数论

Notation

- what is group => 有限或无限个元素或操作的集合

  Let G be a non-empty set, if satisfied: (1) there is a closed algebraic operation; (2) a combination law; (3) a unit cell; (4) a reverse edge, then G is a group

- p => primer 一个素数
- Z_N => 一个基于N的群 (N是一个正整数)
- Z_N^* => 在基于N的群中, 所有和N互素的元素的集合
- gcd => greatest common divider gcd(x, y) x, y的最大公约数
- generator g => 如果 g属于 Z_p^*, **且 {1, g, g^2 , ... , g^{p-2}} = Z_p^*** , 那么g就是一个生成元 , 这个集合中并不是所有与纳素都是生成元 , 也不是只有一个生成元
- ord(g) && <g> => 生成元的阶 描述的是取得最小的 a 使得 g^a = 1 IN p e.g. $Ord_7(2) = 3$
- **一个群的order 就是这个中 Z_N^* 的元素的个数 , 如果 N is a primer then order = N-1**

取模 MOD

- 9 + 8 = 5 in Z_{12}
- 2 - 4 = 10 in Z_{12}

gcd

- 最大公约数 gcd(x, y) => 一定存在整数a, b使得 ax + by = gcd(x, y)
- 如果gcd(x, y) = 1 则称x, y为互素 relatively prime
- x在群Z_N中一个元素有逆元(inversable)说明 => 存在 xy = 1 in N (y为x的逆元) 记为 $x = y^{-1}$
- **定理** 如果 gcd(x, N) = 1 那么x在N中必定存在逆元

Fermat's theorem

如果p是一个素数, 那么所有的 x 属于 Z_p^* 都存在 x^{P-1} = 1 , **但是p-1并不是唯一的数 使得这个等式成立**

说明 x * x^{p-2} = 1 因此 x^{p-2} 便是x的一个逆元

- 利用Fermat's theorem生成一个大素数(1024 bits) :
  - 随机选择一个数 p 属于 [2^{1024},$2^{1025} - 1$]
  - 验证 2^{P-1}= 1 ? 如果是 , 则输入p 为所求的素数

Euler’s generalization of Fermat

def : 定一个N 有 ϕ(N) 是Z $_N^*$ 元素的个数 e.g. ϕ(12) = 4

- ϕ(p) = p-1 (p is a primer)

对于x属于Z $_N^*$, 有x$^{\phi(N)}$ In N = 1 ,实际上这个定理算是Fermat’s theorem的一个扩展, 因为Fermat’s theorem说的只是N为素数的情况

群Z下的幂乘问题

- 一次线性的情况下 : ax + b = 0 => ax = -b => x = (-b) * a^{-1},注意 : a^{-1}为a在Z下的逆元
- 高次情况下 : 求 x^e = c 就是求在群Z下, 存在哪些元素使得 x^e = c
- e = 2 的情况 (quadratic residue)
  - 在一个素数群p下 : 求 x^2 IN Z , 又基本的数学知识知道 : x^2 = (-x)^2 所以说在二次的情况下 x , -x In Z 应该有相同的平方值. e.g : Z$_{11}$ 1^2=10^2 , 2^2 = 9^2 ...
  - quadratic residue Q.R. 就是这些值的平方的结果集合 , e.g. Q.R. in Z$_{11}$ is 1, 4, 9, 5, 3
  - THM : #Q.R. = (p-1) /2 如 (11-1) / 2
- Euler's theorem : if x in Z $_N^*$ is a Q.R. then x$^{\#Q.R.}$ = 1

基于素数的困难问题

1. 离散对数问题(DLOG)

已知 a, g 在 Z $_N^*$ 很好求出g^a 但是已知 g^a 和 g, 求出a确没有很好的办法

2. factoring problem

给出一个素数N = p*q , 很难去根据N 分解出p 和 q .

3. ECDLP

椭圆曲线