

19.791

Midterm 1 on Friday

Today: RSA cryptography

Alice \xrightarrow{M} Bob $M = \text{"super secret message number"}$

- euclidian algorithm is fast
- factorization of large #'s is computationally impossible.
(or rather, computing $\phi(m)$ is hard)

Lemma: $m > 0, (a, m) = 1$. Then if k and \bar{k} are such that $k\bar{k} \equiv 1 \pmod{\phi(m)}$ then $a^{k\bar{k}} \equiv 1 \pmod{m}$.

Proof: $k\bar{k} \equiv 1 \pmod{\phi(m)} \Rightarrow k\bar{k} = 1 + r \cdot \phi(m)$
 $a^{k\bar{k}} = a^{(1+r\phi(m))} = a \cdot 1 \pmod{m} \equiv a \pmod{m}$.

Cor $m > 0, (k, \phi(m)) = 1$

Then if $\{r_1, \dots, r_{\phi(m)}\}$ is reduced residue system, then the set $\{r_1^k, \dots, r_{\phi(m)}^k\}$ is also reduced res. syst.

Pf: To check: $(r_i^k, m) = 1$ and $r_i^k \equiv r_j^k \pmod{m}$ for $i \neq j$.

• $(r_i^k, m) = 1$ follows from $(r_i, m) = 1$.

• Say $r_i^k \equiv r_j^k \pmod{m}$. choose \bar{k} s.t. $k\bar{k} \equiv 1 \pmod{\phi(m)}$. ($\exists \bar{k}$ b/c $(k, \phi(m)) = 1$)
so $r_i \equiv r_i^{k\bar{k}} \equiv r_j^{k\bar{k}} \equiv r_j \pmod{m} \Rightarrow i = j$ by def. reduced res. syst.

Idea: raising to the k^{th} power gives a permutation of $\{r_1, \dots, r_{\phi(m)}\}$

To get inverse permutation, need to compute \bar{k} (and raise to \bar{k} power).

For that, need Euclidean algorithm + $\phi(m)$.

A \xrightarrow{M} B

1. B chooses 2 big primes p_1, p_2 and computes $m = p_1 \cdot p_2, \phi(m) = (p_1 - 1)(p_2 - 1)$.
Also chooses big k in $0 < k < \phi(m)$ with $(k, \phi(m)) = 1$. Choose p_1, p_2 s.t. $0 < M < p_1, p_2$
2. B gives $k + m$ to A. Then A computes $M^k \pmod{m}$ and sends to B
3. B computes \bar{k} , and then $M \equiv (M^k)^{\bar{k}} \pmod{m}$

Compute $M^k \pmod{m}$.

Ex: $999^{179} \pmod{1763}$

$$179 = 1 + 2 + 2^2 + 2^5 + 2^7$$

$$999 (999)^2 (999^2)^2 (999^{2^2})^2 (999^{2^5})^2 \pmod{m}$$

$$999 \equiv 999 \pmod{1763} \quad 999^{2^5} \equiv 918$$

$$999^2 \equiv 143 \quad 999^{2^6} \equiv 10$$

$$999^{2^7} \equiv 143^2 \equiv 1056 \quad 999^{2^8} \equiv 100$$

$$999^{2^9} \equiv (1056)^2 \equiv 920$$

$$999^{179} \equiv 920^2 \equiv 160$$

$$999^{179} \equiv 999 \cdot 143 \cdot 160 \cdot 918 \cdot 100 \equiv 1219 \pmod{1763}$$

Test if m is composite:

If m is prime, then for any a , $0 < a < m$, $a^{m-1} \equiv 1 \pmod{m}$

Ex: $2^{1762} \equiv 742 \pmod{1763}$ so 1763 not prime.

Remark: It can happen that $a^{m-1} \equiv 1 \pmod{m}$ even if m not prime.

Ex: $2^{1386} \equiv 1 \pmod{1387}$.

For prime p , $x^2 \equiv 1 \pmod{p}$, $x \equiv \pm 1 \pmod{p}$.

$2^{693} \equiv 512 \pmod{1387}$, so 1387 not prime.