ST. XAVIER'S COLLEGE
KOLKATA
(AUTONOMOUS)

3rd SEMESTER EXAMINATION
DECEMBER 2021
M. Sc. COMPUTER SCIENCE

CMSM4324

CRYPTOGRAPHY AND NETWORK SECURITY

Wednesday, December 15, 2021
12:00 NOON to 3:00 PM
3 hours
Full Marks : **80**

PLEASE READ THESE INSTRUCTIONS BEFORE YOU START WRITING:

1. Of the questions attempted, the answers to only the first required number of questions (as stipulated in the question paper) will be evaluated. **So please do not attempt extra questions**.
2. Use fountain pen or ball-point pen of **blue** or **black ink**.
3. Write **(not type)** the answers legibly, in your own words as far as practicable, on A4 size sheets.
4. Save the pages of your answer sheets (hand-written document) to a single PDF file and name the document accurately i.e. **Roll No_Paper Code.PDF** (example: 147_PH36141T).
5. Send the PDF file to the following email address **(in REPLY mode) within 30 minutes of the completion of the examination**: **CMSM43242122@SXCCAL.EDU**
6. The scanned answer scripts should have **enough clarity** to enable evaluation.
7. On top of each page **handwrite** the following information: **Name, Roll Number, Paper Code , Date,** and **Page Number**
8. No multiple submissions would be allowed.

The marks are given in **brackets [ ]** at the end of each question or part question.

The question paper consists of **2** pages.

Of the questions attempted, the answers to only the first required number of questions (as stipulated in the question paper) will be evaluated.
So, PLEASE DO NOT ATTEMPT EXTRA QUESTIONS.

GROUP A

Answer **Question No. 1** and **ANY TWO** from the rest.

1. Write short notes on **ANY TWO**. **[2×5=10]**
   i. Advantages of cybersecurity
   ii. Motives behind cybercrime
   iii. Digital signatures

2. Consider the first twelve characters of your full name to be the plain text (Repeat the pattern if it is shorter than 12). Encrypt it using the following algorithm:
   (a) Replace each alphabet with its equivalent 7 bit ascii code.
   (b) Add a 0 bit as the left most bit to make each of the above bit patterns 8 positions long.
   (c) Swap the first 4 bit positions with the last 4 positions for each character.
   (d) Write the hexadecimal equivalent of every four bits. **[15]**

3. (a) Consider the plain text alphabet to be the third character of your name. Using the RSA algorithm and the values as E=3, D=11, N=15, find out what this plain text alphabet encrypts to, and verify that upon decryption, it transforms back to it.
   (b) What is the real crux of RSA? **[12+3=15]**

4. (a) Differentiate between MAC and message digest with an example of your own.
   (b) Citing examples from your final semester project, explain how you plan to achieve the principles of security. **[6+9=15]**

GROUP B

Answer **Question No. 5** and **ANY TWO** from the rest.

5. Answer **ANY TWO** of the following questions. **[2×5=10]**
   (a) Which design of a modern block cipher will be less vulnerable to the attacker – substitution cipher or transposition Cipher? Justify with a proper example.
   (b) Find the solution(s) of the equation $4x + 6 \equiv 4 (\text{mod } 6)$.
   (c) Using the fundamental theorem of arithmetic, find the gcd of 114 and 168.

6. (a) What are the steps of a modern stream cipher? Mention its various categories.
   (b) Generate the Playfair matrix if the keyword is HIMALAYAS. Using this matrix, encrypt your first name.
   (c) What is the importance of Euler's Phi function? Find the value of $\Phi(n)$, where 'n' is the sum of the digits of your class roll number. **[(3+2)+(2+4)+(2+2)=15]**

7. (a) What is Lagrange theorem in connection with a multiplicative group?
   (b) What is a primitive root of a multiplicative group? Explain its significance. Does the group $G = <Z_{50}^*, \times>$ have any primitive root?
   (c) Using Fermat's little theorem, find the multiplicative inverse of 5 in Z_{13}.
   (d) Explain the function that is used in the mixer component of DES cryptosystem.
   [2+(2+2+1)+3+5=15]

8. (a) Explain the steps used in Vigenere cryptosystem. Explain the Kasiski test used for identifying the length of the key used in Vigenere cryptosystem.
   (b) What are Mersenne prime numbers? Give an example.
   (c) What is the challenge-response technique in entity authentication?
   (d) What is EER in biometric authentication? **[(3+5)+(2+1)+2+2=15]**

.