第1.5节 密码学

Section 1.5: Cryptography

知识要点

1. 欧拉函数及欧拉定理
2. 古典密码学
3. 密码学
4. 公钥密码学
5. RSA密码系统
6. 密码协议
7. 同态加密(自学)

1.5.1 欧拉函数

- 【定义】：**欧拉函数**$\Phi(n)$表示在1到n之间的能满足$gcd(k,n) = 1$的那些数的总个数.
- 备注：包括1和n
- 例:求解Φ(12), Φ(1)
- 解:
  - 因为在1，2，3，…，12这些数中有1，5，7，11这4个数都和12是互素的，所以Φ(12)=4;
  - 因为gcd(1, 1) = 1, 所以Φ(1) = 1.

1.5.1 欧拉函数

- 当n比较大时, 欧拉函数值很难计算，但如果n是素数呢?
- 欧拉函数的性质：对于任意素数n，$\Phi(n)=n-1$；当n是合数时，$\Phi(n)<n-1$.
- 备注: 因为当k=1, 2, ..., $n-1$时都存在$\gcd(k,n)=1$, 所以一共有$n-1$个, $\Phi(n)=n-1$. 例如$\Phi(5)$ =4, 因为5是素数.