Lecture 16
Feb. 11-th, 2015

Pubic Key cryptosystem.
Take underlying the encoding scheme is very simple. It is easy to multiply large number together but it is hard to factor a large number.

How secure is the encoding scheme?
We know m and k, where $m = p\cdot q$, p, q are primes.

The only way to decode is to find
$$\phi(m) = (p-1)(q-1) = pq + 1 - (p+q) = m + 1 - (p+q)$$
We have to find $p+q$
p, q are solution to $x^2 - (p+q)x + pq = 0$.

Chapter 20
$ax \equiv b \bmod m$
We look at quadratic congruence $x^2 \equiv a \bmod p$
① Does $x^2 \equiv 3 \bmod 7$ have a solution?
② Does $x^2 \equiv -1 \bmod 13$ have a solution?
③ For which prime p does $x^2 \equiv 2 \bmod p$ have a solution?

③ is called quadratic reciprocity law.

Each number (other than zero) that appears as square appears exactly twice.
Why? $b^2 \equiv (p-b)^2 \bmod p$.
So we only need to compute $1^2, 2^2, \ldots, (\frac{p-1}{2})^2 \bmod p$ to get all the numbers that are square mod p

Def: A non-zero number that is congruent to a square mod p is called a quadratic residual mod p (QR)

Def: A non-zero number that is not congruent to a square mod p is called a quadratic nonresidual mod p. (NR)

QR mod is $\{1, 2, 4, 9, 10, 12\}$
NR mod is $\{2, 5, 6, 7, 8, 11\}$

Observation: p odd prime.
There are exactly $\frac{p-1}{2}$ QRs and $\frac{p-1}{2}$ NRs.

Proof: Check $1^2, 2^2, \ldots, (\frac{p-1}{2})^2 \bmod p$ are all distinct.
Suppose $b_1^2 \equiv b_2^2$, $1 \le b_1 \le b_2 \le \frac{p-1}{2}$

$p \mid b_2^2 - b_1^2 \Rightarrow b_2^2 - b_1^2 = (b_2 + b_1)(b_2 - b_1)$
$2 \le b_2 + b_1 < p \Rightarrow p \nmid b_2 + b_1 \Rightarrow p \mid (b_2 - b_1) \Rightarrow b_2 - b_1 = 0$

Quadratic Residue Multiplication Rule (p odd prime)
1. $QR \times QR = QR$
2. $NR \times NR = NR$
3. $QR \times NR = NR$

Proof:

1. $a_1, a_2 \in QR$, $a_1 \equiv b_1^2$, $a_2 \equiv b_2^2 \Rightarrow a_1a_2 \equiv b_1^2 b_2^2 \equiv (b_1b_2)^2 \mod p$.

2. $a_1 \equiv b_1^2 \mod p$, a_2 NR

Suppose a_1a_2 is QR.

$b_1^2 a_2 \equiv a_1 a_2 \equiv b_3^2$

$b_1 \not\equiv 0 \mod p$, $p \nmid b$.

$\Rightarrow \exists\ c_1 \not\equiv 0$ s.t. $c_1 b_1 \equiv 1$

$\Rightarrow c_1^2 b_1^2 a_2 \equiv c_1^2 b_3^2 \equiv a_2$

$\Rightarrow a_2$ is QR $\Rightarrow$ contradiction.

3. Let a be a NR and consider $\{a, 2a, 3a, \dots, (p-1)a \mod p\}$.

As a set, it is the same as $\{1, 2, 3, \dots, (p-1)\}$.

therefore, it contains $\frac{p-1}{2}$ QRs & $\frac{p-1}{2}$ NRs.

But we proved $a \times QR = NR$, then we have $\frac{p-1}{2}$ NRs.

So $a \times NR$ should be QR.

QR behaves like $+1$

NR behaves like -1.

Legendre Symbol

$$\left.\begin{aligned} \left(\frac{a}{p}\right) &= 1 \text{ if } a \text{ is QR.} \\ \left(\frac{a}{p}\right) &= -1 \text{ if } a \text{ is NR.} \end{aligned}\right\} \Longrightarrow \begin{aligned} \left(\frac{a}{p}\right) &= 1 \text{ if } x^2 \equiv a \mod p \text{ has sol'ns} \\ \left(\frac{a}{p}\right) &= -1 \text{ if } x^2 \equiv a \mod p \text{ has no sol'ns.} \end{aligned}$$

Quadratic Residue Multiplication Rule.

p odd prime.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{q}\right)$$

e.g. Is 75 a square mod 97?

$$\left(\frac{75}{97}\right) = \left(\frac{3 \times 5^2}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5}{97}\right)^2 = \left(\frac{3}{97}\right)$$

Solve $x^2 \equiv 3 \mod 97$

$s \equiv 10^2 \mod 97$.