

# NIS2312-1 2022-2023 Fall

## 信息安全的数学基础 (1)

### Assignment 2

2022 年 9 月 20 日

---

#### Problem 1

RSA 公钥密码方案:

(1) 密钥生成:

随机选取两个大素数  $p, q$ , 计算  $n = pq, \varphi(n) = (p-1)(q-1)$ ; 任意选取一个大整数  $e$  满足  $1 \leq e \leq \varphi(n)$  且满足  $(e, \varphi(n)) = 1$ ; 计算  $d$ , 满足  $de \equiv 1 \pmod{\varphi(n)}$ . 以  $\{e, n\}$  为公钥,  $\{d, n\}$  为私钥.

(2) 加密运算:

对明文  $m < n$  进行加密:  $c = E(m) \equiv m^e \pmod{n}$ .

(3) 解密运算:

接收方对  $c$  进行解密:  $m = D(c) \equiv c^d \pmod{n}$ .

那么:

(1) 试证明解密运算的正确性;

(2) 取素数  $p = 3, q = 11$ , 则  $n = 33, \varphi(n) = 20$ . 取  $e = 7$ . 尝试计算密文  $c = 29$  对应的明文.

#### Problem 2

Rabin 数字签名方案:

随机选取两个大素数  $p, q$  且  $p \equiv q \equiv 3 \pmod{4}$ , 令  $n = pq$ . 以  $\{n\}$  为公钥,  $\{p, q\}$  为私钥. 加密运算是将明文  $m$  加密为  $c \equiv m^2 \pmod{n}$ . 那么:

(1) 尝试设计一种 Rabin 密码算法的解密运算;

(2) 证明你所设计的解密运算的正确性;

(3) 取素数  $p = 7, q = 11$ , 则  $n = 77$ , 对明文  $m = 20$  进行加密得到  $c \equiv m^2 \pmod{n} = 15$ , 尝试计算密文  $c = 15$  对应的明文.

### Problem 3

本原根: 当  $a$  是满足  $(a, n) = 1$  且  $a^{\varphi(n)} \equiv 1 \pmod{n}$  的最小正整数时, 称  $a$  是  $n$  的本原根.

ElGamal 公钥密码方案:

(1) 密钥生成:

随机选择一个大素数  $p$ , 且要求  $p-1$  有大素数因子. 再选择一个模  $p$  的本原元  $g$ . 随机取整数  $x$  满足  $2 \leq x \leq p-2$  作为私钥, 计算出  $h \equiv g^x \pmod{p}$ , 则公钥为  $\{p, g, h\}$ .

(2) 加密运算:

随机选取  $1 \leq y \leq p-2$ , 然后计算  $s \equiv h^y \pmod{p}$ , 计算  $c_1 \equiv g^y \pmod{p}$ , 同时明文  $m < p$  进行加密计算得到  $c_2 \equiv m \cdot s \pmod{p}$ , 发送的密文为  $(c_1, c_2)$ .

(3) 解密运算:

接收方接收到密文  $(c_1, c_2)$  后, 计算  $s \equiv c_1^x \pmod{p}$ , 然后计算出  $s^{-1} \pmod{p}$  的值, 其中  $s \cdot s^{-1} \equiv 1 \pmod{p}$ , 则明文  $m \equiv c_2 \cdot s^{-1} \pmod{p}$ ;

那么:

(1) 证明上述解密运算的正确性.

(2) 当  $p = 2539$ ,  $g = 2$ ,  $x = 51$ ,  $y = 15$  时, 给出明文  $m = 804$  对应的密文  $(c_1, c_2)$  和  $(c_1 = 2300, c_2 = 224)$  对应的明文  $m$ .