

CSE-508 (Network Security)**Date: Oct 16th 2009****Submitted by: Manish Mehra****Theorem:** $\gcd(a, b) = x$ where, x is the smallest positive linear combination of a and b such that $\mathbf{x = sa + tb}$ **Proof:** $\gcd(a, b) \leq x$ **Goals:** $x \leq \gcd(a, b)$ and

$$x \mid a \text{ and } x \mid b \text{ (i.e. } x \text{ should divide both } a \text{ and } b)$$

By division algorithm, if a is divisible by x then, there exists quotient q and a remainder r ($0 \leq r < x$) such that $a = qx + r$. Substituting the value of $x = sa + tb$, we get –

$$a = q(sa + tb) + r$$

$$\Rightarrow r = a(1 - qs) - tb$$

Thus, r is a linear combination of a and b and also $r < x$. Since x is the smallest possible linear combination of a and b and since remainder r should be positive, we can conclude that $r = 0$.

Hence, $x \mid a$. Similarly we can prove that $x \mid b$.

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

Extended Euclidian Algorithm:

Extended Euclidian Algorithm can be used to find out the GCD of two numbers efficiently. The GCD can be expressed as a sum of the two original numbers each multiplied by a positive or negative integer.

Let us compute the GCD of 24 and 33 using this method. The numbers 24 and 33 can be written as –

$$1 \cdot 33 + 0 \cdot 24 = 33$$

$$0 \cdot 33 + 1 \cdot 24 = 24. \text{ This can be written in vector form as –}$$

$$\begin{bmatrix} 1 & 0 & 33 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 24 \end{bmatrix}$$

Now the idea is to perform mod operation recursively till 0 is encountered

$$\begin{array}{lll}
 [1 & 0 & 33] \\
 [0 & 1 & 24] \\
 [1 & -1 & 9] \Rightarrow 33 \bmod 24 \\
 [-2 & 3 & 6] \Rightarrow 24 \bmod 9 \\
 [3 & -4 & \mathbf{3}] \Rightarrow \text{GCD of 24 and 33} \\
 [-4 & 11 & 0] \Rightarrow \text{End}
 \end{array}$$

RSA Steps:

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

1. Pick e randomly such that $\gcd(e, (p-1)(q-1)) = 1$
2. Use Extended Euclidian Algorithm to find s and t such that

$$\begin{aligned}
 se + t(p-1)(q-1) &= 1 \\
 \Leftrightarrow se - 1 &= -t(p-1)(q-1) \\
 \Leftrightarrow se &\equiv 1 \pmod{(p-1)(q-1)}
 \end{aligned}$$

Hence take $d=s$

Modular Inverses:

Give a and m when does there exist a b such that $ab \equiv 1 \pmod{m}$?

How can we find it?

Theorem: b exists $\Leftrightarrow \gcd(a, m) = 1$

Proof: If $\gcd(a, m) = 1$, then there exists s and t such that $sa + tm = 1$

$sa = 1 \pmod{m}$. Hence take $b = s$

Now suppose b exists then, $ab = 1 \pmod{m}$

$$\begin{aligned}
 \Leftrightarrow ab - 1 &= qm \quad \text{for some value of } q \\
 \Leftrightarrow ab - qm &= 1
 \end{aligned}$$

Since 1 is a linear combination of a and m , $\gcd(a, m) \leq 1$

Since gcds are always positive, $\gcd(a, m) = 1$.

Modular Exponentiation:

In RSA, the cipher text is obtained as $c = m^e \bmod N$

A simple program would do it as -

$a = 1$

for $i = 1$ to e : $a = a * m$

However this is not at all efficient for high values of e . This can be done efficiently in the following way -

Let $e = 10011011100001$

Then e can be represented as $\sum_{i=0}^{13} 2^i e_i$

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

Then $m^e = m$

This can be rewritten as $\prod_{i=0}^{13} ((m)^{2^i})^{e_i}$

This implies $O(\log e)$ multiplies for values of i from 0 to 13

Recursive Program: `mod_exp(m, e, N)`

if $e == 0$, return 1

$a = \text{mod_exp}(m, \lfloor e/2 \rfloor, N)$ /* floor function applied to $e/2$ */

$a = a^2 * m^{e_0} \bmod N$

return a

Miller Rabin Primality Test

Observations: $(N-1)^2 \equiv 1 \pmod N$.

$N^2 - 2N + 1 = 1 \pmod N$. In other words, $N-1 \equiv -1 \pmod N$.

Fact: If N is a prime number, then the only X such that $X^2 = 1 \pmod N$ is $X \equiv \pm 1 \pmod N$.

If N is not prime, then there are at least 4 such numbers that square to 1 mod N

We shall make use of Chinese Remainder Theorem to prove the above fact.

Chinese Remainder Theorem

If $N = pq$ where $\gcd(p, q) = 1$, then

$$\mathbb{Z}/N\mathbb{Z} \approx \mathbb{Z}/p\mathbb{Z} * \mathbb{Z}/q\mathbb{Z}$$

$x \mapsto (x \bmod p, x \bmod q)$. The two rings are said to be isomorphic.

$(tqa + sbp) \bmod N \leftarrow (a, b)$ where **$sp + tq = 1$**

$(a, b) \mapsto (tqa + sbp) \bmod N$

$\mapsto (tqa \bmod p, sbp \bmod q)$

$\mapsto (a \bmod p, b \bmod q)$

If p and q are prime, then $(\pm 1)^2 \equiv 1 \pmod p$ and $(\pm 1)^2 \equiv 1 \pmod q$ to get $1 \pmod N$.

$(1 \bmod p, 1 \bmod q) \mapsto tq + sp \equiv 1 \pmod N$

$(-1 \bmod p, -1 \bmod q) \mapsto -tq - sp \equiv -1 \pmod N$

$(1 \bmod p, -1 \bmod q) \mapsto tq - sp$

$(-1 \bmod p, 1 \bmod q) \mapsto -tq + sp$