DHANAMANJURI UNIVERSITY

Four-year course B.A/B.Sc 6th Semester

JUNE-2024

Name of Programme	**:**	**B.A/B.Sc Mathematics (Honours)**
Paper Type	**:**	**DSE-3(Theory)**
Paper Code	**:**	**EMA-307**
Paper Title	**:**	**Cryptography & Network Security**
Full marks	**:**	**100**
Pass Mark	**:**	**40**
Duration	**:**	**3 Hours**

The figures in the margin indicate full marks for the questions.
Answer all the questions:

1. Choose and rewrite the correct answer: $1 \times 5 = 5$

a) The gcd of two consecutive integers $n+1$ and $n+2$ is:

i) 4
ii) 1
iii) 2
iv) 3

b) If p and q are primes, then Euler's totient function is:

i) $\varphi(q) = n(p-1)$
ii) $\varphi(p) = n(q-1)$
iii) $\varphi(n) = p \cdot q$
iv) $\varphi(n) = (p-1)(q-1)$

c) The value of $15^4 \mod 61$ is:

i) 56
ii) 54
iii) 31
iv) 26

d) NIST stands for:

i) National Institute of Science and Technology
ii) National Institute of Standardized Technology
iii) National Institute of Standards and Technology
iv) National Institute of Science and Technology Research

e) The encryption formula in RSA-cryptosystem is:

i) $M = C^e (\mod n)$
ii) $C = M^d (\mod n)$
iii) $C = M^e (\mod n)$
iv) $M = C^d (\mod n)$

2. Write very short answer for each of the following: $2 \times 7 = 14$

a) Define a stream cipher.

b) Write the difference between hieroglyph and petroglyph.

c) Define cryptographic hash function.

d) What do you mean by Discrete Logarithmic Problem?

e) Define order of an integer modulo n and primitive roots.

f) What do you mean by Cryptology?

g) Using Caesar cipher, encrypt the message 'TURN BACK'.

3. Write short answers for each of the following: $3 \times 7 = 21$

a) Show that 2 and 3 are primitive roots of 5.

b) What is the difference between asymmetric and symmetric encryption?

c) 'WE ARE DISCOVERED FLEE AT ONCE' is the message. Transform it into 'rail fence' and write the encrypted message.

d) Show that the linear congruence $ax \equiv b \bmod n$ is solvable if and only if $d|b$, where $d = \gcd(a,n)$.

e) Write three important threats of email.

f) If $N = 25217$ is a product of two primes, where $N = 159^2 - 8^2$, find the two prime numbers.

g) Discuss briefly the RSA algorithm.

4. Answer any six of the following: $4 \times 6 = 24$

a) Explain the four basic conditions of a field.

b) Show that the linear congruence $9x \equiv 6 \pmod{12}$ is solvable and it has 3 incongruent solutions.

c) Using the random sequence of $\{0,1\}$ by flipping a coin in a one-time pad, encipher the message: 'THEMESSAGEISFAKED'. Consider the sequence obtained by flipping a coin as: 010011111001000010.

d) How will you factorize a big number into two primes? Factorize 41989 into two primes.

e) If $p = 19$, $g = 3$, and Alice's secret $a = 5$, Bob's secret $b = 7$, develop a key exchange between Alice and Bob using the Diffie-Hellman Key Exchange.

f) How can a hash function be used in a digital signature? Illustrate in a simplified way.

g) Write the algorithm of Schnorr digital signature scheme.

5. Answer any two of the following: $6 \times 2 = 12$

a) Define Caesar cipher. Write the digital encryption of the statement: "THE POLITICAL STATUS IS CONFUSED" using Caesar cipher.

b) What do you mean by Playfair Cipher? Construct the matrix with the key MONARCHY. And encrypt the word QUESTIONNAIRE by using the proper algorithm.

c) Encrypt the message 'BOOKS ARE DIVINITY' using the Hill cipher with the key $\begin{pmatrix} 5 & 1 \\ 2 & 7 \end{pmatrix}$. Show your calculations and the result.

6. Answer any two of the following: $6 \times 2 = 12$

a) State and prove Fermat's theorem.

b) Solve the simultaneous congruences: $x \equiv 3 \pmod 4$, $x \equiv 1 \pmod 5$, and $x \equiv 3 \pmod 7$. Find the value of x by using the Chinese Remainder Theorem.

c) Consider F_{2^8} with irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ and also consider two polynomials
$f(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^7 + x + 1$.
Find $f(x) + g(x)$ and perform $f(x).g(x) \bmod m(x)$.

7. Answer any two of the following: $6 \times 2 = 12$

a) If the plaintext message is $M = 8$ in a public-key cryptosystem using the RSA-algorithm. perform encryption and decryption where, $p = 7$, $q = 11$, and $e = 17$.

b) If E be the elliptic curve such that $E : y^2 = x^3 + x + 1$ defined over F_{23} . Perform the point addition for the two points $P = (x_1, y_1) = (1, 7)$ and $Q = (x_2, y_2) = (3, 10)$.

c) What is the email infrastructure architecture? Describe the five structures of an email.

****