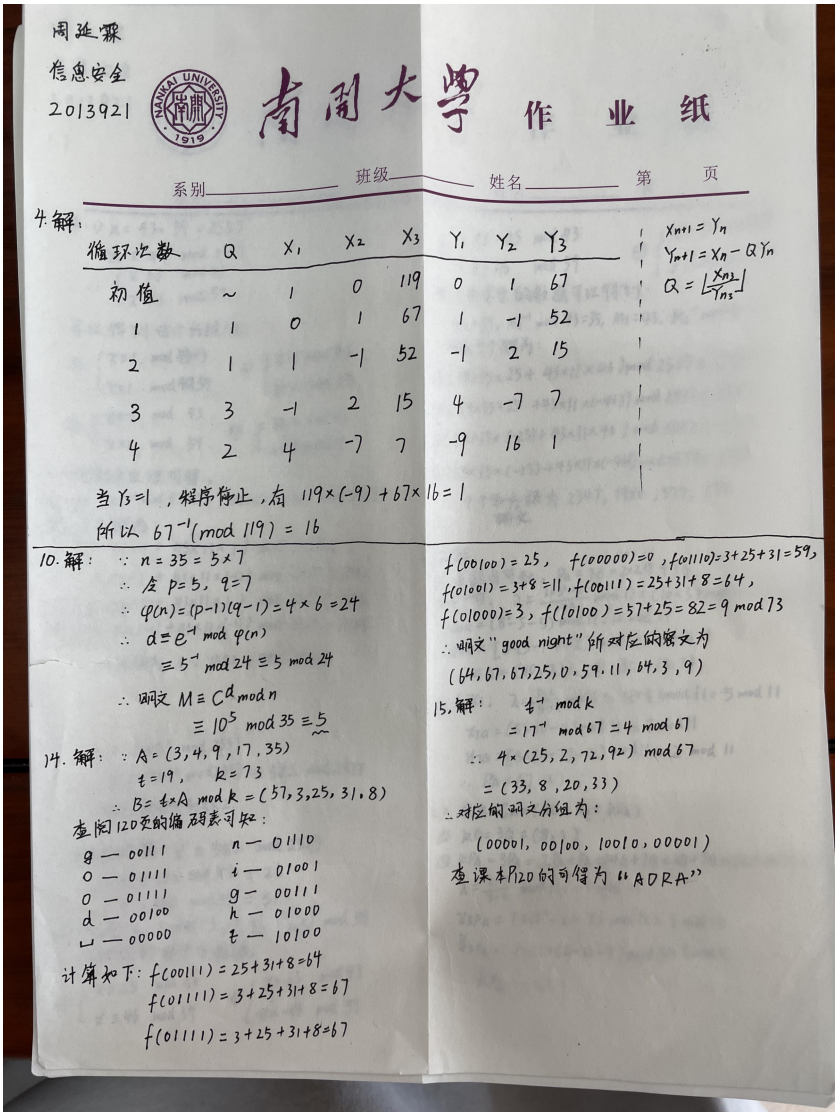
公钥密码作业



周延霖
信息安全
2013921

南開大學 作业纸

系别 班级 姓名 第 页

4. 解：

循环次数	Q	X_1	X_2	X_3	Y_1	Y_2	Y_3
初值	~	1	0	119	0	1	67
1	1	0	1	67	1	-1	52
2	1	1	-1	52	-1	2	15
3	3	-1	2	15	4	-7	7
4	2	4	-7	7	-9	16	1

$X_{n+1} = Y_n$
$Y_{n+1} = X_n - QY_n$
$Q = \lfloor \frac{X_n}{Y_n} \rfloor$

当 $Y_3 = 1$，程序停止，有 $119 \times (-9) + 67 \times 16 = 1$
所以 $67^{-1} \pmod{119} = 16$

10. 解：∵ $n = 35 = 5 \times 7$
∴ 令 $p = 5$, $q = 7$
∴ $\varphi(n) = (p-1)(q-1) = 4 \times 6 = 24$
∴ $d \equiv e^{-1} \bmod \varphi(n)$
$\equiv 5^{-1} \bmod 24 \equiv 5 \bmod 24$
∴ 明文 $M \equiv C^d \bmod n$
$\equiv 10^5 \bmod 35 \equiv 5$

14. 解：∵ $A = (3, 4, 9, 17, 35)$
$t = 19$, $k = 73$
∴ $B = t \times A \bmod k = (57, 3, 25, 31, 8)$
查阅120页的编码表可知：

g — 00111	n — 01110
o — 01111	i — 01001
o — 01111	g — 00111
d — 00100	h — 01000
␣ — 00000	t — 10100

计算如下：$f(00111) = 25 + 31 + 8 = 64$
$f(01111) = 3 + 25 + 31 + 8 = 67$
$f(01111) = 3 + 25 + 31 + 8 = 67$
$f(00100) = 25$, $f(00000) = 0$, $f(01110) = 3 + 25 + 31 = 59$,
$f(01001) = 3 + 8 = 11$, $f(00111) = 25 + 31 + 8 = 64$,
$f(01000) = 3$, $f(10100) = 57 + 25 = 82 = 9 \bmod 73$
∴ 明文 "good night" 所对应的密文为
(64, 67, 67, 25, 0, 59, 11, 64, 3, 9)

15. 解：$t^{-1} \bmod k$
$= 17^{-1} \bmod 67 = 4 \bmod 67$
∴ $4 \times (25, 2, 72, 92) \bmod 67$
$= (33, 8, 20, 33)$
∴ 对应的明文分组为：
(00001, 00100, 10010, 00001)
查课本P120的可得为 "ADRA"

周政霖
信息安全
2013921

南開大學 作业纸

系别 班级 姓名 第 页

17. 解：1) $n = 43 \times 59 = 2537$

因 $x^2 \equiv 1 \mod 2537$

$\therefore \begin{cases} x^2 \equiv 1 \mod 43 \\ x^2 \equiv 1 \mod 59 \end{cases}$

∴ 可以得到四个方程组：

① $\begin{cases} x \equiv 1 \mod 43 \\ x \equiv 1 \mod 59 \end{cases}$ ② $\begin{cases} x \equiv 1 \mod 43 \\ x \equiv -1 \mod 59 \end{cases}$

③ $\begin{cases} x \equiv -1 \mod 43 \\ x \equiv 1 \mod 59 \end{cases}$ ④ $\begin{cases} x \equiv -1 \mod 43 \\ x \equiv -1 \mod 59 \end{cases}$

由中国剩余定理可得，

$M_1 = 59$，$M_1^{-1} \bmod 43 \equiv 35$，$M_2 = 43$，$M_2^{-1} \bmod 59 \equiv 11$

对应4个解为：

① $(59 \times 35 \times 1 + 43 \times 11 \times 1) \mod 2537 \equiv 1$

② $(59 \times 35 \times 1 + 43 \times 11 \times (-1)) \mod 2537 \equiv 1592$

③ $(59 \times 35 \times (-1) + 43 \times 11 \times 1) \mod 2537 \equiv 945$

④ $(59 \times 35 \times (-1) + 43 \times 11 \times (-1)) \mod 2537 \equiv 2536$.

∴ 4个平方根为 1、1592、945、2536.

2) $C = 2347^2 \mod 2537$

$\equiv (-190)^2 \mod 2537 \equiv 582 \mod 2537$

对应的密文为582.

3) 解密即解 $x^2 \equiv 582 \mod 2537$

$\begin{cases} x^2 \equiv 582 \mod 43 = 23 \\ x^2 \equiv 582 \mod 59 = 51 \end{cases}$

又∵$(\pm 25)^2 \equiv 23 \mod 43$，$(\pm 46)^2 \equiv 51 \mod 59$.

∴ 可以得到四个方程组

① $\begin{cases} x \equiv 25 \mod 43 \\ x \equiv 46 \mod 59 \end{cases}$ ② $\begin{cases} x \equiv 25 \mod 43 \\ x \equiv -46 \mod 59 \end{cases}$

③ $\begin{cases} x \equiv -25 \mod 43 \\ x \equiv 46 \mod 59 \end{cases}$ ④ $\begin{cases} x \equiv -25 \mod 43 \\ x \equiv -46 \mod 59 \end{cases}$.

由1)中求出的数据可以得到：

$M_1 = 59$，$M_1^{-1} \bmod 43 = 35$，$M_2 = 43$，$M_2^{-1} \bmod 59 = 11$

∴对应4个解为：

① $(59 \times 35 \times 25 + 43 \times 11 \times 46) \mod 2537 \equiv 2347$

② $(59 \times 35 \times 25 + 43 \times 11 \times (-46)) \mod 2537 \equiv 1960$

③ $(59 \times 35 \times (-25) + 43 \times 11 \times 46) \mod 2537 \equiv 577$

④ $(59 \times 35 \times (-25) + 43 \times 11 \times (-46)) \mod 2537 \equiv 190$

∴ 4个平方根为 2347, 1960, 577, 190.

明文

20. 解：

1) 由题目可知，$P_A = 7G = 2 \times 2G + 3G$

①求 $4G$，$\lambda = \frac{3 \times 5^2 + 1}{2 \times 2} \mod 11 = (10 \times 3) \mod 11 = 8 \mod 11$

$x_{4G} = (8^2 - 5 - 5) \mod 11 = 10 \mod 11$

$y_{4G} = [8 \times (5 - 10) - 2] \mod 11 = 2 \mod 11$

∴ $4G = (10, 2)$ 又∵ $3G = (8, 3)$

②求 $7G$，$\lambda = \frac{3 - 2}{8 - 10} \mod 11 = (1 \times 5) \mod 11 = 5 \mod 11$

$x_{7G} = (5^2 - 10 - 8) \mod 11 = 7 \mod 11$

$y_{7G} = [5 \times (10 - 7) - 2] \mod 11 = 2 \mod 11$

∴ $P_A = (7, 2)$

2) 密文 $C_m = \{kG, P_m + kP_A\}$

① $kG = 3G = (8, 3)$

② $kP_A = 3P_A = 2P_A + P_A = 4G + 7G = 3G + 7G = (2, 7) + (7, 2)$

$\lambda = \frac{2 - 7}{7 - 2} \mod 11 = -1 \mod 11$

$x_{3P_A} = (-1)^2 - 2 - 7) \mod 11 = 3 \mod 11$

$y_{3P_A} = (-1) \times (2 - 3) - 7) \mod 11 = 5 \mod 11$

∴ $kP_A = (3, 5)$

周班霖

信息安全

2013921

南開大學 作业纸

系别 班级 姓名 第 页

① $P_m + kP_B = (10,9) + (3,5)$

$\lambda = \frac{5-9}{3-10} \bmod 11 = -1 \bmod 11$

$x' = ((-1)^2 - 10 - 3) \bmod 11 = 10 \bmod 11$

$y' = ((-1) \times (10-10) - 9) \bmod 11 = 2 \bmod 11$

$\therefore C_m = \{kG, P_m + kP_B\} = \{(8,3), (10,2)\}$

3) 恢复消息 P_m 过程如下：

$P_m = (P_m + kP_B) - n_B(kG)$

$= (10,2) - 7(8,3)$

$= (10,2) - (3,5) = (10,2) + (3,6) = (10,9)$

其中，首先计算 $2(8,3)$

$\lambda = \frac{3 \times 8^2 + 1}{2 \times 3} = 1 \bmod 11$

$x = 1^2 - 8 - 8 = 7 \bmod 11$，$y = 1 \times (8-7) - 3 \equiv 9 \bmod 11$

$\therefore 2(8,3) = (7,9)$

② $3(8,3) = 2(8,3) + (8,3)$

$\lambda = \frac{3-9}{8-7} \equiv 5 \bmod 11$

$x = 5^2 - 7 - 8 = 10 \bmod 11$，$y \equiv 9 \bmod 11$

$\therefore 3(8,3) = (10,9)$

③ $6(8,3) = 2 \times 3(8,3)$

$\lambda \equiv 10 \bmod 11$，$x \equiv 3 \bmod 11$，$y \equiv 6 \bmod 11$

$\therefore 6(8,3) = (3,6)$

④ $7(8,3) = 6(8,3) + (8,3)$

$\lambda \equiv 6 \bmod 11$，$x \equiv 3 \bmod 11$，$y \equiv 5 \bmod 11$

$\therefore 7(8,3) = (3,5)$

⑤ $P_m = (10,2) + (3,6)$

$\lambda \equiv 1 \bmod 11$，$x \equiv 10 \bmod 11$，$y \equiv 9 \bmod 11$

$\therefore$ 最后得到消息 $(10,9)$ 与第3问相同