COMP2711 Homework3

LIU, Jianmeng 20760163

Question 1:

From $32b - 21a = 19$, we have:

$$\begin{aligned} 32b - 21a &\equiv 19 (\text{mod } 21) \\ 32b &\equiv 19 (\text{mod } 21) \quad (*) \end{aligned}$$

To solve this congruence, we need to find a multiple inverse of 32 modulo 21. Notice that $\gcd(32, 21) = 1$, so by using the Euclidean algorithm, we have:

$$\begin{aligned} 32 &= 1 \cdot 21 + 11 \\ 21 &= 1 \cdot 11 + 10 \\ 11 &= 1 \cdot 10 + 1 \end{aligned}$$

Reverse the steps(extended Euclidean algorithm), we have:

$$\begin{aligned} 1 &= 11 - 1 \cdot 10 \\ &= 11 - 1 \cdot (21 - 1 \cdot 11) \\ &= 2 \cdot 11 - 1 \cdot 21 \\ &= 2 \cdot (32 - 1 \cdot 21) - 1 \cdot 21 \\ &= 2 \cdot 32 - 3 \cdot 21 \end{aligned}$$

Thus,

$$\begin{aligned} 2 \cdot 32 - 3 \cdot 21 &\equiv 1 (\text{mod } 21) \\ 2 \cdot 32 &\equiv 1 (\text{mod } 21) \end{aligned}$$

which means 2 is a multiple inverse of 32 modulo 21. To solve $(*)$, we multiply 2 on both sides,

$$\begin{aligned} 2 \cdot 32b &\equiv 2 \cdot 19 (\text{mod } 21) \\ b &\equiv 38 (\text{mod } 21) \equiv 17 (\text{mod } 21) \end{aligned}$$

Thus, $b = 17 + 21k$, where $k \in \mathbb{Z}$. Since $b \in \mathbb{Z}_{42}$, only $k = 0$ and $k = 1$ are valid, which gives $b = 17$ or $b = 38$.

- When $b = 17$, $32 \cdot 17 - 21a = 19$, we get $a = 25 \in \mathbb{Z}_{42}$.
- When $b = 38$, $32 \cdot 38 - 21a = 19$, we get $a = 57 \notin \mathbb{Z}_{42}$.

Therefore, there exists only one pair of a, b, where $a = 25, b = 17$.

Question 2:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(a)From the table above, the original message in integers is:

`12,4,4,19, ,0,19, ,19,7,4, ,15,0,17,10`

(b)According to (a), calculate $f(p)$ for each number p, we can easily get the ciphertext in integers:

`16,2,2,25, ,8,25, ,25,17,2, ,5,8,15,6`

(c) According to (b) and the table above:

`QCCZ IZ ZRB FIPG`

(d) Since $f(p) = (5p + 8) \bmod 26$, we have $5p \equiv f(p) - 8 (\bmod\ 26)$. By extended Euclidean algorithm, it's not difficult to find that a multiple inverse of 5 modulo 26 is 21.

Thus, $p \equiv 21 \cdot [f(p) - 8] \equiv 21 \cdot f(p) + 14 \pmod{26}$.

Therefore, $g(c) = (21c + 14) \bmod 26$.

Question 3:

We first let $m = 9 \cdot 14 \cdot 5 = 630$, $M_1 = m/9 = 70, M_2 = m/14 = 45, M_3 = m/5 = 126$.

By using extended Euclidean algorithm, we know:

4 is an inverse of M_1 modulo 9, since $4 \cdot 70 \equiv 4 \cdot 7 \equiv 1 (\bmod\ 9)$

5 is an inverse of M_2 modulo 14, since $5 \cdot 45 \equiv 5 \cdot 3 \equiv 1 (\bmod\ 14)$

1 is an inverse of M_3 modulo 5, since $1 \cdot 126 \equiv 1 \cdot 1 \equiv 1 (\bmod\ 5)$

So the solutions to the system are those x such that:

$$\begin{aligned} x &\equiv 4 \cdot 70 \cdot 4 + 8 \cdot 45 \cdot 5 + 3 \cdot 126 \cdot 1 \\ &= 3298 \\ &\equiv 148 (\bmod\ 630) \end{aligned}$$

Therefore, the solutions are those x such that $x \equiv 148 (\bmod\ 630)$, which can also be written as $x = 148 + 630k, k \in \mathbb{Z}$.

Question 4:

Note that $1027_{10} = 2^{10} + 2^1 + 2^0 = (100\ 0000\ 0011)_2$, compute:

$$\begin{aligned}
8^{2^0} &\equiv 8 (\bmod\ 22) \\
8^{2^1} &\equiv (8^2) \equiv 20 (\bmod\ 22) \\
8^{2^2} &\equiv (20^2) \equiv 4 (\bmod\ 22) \\
8^{2^3} &\equiv (4^2) \equiv 16 (\bmod\ 22) \\
8^{2^4} &\equiv (16^2) \equiv 14 (\bmod\ 22) \\
8^{2^5} &\equiv (14^2) \equiv 20 (\bmod\ 22) \\
8^{2^6} &\equiv (20^2) \equiv 4 (\bmod\ 22) \\
8^{2^7} &\equiv (4^2) \equiv 16 (\bmod\ 22) \\
8^{2^8} &\equiv (16^2) \equiv 14 (\bmod\ 22) \\
8^{2^9} &\equiv (14^2) \equiv 20 (\bmod\ 22) \\
8^{2^{10}} &\equiv (20^2) \equiv 4 (\bmod\ 22)
\end{aligned}$$

According to repeated squaring method, we know that

$$\begin{aligned}
8^{1027} &= 8^{2^{10}} \cdot 8^{2^1} \cdot 8^{2^0} \\
&\equiv 4 \cdot 20 \cdot 8 (\bmod\ 22) \\
&\equiv 2 (\bmod\ 22)
\end{aligned}$$

Therefore, $8^{1027} \equiv 2 (\bmod\ 22)$

Question 5:

To eliminate y, we multiply the first congruence by 15, the second by 18:

$$\begin{cases} 315x + 270y \equiv 195 \equiv 58 (\bmod\ 137) & (1) \\ 576x + 270y \equiv 162 \equiv 25 (\bmod\ 137) & (2) \end{cases}$$

$(2) - (1)$, we get:

$$261x \equiv -33 (\bmod\ 137)$$

Factorize both sides, we get:

$$3^2 \cdot 29x \equiv -3 \cdot 11 (\bmod\ 137) \quad (*)$$

As $116 \cdot 13 = 2^2 \cdot 13 \cdot 29 \equiv 1 (\bmod\ 137)$, we know that a multiple inverse of 29 modulo 137 is $2^2 \cdot 13$.

Multiple both sides of $(*)$ by $2^2 \cdot 13$, we get:

$$3^2 \cdot (2^2 \cdot 13 \cdot 29)x \equiv -2^2 \cdot 3 \cdot 11 \cdot 13 (\text{mod } 137)$$
$$3^2 \cdot x \equiv 65 (\text{mod } 137) \quad (**)$$

As $99 \cdot 18 = 2 \cdot 3^4 \cdot 11 \equiv 1(\text{mod } 137)$, we know that a multiple inverse of 3^2 modulo 137 is $2 \cdot 3^2 \cdot 11$. Multiple both sides of $(**)$ by $2 \cdot 3^2 \cdot 11$, we get:

$$3^2 \cdot 2 \cdot 3^2 \cdot 11 \cdot x \equiv 65 \cdot 2 \cdot 3^2 \cdot 11 (\text{mod } 137)$$
$$x \equiv 129 (\text{mod } 137)$$

Since $0 \leq x \leq 136$, $x = 129$ is the only solution.
Bring $x = 129$ back to $21x + 18y \equiv 13(\text{mod } 137)$, we get:

$$18 \cdot y \equiv 44 (\text{mod } 137)$$
$$2 \cdot 3^2 \cdot y \equiv 44 (\text{mod } 137)$$

Apply the similar method while finding x, as $99 \cdot 18 = 2 \cdot 3^4 \cdot 11 \equiv 1(\text{mod } 137)$, we know that a multiple inverse of $2 \cdot 3^2$ modulo 137 is $3^2 \cdot 11$, multiple it on both sides:

$$2 \cdot 3^2 \cdot 3^2 \cdot 11 \cdot y \equiv 44 \cdot 3^2 \cdot 11 (\text{mod } 137)$$
$$y \equiv 109 (\text{mod } 137)$$

Since $0 \leq y \leq 136$, $y = 109$ is the only solution.
Therefore, the system has only one solution, $x = 129, y = 109$.