Lecture 15
Feb 9th, 2015

Chapter 17

$$x^k \equiv b \bmod m$$

$$\gcd(k, \phi(m)) = 1, \gcd(b, m) = 1$$

In this case, we can compute the solution early.

Step 1. Compute $\phi(m)$

Step 2. Find u, v (positive integers such that $k \cdot u - \phi(m) \cdot v = 1$

Step 3. Compute $b^u \bmod m$ by successive squaring $x \equiv b^u \bmod m$ is the solution.

$$x^k \equiv (b^u)^k = b^{uk} = b^{1+\phi(m)v} \equiv b(b^{\phi(m)})^v \equiv b \bmod m$$

since $b^{\phi(m)} \equiv 1 \bmod m$

Step 2 & Step 3 have easy algorithms
Step 1 is difficult.

This is the heart of constructing S___ codes.

e.g. $x^{329} \equiv 452 \bmod 1147$

$1147 = 31 \times 37$

$\phi(1147) = 30 \times 36 = 1080$

$\gcd(329, 1080) = 1$

Solve $329u - 1080v = 1$, $u = 929$

Compare $452^{929} \bmod 1147$

$929 = 2^9 + 2^8 + 2^7 + 2^5 + 1$

$452^{2^5} \equiv 417$

$452^{2^7} \equiv 565$

$452^{2^8} \equiv (629)^2 \equiv 359$

$452^{929} \equiv 452^{2^9} \times 452^{2^8} \times 452^{2^7} \times 452^{2^5} \times 452$

The solution is $x \equiv 763 \bmod 1147$

Our method does not work if any of the conditions:

- $\gcd(k, \phi(m)) = 1$
- $\gcd(b, m) = 1$

either is not satisfied

e.g. $x^5 \equiv 6 \bmod 9$

$9 = 3^2$, $\phi(9) = 6$

$\gcd(5, 6) = 1$, $1 = 6 - 5$

$u = 5$, but $x \equiv 6^5$ is not a solution.

Chapter 18.

First step: Convert a message into a string of numbers

Set A=11, B=12, ... Z=36

"To be or not to be"

TOBEORNOTTOBE

30 25 12 15 25 28 24 25 30 30 25 12 15

Second : choose two large prime p, q and we get $m=p \cdot q$, $\phi(m)=(p-1)(q-1)$

choose k such that $\gcd(k, \phi(m))=1$, we publish m, k but keep p, q secret.

Third : we break the message into a string of digits that are less than m.
e.g. if m is about 10^6, we would write the message as a list of six digit number.

So now the message is a list of number $a_1, a_2, \cdots, a_r$.

Forth : use successive squaring to compute $a^k \bmod m$, $\cdots$, $a_r^k \bmod m$. Then form a new list of numbers $b_1, \cdots, b_r$ encoded message.

e.g. $p=12553$, $q=13007$

$m=p \cdot q=163276871$

$\phi(m)=163276871$

choose $k=79921$

Since m is 9 digits long, we break the message into 8 digits numbers:

30251215, 25282425, 30302512, 15

Compare k^{th} power mod m

$30251215^k \equiv 149419241$

$25282425^k \equiv 62721998$

$30302512^k \equiv 118084566$

$15^{79921} \equiv 40481382$

So the encoded message is:

149419241, 62721998, 118084566, 40481382

In order to decode, we need to solve:

$x_1^k \equiv b_1 \bmod m$

$x_2^k \equiv b_2 \bmod m$

$\cdots$

$x_r^k \equiv b_r \bmod m$

Since we know $\phi(m)$ we can solve and recover the original message.