MMTE-006

ASSIGNMENT BOOKLET

It is compulsory to submit the assignment before submitting the examination form.

M.Sc. (Mathematics with Applications in Computer Science)

CRYPTOGRAPHY

(July 1, 2022 – June 30, 2023)

School of Sciences
Indira Gandhi National Open University
Maidan Garhi, New Delhi 110068
2022-2023

Dear Student,
Please read the section on assignments in the Programme Guide that we sent you after your enrolment. As you may know already from the programme guide, the continuous evaluation component has 20% weightage. This assignment is for the continuous evaluation component of the course.

Instructions for Formating Your Assignments

Before attempting the assignment please read the following instructions carefully.

1) On top of the first page of your answer sheet, please write the details exactly in the following format:

ROLL NO. : .....

NAME : .....

ADDRESS : .....

.....

.....

COURSE CODE : ....

COURSE TITLE : .....

STUDY CENTRE : ..... **DATE** .....

PLEASE FOLLOW THE ABOVE FORMAT STRICTLY TO FACILITATE EVALUATION AND TO AVOID DELAY.

2) Use only foolscap size writing paper (but not of very thin variety) for writing your answers.

3) Leave 4 cm margin on the left, top and bottom of your answer sheet.

4) Your answers should be precise.

5) While solving problems, clearly indicate which part of which question is being solved.

6) Write all the answers in your own words. Do not copy from the internet, from your fellow students or from any other source. If your assignment is found to be copied, it will be rejected.

7) This assignment is valid only up to 30th June, 2023. If you fail in this assignment or fail to submit it by 30th June, 2023, then you need to get the assignment for 2023-24 and submit it as per the instructions given in the Programme Guide.

8) It is **compulsory** to submit the assignment before you submit your examination form.

We **strongly** suggest that you retain a copy of your answer sheets.

Wish you good luck.

Assignment

Course Code: MMTE-006
Assignment Code: MMTE-006/TMA/2022–23
Maximum Marks: 100

Note: The notations and conventions in this assignment are those used in the course material. Block numbers, unit numbers, etc. refer to the course material.)

1) a) Let $f(x) = x^3 - x - 1 \in \mathbf{Z}_5[x]$. Find the product of $x^2 + 2x + 1 + (f(x))$ and $x^2 + 3x - 1 + (f(x))$ using the algorithm in page 23, block 1. You should show all the steps as in example 11, page 22, block 1. (3)

b) Let $f(x) = x^4 + x + 1 \in \mathbf{F}_2[x]$. We represent the field $\mathbf{F}_{2^4}$ by $\mathbf{F}_2[x]/(f(x))$. Let us write $\gamma = x + (f(x))$. The table of values is given below:

i	γ^i	Vector	i	γ^i	Vector
0	1	$(0,0,0,1)$	8	γ^2+1	$(0,1,0,1)$
1	γ	$(0,0,1,0)$	9	$\gamma^3+\gamma$	$(1,0,1,0)$
2	γ^2	$(0,1,0,0)$	10	$\gamma^2+\gamma+1$	$(0,1,1,1)$
3	γ^3	$(1,0,0,0)$	11	$\gamma^3+\gamma^2+\gamma$	$(1,1,1,0)$
4	$\gamma+1$	$(0,0,1,1)$	12	$\gamma^3+\gamma^2+\gamma+1$	$(1,1,1,1)$
5	$\gamma^2+\gamma$	$(0,1,1,0)$	13	$\gamma^3+\gamma^2+1$	$(1,1,0,1)$
6	$\gamma^3+\gamma^2$	$(1,1,0,0)$	14	γ^3+1	$(1,0,0,1)$
7	$\gamma^3+\gamma+1$	$(1,0,1,1)$			

i) Prepare logarithm and antilogarithm tables as given in page 23 of block 1. (4)

ii) Compute $\frac{(\gamma^4+\gamma^2)+(\gamma^3+\gamma+1)}{(1+\gamma^2+\gamma^4)(1+\gamma^3)}$ and $\frac{\gamma^2(\gamma^2+\gamma+1)}{(\gamma^3+\gamma^2)(1+\gamma^5)}$ using the logarithm and antilogarithm tables. (3)

2) a) Decrypt each of the following cipher texts:

i) Text: "CBBGYAEBBFZCFEPXYAEBB", encrypted with affine cipher with key $(7,2)$. (3)

ii) Text:"KSTYZKESLNZUV", encrypted with Vigenère cipher with key "RESULT". (3)

b) Another version of the columnar transposition cipher is the cipher using a key word. In this cipher, we encrypt as follows: Given a key word, we remove all the duplicate characters in the key word. For example, if the key word is 'SECRET', we remove the second 'E' and use 'SECRT' as the key word. To encrypt, we form a table as follows: In the first row, we write down the key word. In the following rows, we write the plaintext. Suppose we want to encrypt the text 'ATTACKATDAWN'. We make a table as follows:

S	**E**	**C**	**R**	**T**
A	T	T	A	C
K	A	T	D	A
W	N	X	X	X

Then we read off the columns in alphabetical order. We first read the column under 'C', followed by the columns under 'E', 'R', 'S' and 'T'. We get the cipher text TTX TAN ADX AKW CAX. To decrypt, we reverse the process. Note that, since we know the length of the keyword, we can find the length of the columns by dividing the length of the message by the length of the keyword.

Given the ciphertext 'HNDWUEOESSRORUTXLARFASUXTINOOGFNEGASTORX' and the key word 'LANCE', find the plaintext. (4)

3) a) Find the inverse of 13 $\pmod{51}$ using extended euclidean algorithm. (4)

b) Use Miller-Rabin test to check whether 75521 is a strong pseuodprime to the base 2. (5)

4) a) In this exercise, we introduce you to Hill cipher. In this cipher, we convert our message to numbers, just as in affine cipher. However, instead of encrypting character by character, we encrypt pairs of characters by multiplying them with an **invertible matrix** with co-efficients in $\mathbf{Z}_{26}$.

Here is an example: Suppose we want to ENCRYPT "ALLISWELL". Since we require the plaintext to have even number of characters, we pad the message with the character 'X'. We break up the message into pairs of characters AL, LI, SW, EL and LX. We convert each pair of characters into a pair elements in $\mathbf{Z}_{26}$ as follows:

AL	$(\overline{0},\overline{11})$
LI	$(\overline{11},\overline{8})$
SW	$(\overline{18},\overline{22})$
EL	$(\overline{4},\overline{11})$
LX	$(\overline{11},\overline{23})$

Next, we choose an inveritble 2×2 matrix with coefficients in $\mathbf{Z}_{26}$, for example, $A=\begin{bmatrix}\overline{3} & \overline{1}\\ \overline{7} & \overline{4}\end{bmatrix}$.

This matrix has determinant $\overline{3}\cdot\overline{4}-\overline{7}\cdot\overline{1}=\overline{5}$ and $\overline{5}$ is a unit in Z_{26} with inverse $\overline{21}$. We write each pair of elements in Z_{26} as a column vector and multiply it by A:

$$A\begin{bmatrix}\overline{0}\\ \overline{11}\end{bmatrix}=\begin{bmatrix}\overline{11}\\ \overline{18}\end{bmatrix}, A\begin{bmatrix}\overline{11}\\ \overline{8}\end{bmatrix}=\begin{bmatrix}\overline{15}\\ \overline{5}\end{bmatrix},\dots$$

We then convert each pair of numbers to a pair of characters and write them down. In this example, we get the cipher text "LSPFYGXUEN" corresponding to the plain text "ALLWELL".

To decrypt, we convert pairs of characters to pairs of numbers and multiply by $A^{-1}=\overline{5}^{-1}\begin{bmatrix}\overline{4} & \overline{-1}\\ \overline{-7} & \overline{3}\end{bmatrix}=\overline{21}\begin{bmatrix}\overline{4} & \overline{-1}\\ \overline{-7} & \overline{3}\end{bmatrix}=\begin{bmatrix}\overline{6} & \overline{5}\\ \overline{9} & \overline{11}\end{bmatrix}$ and we have

$$\begin{bmatrix}\overline{6} & \overline{5}\\ \overline{9} & \overline{11}\end{bmatrix}\begin{bmatrix}\overline{11}\\ \overline{18}\end{bmatrix}=\begin{bmatrix}\overline{0}\\ \overline{18}\end{bmatrix},\dots.$$

Decrypt the text "TWDXHUJLUENN" which was encrypted using the Hill's cipher with the matrix $\begin{bmatrix}\overline{3} & \overline{1}\\ \overline{0} & \overline{9}\end{bmatrix}$ as the encryption matrix. (6)

5) a) Decrypt the ciphertext 101000111001 which was encrypted with the Toy block cipher once using the key 101010010. Show all the steps. (5)

b) A 64 bit key for the DES is given below

11000111	10000101
11110111	11000001
11111011	10101011
10011101	10010001

i) Check whether the key is error free using the parity bits.

ii) Find the keys for the second round. (4)

6) a) Considering the bytes 10001001 and 10101010 as elements of the field $\mathbf{F}_2[X]/\langle g(X)\rangle$, where $g(X)$ is the polynomial $X^8+X^4+X^3+X+1$, find their product and quotient. (6)

b) Find a recurrence that generates the sequence 110110110110110. (6)

7) a) Apply the frequency test, serial test and autocorrelation test to the following sequence at level of significance $\alpha = 0.05$:
01100111000011001001100. (6)

b) Apply poker test to the following sequence with level of significane $\alpha = 0.05$. (4)
10011010000100001011111011
01110100101101100100110.

c) Apply runs test to the following sequence:
10011010000100001011111011
01110100101101100100110
01100111000011001001110
11000011010101111010011110
00100011110000011010100 10
10001101000001101001011 01
1110001001 (5)

8) a) Decrypt the message $c = 23$ that was encrypted using RSA algorithm with $e = 43$ and $n = 77$. (4)

b) i) Bob uses ElGamal cyrptosystem with parameters $p = 47$, $g = 5$ and the secret value $x = 3$. What values will he make public? (2)

ii) Alice wants to send Bob the message $\mathscr{M} = 15$. She chooses $k = 5$. How will she compute the cipher text? What information does she send to Bob? (4)

iii) Explain how Bob will decrypt the message. (4)

9) a) Solve the discrete logarithm problem $5^x \equiv 22 \pmod{47}$ using Baby-Step, Giant-Step algorithm. (7)

b) Alice wants to use the ElGamal digital signature scheme with public parameters $p = 47$, $\alpha = 2$, secret value $a = 7$ and $\beta = 34$. She wants to sign the message $\mathscr{M} = 20$ and send it to Bob. She chooses $k = 5$ as the secret value. Explain the procedure that Alice will use for computing the signature of the message. What information will she send Bob? (4)

c) Alice wants to use the Digital Signature algorithm for signing messages. She chooses $p = 83$, $q = 41$, $g = 2$ and $a = 3$. Alice wants to sign the message $\mathscr{M} = 20$. She chooses the secret value $k = 8$. Explain the procedure that Alice will use for computing the signature. What information will she send Bob? (4)