \pmod{(p-1)(q-1)}$$

so take, $d = s$.

Modular Inverses:

Given a & m , When does there exist a, b such that

$$a \cdot b = 1 \pmod m \text{ and how can we find it?}$$

Theorem:-

“ b ” exists

$$\Leftrightarrow \gcd(a, m) = 1$$

Proof (Using extended Euclidean algorithm):-

If $\gcd(a, m) = 1$, then $\exists s, t$ such that $s \cdot a + t \cdot b$ is not equal to 1

hence, $sa = 1 \pmod m$

so, $b = s$

Now suppose “ b ” exists

then $ab = 1 \pmod m$

so, $ab - 1 = qm$

$$ab - qm = 1$$

1 is now a linear combination of a, m .

$$\Leftrightarrow \gcd(a, m) \leq 1$$

since, gcd's are always positive,

$$\mathbf{\gcd(a, m) = 1}$$

Modular exponentiation

$$c = m^e \pmod{N}$$

$$e = 10011011100001$$

$$\begin{array}{ccc} \uparrow & & \uparrow \uparrow \\ e_{13} & & e_1 e_0 \end{array}$$

$$\text{So, } e = \sum_{i=0}^{13} 2^i e_i$$

$$\sum_{i=0}^{13} 2^i e_i$$

→ $m^e = m$ (on substitution)

$$= \prod_{i=0}^{13} (m^{(2^i)^{e_i}} \pmod{N} \quad (\text{Since, } m^{ex} = (m^e)^x \text{ and } m^{(a+b)} = m^a m^b)$$

$$\begin{array}{l} (m^2)^0 = m \quad (m^2)^1 = m^2 \\ (m^2)^2 = m^4 \quad \rightarrow \quad (m^2)^i = (m^{(2^{i-1})})^2 \end{array}$$

And so on, so forth we get
 $O(\log e)$ multiplies

mod exp (m, e, N)

if $e = 0$, return 1;

$a = \text{mod exp}(m, \lfloor e/2 \rfloor, N)$;

$a = a^2 \times m^{e_0} \pmod{N}$, return a;

Modular exponentiation

Example:

$$4^{13} \pmod{7}$$

$$13 = 8 + 4 + 1$$

$$4^{13} = 4^8 4^4 4^1$$

mod 7:

$$4^1 = 4$$

$$4^2 = 2 \quad \rightarrow \quad 4^{13} = 2.4.4 \pmod{7}$$

$$4^4 = 4 \quad = 4 \pmod{7}$$

$$4^8 = 2$$

Miller – Robin Primality test:

Observation:

$$(N-1)^2 = 1 \pmod{N}$$

$$(N-1)^2 = N^2 - 2N + 1$$

So, $(N-1)^2 - 1 = N^2 - 2N$
 $=$ a multiple of N

$$N - 1 = -1 \pmod{N}$$

$$(N-1)^2 = (-1)^2 \pmod{N}$$

$$= 1 \pmod{N}$$

Fact:

If, N is prime, Then the only X such that, $X^2 = 1 \pmod{N}$ is

$$X = \pm 1 \pmod{N}$$

If N is not prime, there are atleast 4 numbers that square to 1 mod N

To prove this, we use *Chinese Remainder Therorem*

If $N = p \cdot q$, where $\gcd(p,q) = 1$, then $\mathbb{Z} \mid \mathbb{N}\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$$X \begin{array}{l} \xrightarrow{\text{-----}} (x \pmod{p}, x \pmod{q}) \\ \xleftarrow{\text{-----}} (a, b), \text{ where } sp + tq = 1 \\ \begin{array}{l} \xrightarrow{\text{-----}} tqa + spb \pmod{N} \\ \xrightarrow{\text{-----}} (tqa \pmod{p}, spb \pmod{q}) \\ \qquad \qquad \qquad = (a \pmod{p}, b \pmod{q}) \end{array} \end{array}$$

since, $tq \pmod{p} = 1$ & $sp \pmod{q} = 1$

➔ these 2 functions are inverse of each other

What numbers give you 1.mod.p?

(If p, q is prime)

$$(\pm 1)^2 = 1 \pmod{p}$$

$$(\pm 1)^2 = 1 \pmod{q}$$

$$(1 \pmod{p}, 1 \pmod{q}) \xrightarrow{\text{-----}} tq + sb = 1 \pmod{N}$$

$$(-1 \pmod{p}, -1 \pmod{q}) \xrightarrow{\text{-----}} -tq - sp \pmod{N} = -1 \pmod{N}$$

$$(1 \pmod{p}, -1 \pmod{q}) \xrightarrow{\text{-----}} tq - sp \pmod{N}$$

$$(-1 \pmod{p}, 1 \pmod{q}) \xrightarrow{\text{-----}} -tq + sp \pmod{N}$$