



Midterm Solutions

Connie Lin & Cathy Cheng

Question 1

- Find the determinant and the multiplicative inverse of the following residue matrix A over Z_{10} .

$$A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$$

- Grading:
 - 3 points for correct determinant
 - 2 points for miscount or not simplify
 - 3 points for correct multiplicative inverse
 - 2 points for miscount or not simplify

Question 1 Solution

o Determinant of $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

o $\text{Det} \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

o $= (-1)^{1+1} \times 3 \times \det[1] + (-1)^{1+2} \times 0 \times \det[1]$

o Inverse of $A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}$

o A^{-1}

$$\frac{1}{3} = 1 \times 3^{-1} = 1 \times 7 = 7$$

o $= \frac{1}{3 \times 1 - 0 \times 1} \begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} \frac{1}{3} & 0 \\ -\frac{1}{3} & 1 \end{bmatrix} = \begin{bmatrix} 7 & 0 \\ -7 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 0 \\ 3 & 1 \end{bmatrix}$

Question 2

Find all solutions to the following sets of linear equations:

(a) $7x + 3y \equiv 3 \pmod{7}$

$$4x + 2y \equiv 5 \pmod{7}$$

(b) $2x + 3y \equiv 5 \pmod{8}$

$$x + 6y \equiv 3 \pmod{8}$$

Grading:

5 points total for (a)

3 points for correct answer, 2 points for showing work

5 points total for (b)

3 points for correct answer, 2 points for showing work

Question 2 Solution(cont.)

a) $7x + 3y \equiv 3 \pmod{7}$
 $4x + 2y \equiv 5 \pmod{7}$

$$\circ \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \end{bmatrix}$$

$$\circ \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}^{-1} \begin{bmatrix} 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 5 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \end{bmatrix}$$

$$\begin{aligned} \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}^{-1} &= \frac{1}{7 \times 2 - 3 \times 4} \begin{bmatrix} 2 & -3 \\ -4 & 7 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & -3 \\ -4 & 7 \end{bmatrix} = \begin{bmatrix} 1 & -\frac{3}{2} \\ -2 & \frac{7}{2} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 \\ 5 & 0 \end{bmatrix} \end{aligned}$$

Question 2 Solution(cont.)

b) $2x + 3y \equiv 5 \pmod{8}$

$$1x + 6y \equiv 3 \pmod{8}$$

$$\circ \begin{bmatrix} 2 & 3 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \end{bmatrix}$$

$$\circ \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 6 \end{bmatrix}^{-1} \begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 & 5 \\ 7 & 2 \end{bmatrix} \begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 45 \\ 41 \end{bmatrix} = \begin{bmatrix} 5 \\ 1 \end{bmatrix}$$

$$\begin{aligned} \begin{bmatrix} 2 & 3 \\ 1 & 6 \end{bmatrix}^{-1} &= \frac{1}{2 \times 6 - 3 \times 1} \begin{bmatrix} 6 & -3 \\ -1 & 2 \end{bmatrix} = \frac{1}{9} \begin{bmatrix} 6 & -3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{9} & \frac{2}{9} \end{bmatrix} \\ &= \begin{bmatrix} 6 & 5 \\ 7 & 2 \end{bmatrix} \end{aligned}$$

Question 3

o Alice can use only the additive cipher on her computer to send a message to a friend. She thinks that the message is more secure if she encrypts the message two times, each time with a different key. Is she right? Defend your answer.

o Grading:

o 5 points for correct answer

o 5 points for correct defense

Question 3 Solution

o NO!

o Example:

- o If she uses $k = 2$ for the first round and $k = 3$ for the second round; this is the same as just using $k = 5$ for one round.
- o In general using k_1, k_2, \dots, k_i for i rounds is the same as using $k = \sum k_i \pmod{26}$ for 1 round.

Question 4

- o Alice has a long message to send. She is using the mono-alphabetic substitution cipher. She thinks that if she compresses the message, it may protect the text from single-letter frequency attack by Eve. Does the compression help? Should she compress the message before the encryption or after the encryption? Defend your answer.
- o Grading:
 - o 3 points for correct YES/NO response
 - o 3 points for correct Before/After response
 - o 4 points for logical defense

Question 4 Solution




- o YES!
- o She should compress before the encryption.
- o Compression in general creates a text which is not in the source language. This means that the compressed plaintext does not preserve the frequency of characters. Thus making single-letter frequency attack useless.

Question 5

- Find the result of $00100110 \otimes 10011110$ in $\text{GF}(2^8)$ with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
- Find the inverse of 00100110 in $\text{GF}(2^8)$ with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
- Grading:
 - 5 points total for (a)
 - 3 points for correct answer, 2 points for showing work
 - 5 points total for (b)
 - 3 points for correct answer, 2 points for showing work

Question 5 Solution

(a) **00100110** \otimes 10011110 mod **100011011**

	Left-shift	Exclusive-OR
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	1 <u>00111100</u>	<u>00111100</u> \oplus 00011011 = 00100111 
$x^2 \otimes P_2$	01001110	01001110 
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	1 <u>00111000</u>	<u>00111000</u> \oplus 00011011 = 00100011
$x^5 \otimes P_2$	01000110	01000110 
$x^6 \otimes P_2$	10001100	10001100

Question 5 Solution(cont.)

$x^7 \otimes P_2$

100011000

00011000 \oplus **00011011** = 00000011

$$\begin{aligned} P_1 \otimes P_2 &= 00100111 \oplus 01001110 \oplus 01000110 \\ &= 00101111 \end{aligned}$$

$$\Rightarrow x^5 + x^3 + x^2 + X + 1$$

Question 5 (b) Solution(cont.)

q	r1	r2	r	t1	t2	t
$x^3 + 1$	$x^8 + x^4 + x^3 + x + 1$	$x^5 + x^2 + x$	$x^3 + x^2 + 1$	0	1	$x^3 + 1$
$x^2 + x + 1$	$x^5 + x^2 + x$	$x^3 + x^2 + 1$	$x^2 + 1$	1	$x^3 + 1$	$x^5 + x^4 + x^3 + x^2 + x$
$x + 1$	$x^3 + x^2 + 1$	$x^2 + 1$	x	$x^3 + 1$	$x^5 + x^4 + x^3 + x^2 + x$	$x^6 + x^3 + x + 1$
x	$x^2 + 1$	x	1	$x^5 + x^4 + x^3 + x^2 + x$	$x^6 + x^3 + x + 1$	$x^7 + x^5 + x^3$
x	x	1	0	$x^6 + x^3 + x + 1$	$x^7 + x^5 + x^3$	$x^8 + x^4 + x^3 + x + 1$
	1	0		$x^7 + x^5 + x^3$	$x^8 + x^4 + x^3 + x + 1$	

Question 6

- A 6×2 S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusive-ors the even-numbered bits to get the right bit of the output. If the input is 110010, what is the output? If the input is 101101, what is the output?
- Grading:
 - 5 points for correct 1st output
 - 5 points for correct 2nd output

Question 6 Solution

0 110010

0 $1 \oplus 0 \oplus 1 = 0$

0 $1 \oplus 0 \oplus 0 = 1$



5	4	3	2	1	0
---	---	---	---	---	---

01

or

6	5	4	3	2	1
---	---	---	---	---	---

10

0 101101

0 $1 \oplus 1 \oplus 0 = 0$

0 $0 \oplus 1 \oplus 1 = 0$



00

Question 7

- o What is the key complement property in DES? How can you use this property to perform brute-force attack in 2^{55} encryptions instead of 2^{56} encryptions?
- o Grading:
 - o 5 points for explanation of WHAT question
 - o 5 points for explanation of HOW question

Question 7 Solution

- Key Complement Property:

- $E_k(P) = C \Leftrightarrow E_{k'}(P') = C'$

- Because of the above property, only half of the keys need to be considered. Thus when brute-forcing, instead of trying 2^{56} , you only need to try $2^{56}/2 = 2^{55}$

Question 8

- o What's the purpose of the Cipher-text Stealing Technique? How can it be applied to EBC mode and CBC mode?
- o Grading:
 - o 4 points for explanation of purpose
 - o 3 points for EBC mode explanation
 - o 3 points for CBC mode explanation

Question 8 Solution

o Ciphertext stealing technique is used to make it possible to use ECB/CBC mode without padding.

o ECB:

o $X = E_K(P_{N-1}) \rightarrow C_N = \text{head}_m(X)$

o $Y = P_N | \text{tail}_{n-m}(X) \rightarrow C_{N-1} = E_K(Y)$

o CBC:

o $U = P_{N-1} \oplus C_{N-2} \rightarrow X = E_K(U) \rightarrow C_N = \text{head}_m(X)$

o $V = P_N | \text{pad}_{n-m}(0) \rightarrow Y = X \oplus V \rightarrow C_{N-1} = E_K(Y)$

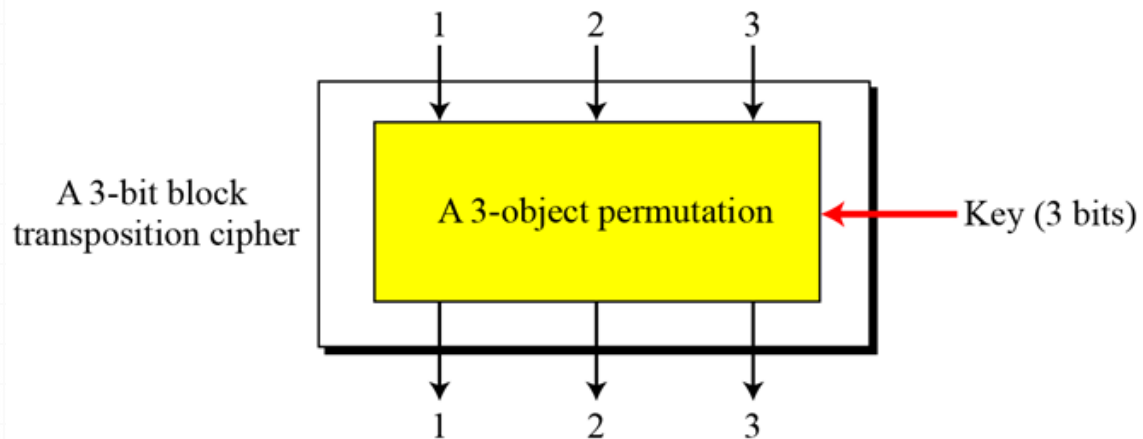
Question 9

- A full-size key n -bit transposition cipher can be modeled as a permutation. What's its key length? Defend your answer.
- A full-size key n -bit substitution cipher can be modeled as a permutation. What's its key length? Defend your answer.
- Grading:
 - 5 points for each part (a) and (b)

Question 9 Solution

- A full-size key n -bit transposition cipher
- Possible keys: $n!$
- Key length: $\log n!$

Figure 5.2 *A transposition block cipher modeled as a permutation*



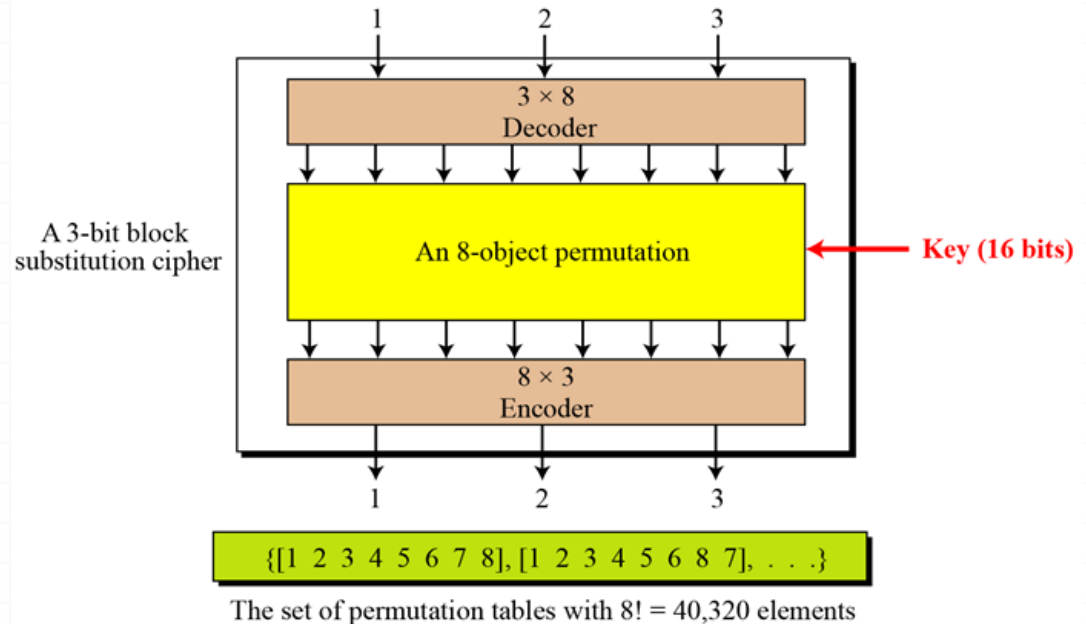
$\{[1\ 2\ 3], [1\ 3\ 2], [2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2], [3\ 2\ 1]\}$

The set of permutation tables with $3! = 6$ elements

Question 9 Solution

- A full-size key n -bit substitution cipher
- Possible keys: $2^n!$
- Key length: $\log 2^n!$

Figure 5.3 *A substitution block cipher model as a permutation*



Question 10

o List the parameters for the three AES versions.

o Solution:

Block Size	Key Size	# Rounds
128 bits	128 bits	10
128 bits	192 bits	12
128 bits	256 bits	14

o Grading:

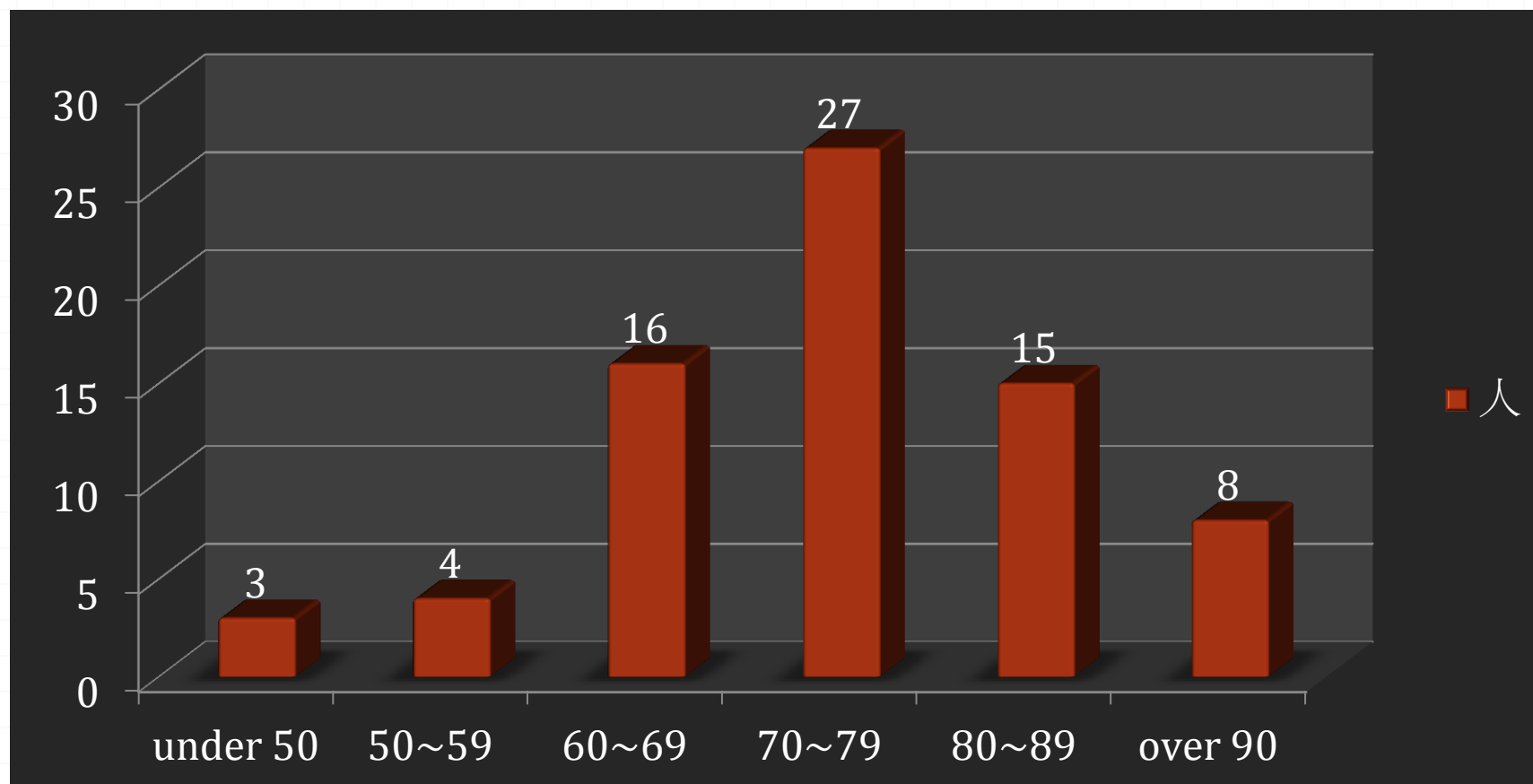
o 1 point each of the 9

o +1 for getting any one correct

總人數：76
應考數：73
缺考數： 3 人

statistic

總平均：74.1
標準差：11.98



statistic

各小題得分統計

Problem	Full points	AVG
P1	25	7.9
P2	42	7.6
P3	72	9.8
P4	22	4.5
P5	36	6.9
P6	64	9.4
P7	54	7.9
P8	15	5.9
P9	50	7.4
P10	20	6.4
	人	分