Lec 9

Fermat's Little Theorem

p be a prime

$$x_{p-1} \equiv 1(mod\ p)$$

用后边的p来拆分前边的指数

proof :

proof. we consider two sets $A = \{1, 2, \cdots, p-1\}$ $gcd(x, p) = 1$

$B = \{x, 2x, \cdots, (p-1)x \bmod p\}$

① If we can prove that $A = B$, then
we multiply all the elements together for each set, then the products should be the same.

$$\cancel{1 \cdot 2 \cdots (p-1)} \equiv x \cdot 2x \cdots (p-1)x \pmod p$$
$$\equiv x^{p-1} \cancel{1 \cdot 2 \cdots (p-1)} \pmod p$$

· note that all these numbers $1, 2, \cdots (p-1)$ are relatively prime to p.
So we can divide both sides by $1, 2, \cdots (p-1)$ $x^{p-1} \equiv 1 \pmod p$

② it remains to prove $A = B$ Clearly, $0 \notin B$
Any two elements of B are different. $ix \equiv jx \bmod p$ $1 \le i, j \le p-1$

$p \mid (i-j)x$ $gcd(x, p) = 1$ $p \mid i-j$ $i-j=0$ $i=j$.

Euler's Theorem

Euler's totient function

RSA

pick two large primes, p q

n=pq

$\phi(n) = (p-1)(q-1)$ by Euler's low

e : Encryption Key   **(e,n)**

d : Decryption Key   **(d)**

$gcd(e, \phi(n)) = 1$
$ed \equiv 1(mod\phi(n))$

> **given e and $\phi(n)$ how to find d?**
>
> This is equivalent to finding the modular inverse of modulo $\phi(n)$.
>
> Extended Euclidean algorithm

$C = M^e mod\ n(RSA\ encryption)$
$M = C^d mod\ n(RSA\ decryption)$

Theorem(Correctness)

Theorem (*Correctness*) : Let p and q be two odd primes, and define $n = pq$. Let e be relatively prime to $\phi(n)$ and let d be the multiplicative inverse of e modulo $\phi(n)$. For each integer x such that $0 \leq x < n$,

$x^{ed} \equiv x(mod\ n)$

Proof :

$x^{ed} \equiv x \pmod n$

① $\gcd(x,n)=1$ use Euler's theorem $x^{\phi(n)} \equiv 1 \bmod n$

$ed \equiv 1 \bmod \phi(n)$ $ed = k\phi(n)+1$ $x^{ed} \equiv x^{k\phi(n)+1} \equiv (x^{\phi(n)})^k \cdot x \equiv x \bmod n$

② $\gcd(x,n)=p$ w.l.o.g. assume that $x=tp$ $\gcd(x,q)=1$ $x^{q-1} \equiv 1 \bmod q$

$n \mid x^{ed} - x = \underbrace{x}_{p}\underbrace{(x^{ed-1}-1)}_{q}$ $x^{ed-1} \equiv x^{k(p-1)(q-1)} \equiv (x^{q-1})^{k(p-1)} \equiv 1 \bmod q$

$x^{ed} \equiv x \pmod n$

③ $\gcd(x,n)=q$ similar to ②

④ $\gcd(x,n)=n$ trivial $x=0$

Digital Signature

$S = M^d\ mod\ n(RSA\ signature)$
$M = S^e\ mod\ n(RSA\ verification)$

Two main applications of public-key crypto

① digital signature

② encryption But public-key crypto is usually NOT efficient

encrypt ~~the~~ secret key of symmetric crypto

efficient

Discrete Logarithm