1. (i) Confidentiality: protect the data by security mechanisms
(ii) Integrity: data can only be modified by authorized entities using authorized mechanisms.
(iii) Availability: data must be available to authorized entities.

2. (i) Data confidentiality: encryption/decryption of data.
(ii) Data integrity: avoid modification and replaying from attackers.
(iii) Authentication: proving that the user is authorized.
(iv) Non-repudiation: sender/receiver can't deny the fact that he had sent the data.
(v) Access control: using some mechanisms to allow some activities.

3. (i) We write an integer a to another form $a_n \cdots a_2 a_1 a_0$, where a_0 is the rightmost digit.

(ii) $8 = 2^3$
$10 = 2^1 \times 5^1$
It's clear that $8 \mid 10^n$ for $n \geq 3$
because $2^3 \mid (2^1 \times 5^1)^n$ for $n \geq 3$.

(iii) $r \equiv a \bmod 8 \pmod 8$
$\equiv (a_0 \times 10^0 + a_1 \times 10^1 + a_2 \times 10^2 + \cdots + a_n \times 10^n) \bmod 8$

$$\equiv [(a_0 \times 10^0 \bmod 8) + (a_1 \times 10^1 \bmod 8) + \cdots (a_n \times 10^n \bmod 8)] \bmod 8$$

$$\equiv [(a_0 \times 10^0 \bmod 8) + (a_1 \times 10^1 \bmod 8) + (a_2 \times 10^2 \bmod 8) + 0 + 0 + \cdots + 0] \bmod 8$$

$$\equiv [(a_0 \times 10^0 + a_1 \times 10^1 + a_2 \times 10^2) \bmod 8] \bmod 8$$

$$\equiv (a_0 \times 10^0 + a_1 \times 10^1 + a_2 \times 10^2) \bmod 8$$

4(a)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	84	320	84	1	0	1	0	1	0
3	320	84	68	0	1	-3	1	0	1
1	84	68	16	1	-3	4	0	1	-1
4	68	16	4	-3	4	-19	1	-1	5
4	16	4	0	4	-19	80	-1	5	-21
	4	0		-19	80		5	-21	

$\gcd(84, 320) = 4$, $s = -19$, $t = 5$

(b)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	400	60	40	1	0	1	0	1	-6
1	60	40	20	0	1	-1	1	-6	7
2	40	20	0	1	-1	3	-6	7	-20
	20	0		-1	3		7	-20	

$\gcd(400, 60) = 20$, $s = -1$, $t = 7$

5.(2) $180s + 7t = \gcd(180, 7) = 1$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
25	180	7	5	1	0	1	0	1	-25
1	7	5	2	0	1	-1	1	-25	26
2	5	2	1	1	-1	3	-25	26	-77
2	2	1	0	-1	3	X	26	-77	X
	1	0		3	X		-77	X	

(X: doesn't matter)

$7^{-1} \equiv -77 \pmod{180}$

$\equiv 103 \pmod{180}$

Because $\gcd(180, 7) = 1$, there's only 1 solution:

103

$180s + 132t = \gcd(180, 132) \neq 1$

(b)

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
1	180	132	48	1	0	1	0	1	-1
2	132	48	36	0	1	-2	1	-1	3
1	48	36	12	1	-2	3	-1	3	-4
3	36	12	0	-2	3	X	3	-4	X
	12	0		3	X		-4	X	

(X: doesn't matter)

~~$132^{-1} \equiv -4 \pmod{180}$~~

~~$\equiv 176 \pmod{180}$~~

Because $\gcd(180, 132) = 12$, there are 0 solutions

~~$x = x_0 + k \cdot \frac{180}{12} \quad (k \in \mathbb{Z})$~~

~~$= x_0 + 15k$~~

~~$X = \{11, 26, 41, 56, 71, 86, 101, 116, 131, 146, 161, 176\}$ in $\mathbb{Z}_{180}$~~

6. $39s + 15t = 270 = c$

↑ a ↑ b

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
2	39	15	9	1	0	1	0	1	-2
1	15	9	6	0	1	-1	1	-2	3
1	9	6	3	1	-1	2	-2	3	-5
2	6	3	0	-1	2	X	3	-5	X
	3	0		2	X		-5	X	

(X: doesn't matter)

$d = \gcd(39, 15) = 3$

$x_0 = \frac{c}{d} \times s = 180$

$y_0 = \frac{c}{d} \times t = -450$

$x = x_0 + k \times \frac{b}{d} = 180 + 5k \quad (k \in \mathbb{Z})$

$y = y_0 - k \times \frac{a}{d} = -450 - 13k$

Because $x \geq 0$ && $y \geq 0$, $-35 \geq k \geq -36$,

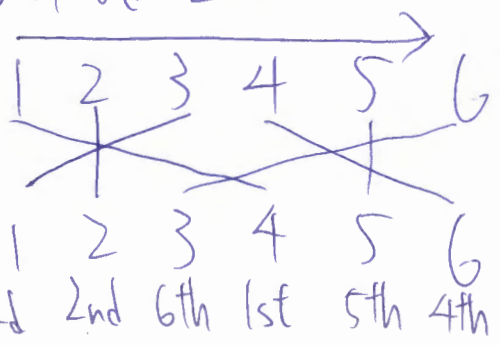
the ~~combination possible~~ set of possible stamp combination is $\{(5, 5), (0, 18)\}$ for 39-cent and 15-cent respectively.

7. (i) Method 1:

$$\begin{matrix}3&2&6&1&5&4\\1&2&3&4&5&6\end{matrix} \xrightarrow{\text{swap rows}} \begin{matrix}1&2&3&4&5&6\\3&2&6&1&5&4\end{matrix}$$

$$\xrightarrow{\text{sort by 2nd row}} \begin{matrix}4&2&1&6&5&3\\1&2&3&4&5&6\end{matrix} \Rightarrow \text{the 1st row is the answer}$$

(ii) Method 2:



src

↓ encryption ↑ decrypt

dest

4 2 1 6 5 3 #

8.(a) $Z_{16} = \{0, 1, 2, \cdots, 15\}$

$0^0 = 0$

$1^0 = 0$
$1^1 = 1$
$1^2 = 2$
$\vdots$
$1^{15} = 15$
} Z_{16}

$2^0 = 0$
$2^1 = 2$
$2^2 = 4$
$2^3 = 6$
$\vdots$
$2^7 = 14$

$3^0 = 0$
$3^1 = 3$
$3^2 = 6$
$3^3 = 9$
$\vdots$
$3^5 = 15$
$3^6 = 2$
$3^7 = 5$
$\vdots$
$3^{10} = 14$
$3^{11} = 1$
$\vdots$
$3^{15} = 13$
} Z_{16}

$4^0 = 0$
$4^1 = 4$
$4^2 = 8$
$4^3 = 12$

$5 \Rightarrow Z_{16}$

$6^0 = 0$
$6^1 = 6$
$6^2 = 12$
$6^3 = 2$
$6^4 = 8$
$6^5 = 14$
$6^6 = 4$
$6^7 = 10$

coprime with 16

$7 \Rightarrow Z_{16}$

$8^0 = 0$
$8^1 = 8$

$9 \Rightarrow Z_{16}$

$10^0 = 0$
$10^1 = 10$
$10^2 = 4$
$10^3 = 14$
$10^4 = 8$
$10^5 = 2$
$10^6 = 12$
$10^7 = 6$

$11 \Rightarrow Z_{16}$

$12^0 = 0$
$12^1 = 12$
$12^2 = 8$
$12^3 = 4$

$13 \Rightarrow Z_{16}$

$14^0 = 0$
$14^1 = 14$
$14^2 = 12$
$14^3 = 10$
$14^4 = 8$
$14^5 = 6$
$14^6 = 4$
$14^7 = 2$

$15 \Rightarrow Z_{16}$

subgroups of G:

$H_1 = \langle \{0\}, + \rangle$

$H_2 = \langle \{0, 2, 4, 6, 8, 10, 12, 14\}, + \rangle$

$H_3 = \langle \{0, 4, 8, 12\}, + \rangle$

$H_4 = \langle \{0, 8\}, + \rangle$

$H_5 = \langle Z_{16}, + \rangle$

(b) $Z_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$

$1^0 = 1$

$3^0 = 1$
$3^1 = 3$
$3^2 = 9$
$3^3 = 11$

$5^0 = 1$
$5^1 = 5$
$5^2 = 9$
$5^3 = 13$

$7^0 = 1$
$7^1 = 7$

$9^0 = 1$
$9^1 = 9$

$15^0 = 1$
$15^1 = 15$

inverse

$11^0 = 1$
$11^1 = 11$
$11^2 = 9$
$11^3 = 3$

inverse

$13^0 = 1$
$13^1 = 13$
$13^2 = 9$
$13^3 = 5$

subgroups of G:

$H_1 = \langle \{1\}, * \rangle$

$H_2 = \langle \{1, 3, 9, 11\}, * \rangle$

$H_3 = \langle \{1, 5, 9, 13\}, * \rangle$

$H_4 = \langle \{1, 7\}, * \rangle$

$H_5 = \langle \{1, 9\}, * \rangle$

$H_6 = \langle \{1, 15\}, * \rangle$

9. abelian : commutative : $a + b = b + a$

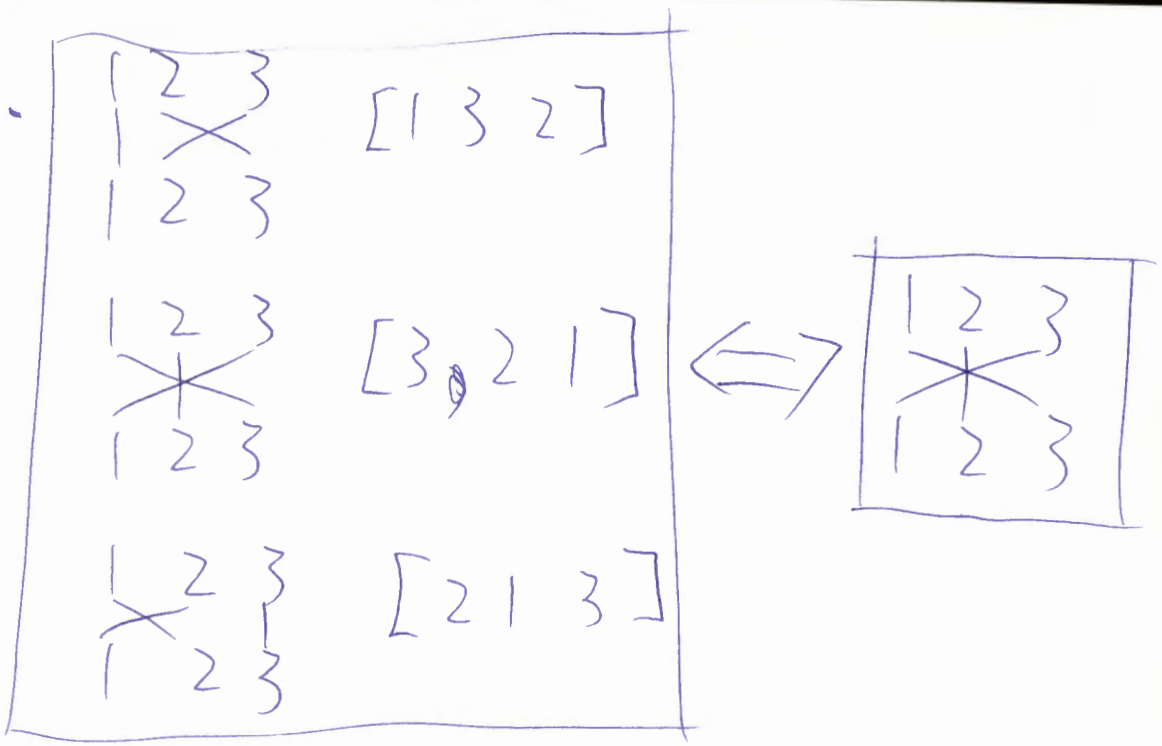
$*$	0	1	2	3	$\leftarrow x_j$
0	0	1	2	3	
1	1	2	3	0	
2	2	3	0	1	
3	3	0	1	2	

$\uparrow$ x_i

symmetric

$x_i + x_j = x_j + x_i$

10.



$\Leftrightarrow$

$[1\ 3\ 2] \circ [3\ 2\ 1] \circ [2\ 1\ 3]$

$= [3\ 2\ 1]$

$[3\ 2\ 1]^{-1} = [3\ 2\ 1]$

Bob can use one permutation $[3\ 2\ 1]$ to encrypt the message and can also use only one permutation $[3\ 2\ 1]$ to decrypt the message.

e.g Alice: "abc" => permutate using [1 3 2] => "acb"

using [3 2 1] => "bca" using [2 1 3] => "cba"

Bob: "abc" permutate using [3 2 1] => "cba"

decrypt using [3 2 1] => "abc"

Thus a combination of permutations can not strengthen the security.