

# Network Security - CSE 508 - Fall 09

Faculty - Rob Johnson

Friday October 16, 2009

## 1 Number Theory - Contd.

### 1.1 Theorem

- Given  $\gcd(a, b) = X$ , where  $X$  is the smallest positive linear combination of  $a, b$ , i.e.  $X = sa + tb$ , and  $X \leq \gcd(a, b)$
- Also given,  $X|a$  and  $X|b$ , and  $\exists q$  and  $0 \leq r < X$
- Prove that  $a = qx + r$
- Proof
  - $\Rightarrow a = qx + r$
  - $\Rightarrow a = q(sa + tb) + r$
  - $\Rightarrow r = (1 - qs)a - qtb$
- Thus  $r$  is the linear combination of  $a$  and  $b$ , and  $r < X$ . Since  $X$  is the smallest linear combination of  $a, b$ ,  $r$  must be positive. Hence  $r = 0$ . So  $X|a$ , similarly,  $X|b$ . Hence  $X \leq \gcd(a, b)$

### 1.2 Extended Euclidean Algorithm

- Let us take the example of applying the above algorithm on 33,24
- The most basic linear combinations of 33, 24 are  $1*33+0*24 = 33$  and  $0*33+1*24 = 24$
- This can be represented as  $A = [1 \ 0 \ 33]$  and  $B = [0 \ 1 \ 24]$
- We subtract the second vector from the first  $A(3) \text{ modulo } B(3)$  times.
- Repeating the above step, we get a series of vectors as follows:

$$\begin{aligned} & [1 \ 0 \ 33] \\ & -1 [0 \ 1 \ 24] \\ & -2 [1 \ -1 \ 9] \\ & -1 [-2 \ 3 \ 6] \end{aligned}$$

$$-2 [3 \ -4 \ 3]$$

$$[-8 \ 11 \ 0]$$

- Thus  $[3 \ -4 \ 3]$  is the solution to the linear combination equation.

## 2 Application of Extended Euclidean Algorithm

- One of the steps in RSA tells us to pick two nos,  $e$  and  $d$  such that

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

- Solution: Pick  $e$  randomly such that  $\gcd(e, (p-1)(q-1)) = 1$

Use Extended Euclidean Algorithm to find  $s, t$  such that  $se + (p-1)(q-1)t = 1$

Since  $e, (p-1)(q-1)$  are relatively prime  $s, t$  exists. Hence,

$$\Rightarrow se + t(p-1)(q-1) = 1$$

$$\Rightarrow se - 1 = -t(p-1)(q-1)$$

$$se \equiv 1 \pmod{(p-1)(q-1)}$$

- So we can conclude the second no.  $d$  as  $s$ .

### 2.1 Modular Inverses

- Given  $a, m$  when does there exist  $b$  such that  $ab \equiv 1 \pmod{m}$  and how can we find it.
- Theorem:  $b$  exists  $\Leftrightarrow \gcd(a, m) = 1$ . We use Extended Euclidean algorithm to find it.

### 2.2 Modular Exponentiation

- $c = m^e \pmod{N}$ , where  $e = 10011011100001$  such that the MSB is  $e_{13}$  and LSB is  $e_0$

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

$$\text{Therefore } c = m^{\sum_{i=0}^{13} 2^i e_i}$$

$$\text{Which is equal to } \prod_{i=0}^{13} (m^{2^i})^{e_i}$$

For instance,  $m^{2^0} = m$

and,  $m^{2^1} = m^2$

Hence,  $m^{2^i} = (m^{2^{i-1}})^2$

This takes  $O(\log e)$  multiplications.

### 3 Miller Rabin Primality test

- Observation:  $(N - 1)^2 \equiv 1 \pmod{N}$  as  $(N - 1)^2$  expands to  $N^2 - 2N + 1$
- Fact: If  $N$  is prime, then the only  $X$  such that  $X^2 \equiv \pm 1 \pmod{N}$  is  $X \equiv \pm 1 \pmod{N}$   
If  $N$  is not prime, then there are at least 4 values that square to  $1 \pmod{N}$ .

#### 3.1 Chinese Remainder Theorem

- To prove the above we use the Chinese Remainder Theorem
  - If  $N = pq$  where  $\gcd(p, q) = 1$ , then  $Z/NZ \simeq Z/pZ * Z/qZ$
  - This is an example of Isomorphic pairs which are readily interchangeable.
  - In one direction,  $Z \mapsto (X \pmod{p}, X \pmod{q})$
  - In the other direction,  $(a, b) \mapsto (tqa + spb) \pmod{N}$  where  $sp + tq = 1$
- Using the Chinese Remainder Theorem above, we have
    - $(\pm 1)^2 \equiv 1 \pmod{p}$
    - $(\pm 1)^2 \equiv 1 \pmod{q}$
    - $(1 \pmod{p}, 1 \pmod{q}) \mapsto tq + sp$  and hence is  $\equiv 1 \pmod{N}$
    - $(-1 \pmod{p}, -1 \pmod{q}) \mapsto -tq - sp$  and hence is  $\equiv -1 \pmod{N}$
- Similarly,
- $(1 \pmod{p}, -1 \pmod{q}) \mapsto (tq - sp) \pmod{N}$
  - $(-1 \pmod{p}, 1 \pmod{q}) \mapsto (-tq + sp) \pmod{N}$