Introducton

- 数学基础
- 古典密码
- 散列算法（单向 加密函数不存在反函数）常用于比较Hash值是否相等来校验文件完整性
  - MD5(128位) MD5校验
  - SHA-1
- RC4 流加密算法 快捷的适用于视频流加密算法
- DES(Data Encryption Standard)
- AES(Advanced Encryption Standard)：加密密钥不等于解密密钥
  - RSA key1 $\nRightarrow$ key2
  - ECC（椭圆曲线算法）

> 勒索病毒：AES的256位随机密钥设为k,用k加密硬盘上的文档
> $k^{'} = RSA(k, key1)$;用key1加密k，算出k'发送给黑客
> $k = RSA(k^{'}, key2)$;黑客用key2解密k'得到k

第1章 数学基础

整除

a整除b:

$$b = a \times k \Leftrightarrow a \mid b$$

- 对于任意整数a,都有$1 \mid a; a \neq 0 \Rightarrow a \mid 0, a \mid a$
- $a \mid b \wedge b \mid c \Rightarrow a \mid c$
- $a \mid b \wedge a \mid c \Rightarrow a \mid (s \times b + t \times c), s, t \in Z$

素数与互素

- 素数
  若整数p只有因子± 1及$\pm p$,则称p为素数
- 互素(relatively prime)
  对于整数a,b,若$gcd(a, b) = 1$,则称a、b互素

> 任一整数a（a>0）都能唯一分解成以下形式:
>
> $$a = p_1 \times p_2 \times p_3 \times \cdots \times p_t$$
>
> 其中$p_1, p_2, p_3, ..., p_t$是素数

最大公约数(greatest common divisor)

$$a, b \in Z, a, b\text{不同时为}0，\ d = gcd(a, b)$$

$$a \times x + b \times y = d \quad (x, y \in Z)$$

特别的，当a，b互素时，则一定存在整数x, y使得$d = 1, a \times x + b \times y = 1$

同余(congruent)

模运算

- 加法逆元

$$a + b \equiv 0 \pmod{n}$$

- 乘法逆元

$$a \times b \equiv 1 \pmod{n}$$

> 设n是一个正整数，$Z_n = 0, 1, 2, \cdots, n-1$,对于$u \in Z_n$，存在$v \in Z_n$，使得 $uv \equiv 1 \pmod{n}$的充分必要条件是$gcd(u, n) = 1$

- 扩展欧几里得法（extended Euclidean algorithm）

在mod运算中，设a是正整数，则计算过程中的-a必须转化成a的加法逆元，1/a必须转化成a的乘法逆元