第九章作业

1633734 朱志儒

思考题

9.1 公钥密码体制的主要成分：明文、加密算法、公钥和私钥、密文、解密算法。

9.2 用户保密私钥，公钥可供其他人使用。私钥可用来加密消息得到数字签名，公钥可以用于加密消息，其只能由私钥的拥有者解密。

9.3 公钥密码体制的三种应用：加密/解密、数字签名、密钥交换

9.4 公钥密码体制应该满足的要求：

（1）产生一对密钥在计算上是容易的；

（2）已知公钥和要加密的信息，发送方产生相应的密文在计算上是容易的；

（3）接受方使用其私钥对接受的密文解密以恢复明文在计算上是容易的；

（4）已知公钥时，攻击者要确定私钥在计算上是不可行的；

（5）已知公钥和密文时，攻击者要恢复明文在计算上是不可行的；

（6）加密和解密函数的顺序可以交换。

9.5 单向函数：每个函数值都存在唯一的逆，并且计算函数值是容易的，但求逆却是不可行的。

9.6 单向陷门函数是满足下列条件的一类不可逆函数：

（1）若 k 和 X 已知，则容易计算$\mathrm{Y} = \mathrm{f_k}(X)$；

（2）若 k 和 Y 已知，则容易计算$X = f_k^{-1}(Y)$；

（3）若 Y 已知但 k 未知，则计算出$X = f_k^{-1}(Y)$是不可行的。

习题

9.2

a. $n = 33; \varphi(n) = 20; d = 3; C = 26.$

b. $n = 55; \varphi(n) = 40; d = 27; C = 14.$

c. $n = 77; \varphi(n) = 60; d = 53; C = 57.$

d. $n = 143; \varphi(n) = 120; d = 11; C = 106.$

e. $n = 527; \varphi(n) = 480; d = 343; C = 128$

9.3 由题可得：明文 $M = 5$

9.4 使用试探法可以得到 $p = 59, q = 61$，所以 $\varphi(n) = pq = 3480$，则 31 模 3480 的乘法逆元为 3031，故该用户的私钥是（3031，3599）。

9.6 有帮助，如果明文有 n 模 n 的公因子，那么密文也有 n 模 n 的公因子，加密一个小于 pq 的分组，因子必须是 p 或 q，且明文必须是 q 或 p 的倍数。我们可以测试每个分组的素数，如果是素数，则为 p 或 q。在这种情况下，我们分成 n 来找到另一个因子。如果不是素数，我们将其考虑在内并尝试将因子作为 n 的除数。

9.7 不，这不安全。一旦 Bob 泄露了他的私钥，Alice 就可以使用它来计算 Bob 的模数 N。然后，Alice 可以破解 Bob 发送的任何消息。

9.8 考虑一组字母字符{A，B，…，Z}。表示字母表中每个字母位置的相应整数形成一组消息块值 SM＝{0,1,2，…，25}。该组对应的密文块值 SC＝{0^e mod N，1^e mod N，…，25^e mod N}，并且可以由具有 Bob 的公钥的每个人计算。因此，针

对该问题中描述的方案最有效攻击是针对 M 的所有可能值计算 $M^e \bmod N$，然后创建以密文作为索引的查找表，其中相应的明文作为适当的值。

9.9

（a）$n = 233$

$233 - 1 = 2^3 \times 29$, k=3, q=29

$a^q \bmod n = 2^{29} \bmod 233 = 1$

可能是素数

$n = 235$

$235 - 1 = 2^1 \times 117$, k=1, q=117

$a^q \bmod n = 2^{117} \bmod 235 = 222$

$222 \neq 1$ 且 $222 \neq 235 - 1$

合数

$n = 237$

$237 - 1 = 2^2 \times 59$, k=2, q=59

$a^q \bmod n = 2^{59} \bmod 237 = 167 \neq 1$

$167 \neq 237 - 1$

$167^2 \bmod 237 = 160 \neq 237 - 1$

合数

$n = 239$

$239 - 1 = 2^1 \times 119.$

$2^{119} \bmod 239 = 1$

可能是素数

$n = 241$

$241 - 1 = 2^4 \times 15$

$2^4 \bmod 241 = 16$

$16 \neq 1$ 且 $16 \neq 241 - 1$

$16^2 \bmod 241 = 256 \bmod 241 = 15$

$15 \neq 241 - 1$

$15^2 \bmod 241 = 225 \bmod 241 = 225$

$225 \neq 241 - 1$

$225^2 \bmod 241 = 15$

$15 \neq 241 - 1$

可能是素数

（b）M=2, e=23, n=233 × 241=56153 则 p=233， q=241， $e = 23 = (10111)_2$

I		4	3	2	1	0
ei		1	0	1	1	1
D	1	2	4	32	2048	**21,811**

（c）因为 n=233 × 241=56153, p=233, q=241，则$\phi(n) = (p-1)(q-1) = 55680$,

由扩展欧几里得算法可得 $d = 23^{-1} \bmod 55680 = 19367$

（d）不使用中国剩余定理：$M = 21{,}811^{19{,}367} \bmod 56{,}153 = 2$

使用中国剩余定理：

$d_p = d \bmod (p-1)$ $\quad$ $d_q = d \bmod (q\text{-}1)$

$d_p = 19367 \bmod 232 = 111\, d_q = 19367 \bmod 240 = 167$

$C_p = C \bmod p$

$M_p = C_p{}^{d_p} \bmod p = 141^{111} \bmod 233 =2$

$C_q = C \bmod q$

$M_q = C_q{}^{d_q} \bmod q$

$M_q = 121^{167} \bmod 241 = 2$

$M = 2.$

9.10 第 3 个元素，因为它等于第一个的平方；

第 5 个元素，因为它等于第 1 个和第 5 个的乘积；

第 7 个元素，因为它等于第一个的立方。

9.15 攻击者 X 拦截 A 发送给 B 的消息，例如$(A, E(PU_b, M), B)$；

X 将$(X, E(PU_b, M), B)$发送给 B；

B 通过发送$(B, E(PU_X, M), X)$给 X 以确认收到；

X 使用他的密钥解密$E(PU_X, M)$，从而获得 M。

9.16

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	1	0	1	0	1	0	0
c	1	2	4	5	11	23	46	93	186	372
f	5	25	625	937	595	569	453	591	59	1013

9.18 因为 $Z = r^e \bmod n$，则 $r = Z^d \bmod n$，Bob 计算 $tY \bmod n = r^{-1}X^d \bmod n = r^{-1}Z^dC^d \bmod n = C^d \bmod n = M$，从而得到 M。

9.21 背包体制里的项：$90 + 455 + 341 + 132 + 56 + 82 = 1.156 \times 10^3$

9.22

（a）$w^{-1} \equiv 3 \pmod{20}$; $\mathbf{a} = (7, 1, 15, 10)$; $C = 18$。

（b）$w^{-1} \equiv 387 \pmod{491}$; $\mathbf{a} = (203, 118, 33, 269, 250, 9, 112, 361)$; $C = 357$

（c）$w^{-1} \equiv 15 \pmod{53}$; $\mathbf{a} = (39, 32, 11, 22, 37)$; $C = 119$

（d）$w^{-1} \equiv 1025 \pmod{9291}$; $\mathbf{a} = (8022, 6463, 7587, 7986, 65, 8005, 6592, 7274)$; $C = 30869$