UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET		
COURSE CODE	:	BNS 3233
COURSE	:	CRYPTOGRAPHY
SEMESTER/SESSION	:	SEM 2, SESSION 2024/2025
DURATION	:	3 HOURS

Instructions:

1. This booklet contains **5** questions. Answer **ALL** questions.
2. All answers should be written in answer booklet.
3. Write legibly and draw sketches wherever required.
4. If in doubt, raise your hands and ask the invigilator.

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE TOLD TO DO SO

THIS BOOKLET CONTAINS 5 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

a) Describe this information protection by cryptography below:
   i) Integrity (2 marks)
   ii) Authenticity (2 marks)
   iii) Confidentiality (2 marks)

b) State information protection by cryptography for description below:
   i) Authorized users are provided the decryption key to access the information (1 mark)
   ii) Prevents an individual from fraudulently denying they were involved in a transaction. (1 mark)

c) Differentiate **TWO (2)** characteristics between Symmetric and Asymmetric key encryption. (4 marks)

d) Cryptographic systems are also classified along **THREE (3)** Independent Dimensions. Outline **THREE (3)** independent dimension of cryptography (3 marks)

QUESTION 2

a) State **THREE (3)** examples of classical cipher that applied substitution or transposition technique. (3 marks)

b) Answer following questions. A conversion table for letters and numbers is shown in **Table 1**:

Table 1: Conversion table of alphabet

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

   i) You have intercepted a message encrypted with Vernam Cipher. Decrypt the ciphertext of VGGQTOFFAKQQSSWJ using key ECUMHNBOHWPZOSDC (5 marks)
   ii) Encrypt plaintext "TROJAN" using Hill Cipher with Key: $\begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$ (9 marks)

QUESTION 3

a) Use modular exponentiation theorem to compute:

i) $19^{123} \bmod 23$ (5 marks)

ii) $21^{93} \bmod 47$ (5 marks)

b) Analyze the value of GCD. Given a=378, b= 119.

i) Solve GCD (a, b) by using Euclidean's Algorithm. (2.5 marks)

ii) Find integers s and t by using Extended Euclidean's Algorithm. (4.5 marks)

QUESTION 4

a) In Diffie-Hellman Key Exchange, given that g=5, p=23, Secret Key X_A=6, X_B=15.

i) Show calculation to determine Public Key Y_A and Y_B (4 marks)

ii) Shared Key S_A and S_B (4 marks)

b) The decryption function of RSA is defined as:

$$P = C^d \bmod n$$

i) State the decryption function of RSA. (1 mark)

ii) State the public key in RSA, $PU\{\ \}$. (1 mark)

iii) State the private key in RSA, $PR\{\ \}$. (1 mark)

iv) Describe the steps for generating the public/private key pair. You must state the conditions/properties of any values to be selected or calculated. (5 marks)

c) Using simplified RSA scheme with Public Key $PU\{7, 187\}$ and Private Key $PR\{23, 187\}$. Answer following question:

i) Solve RSA encryption if given that plaintext is 5. (4 marks)

ii) Solve RSA decryption. (6 marks)

QUESTION 5

a) Designing a good keystream generator in Stream Cipher is challenging. Discuss the reason what characteristic of a good keystream. (4 marks)

b) Despite being weak on its own substitution and transposition are still used in the design of modern cryptography. Give **ONE (1)** example on how substitution and transposition being applied in Data Encryption Standard (DES).

i) Substitution in DES algorithm (1 mark)

ii) Transposition in DES algorithm (1 mark)

c) Name **THREE (3)** examples of Stream Cipher. (2 marks)

d) Answer following question based on **Table 2**:

Table 2: S-Box in DES algorithm

row \ col	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Table 2 shows S-box of DES algorithm. In DES algorithm, T" ← ($S_1(B_1)$, $S_2(B_2)$, ... $S_8(B_8)$). $S_i(B_i)$ maps B_i to the entry in row and column of Si. Show your calculation the result of 100011 passing S-Box 3 by answering following questions:

i) Solve the value of row in decimal. (1 mark)

ii) Solve the value of column in decimal. (1 mark)

iii) By referring S-Box (using your answer in (i) and (ii)), state the value of 4-bits of output. (1 mark)

e) Discuss algorithm of DES $(L_0, R_0) \leftarrow IP\left(m_1, m_2, \ldots m_{64}\right)$ (2 marks)

f) Advanced Encryption Standard (AES) has four stages which are AddRoundKey, SubByte, ShiftRow and MixColumn. On which stage that provide:
   i) Diffusion (1 mark)
   ii) Confusion (1 mark)

g) MixColumn in AES operates on the state column-by-column treating each column as a 4-term polynomial $a(x) = a_3x^3 + a_2x^2\, a_1x^1 + a_0$.
   i) Solve $(\{02\}.C3)$ into a polynomial format. (3 marks)
   ii) By answering question (i), divided your answer with irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Write your last answer in binary. (3 marks)

h) Solve this initial round in AES algorithm $A8 \oplus BE$. Write the final answer in hex. (4 marks)

----------End of questions----------