No. of Printed Pages : **4**

Sl. No.

C8-R4 : INFORMATION SECURITY

DURATION : 03 Hours **MAXIMUM MARKS : 100**

Roll No. : | | | | | | |

Answer Sheet No. : | | | | | | |

Name of Candidate : _____ **; Signature of Candidate :** _____

INSTRUCTIONS FOR CANDIDATES :

- Carefully read the instructions given on Question Paper, Answer Sheet.
- Question Paper is in English language. Candidate has to answer in English Language only.
- **Question paper contains Seven questions. The Question No. 1 is compulsory. Attempt any FOUR Questions from Question No. 2 to 7.**
- **Parts of the same question should be answered together and in the same sequence.**
- **Questions are** to be answered in the **ANSWER SHEET** only, supplied with the Question Paper.
- **Candidate cannot leave the examination hall/ room without signing on the attendance sheet and handing over his/her Answer Sheet to the Invigilator. Failing in doing so, will amount to disqualification of Candidate in this Module/Paper.**
- After receiving the instruction to open the booklet and before answering the questions, the candidate should ensure that the Question Booklet is complete in all respects.

DO NOT OPEN THE QUESTION BOOKLET UNTIL YOU ARE TOLD TO DO SO.

1. (a) Explain the Vigenere Cipher and its advantage over the Shift Cipher. Give one example.

(b) Explain the following terms :

(i) ElGamal encryption process.

(ii) Authenticated Encryption.

(c) Explain the working of a Pseudo-Random Number Generator (PRNG). How does it differ from a true random number generator (TRNG) ?

(d) Differentiate between steganography and cryptography in cyber security.

(e) What is the purpose of the S-boxes in DES? How do S-Boxes Work in DES ?

(f) What is the Chinese Remainder Theorem ? Solve $x \equiv 2(\text{mod}3)$ and $x \equiv 3(\text{mod } 5)$.

(g) Explain the significance of statistical tests in evaluating the quality of random number generators.

(7x4)

2. (a) How does AES in ECB (Electronic Codebook) mode differ from CBC (Cipher Block Chaining) mode ?

(b) List and briefly define categories of security services.

(c) Explain the Digital Signature Standard (DSS) and list its main digital signature algorithms. How does Elliptic Curve Digital Signature Algorithm improve over traditional DSA and RSA ?

(6+6+6)

3. (a) Define Message Authentication Code (MAC) and its role. Identify and briefly describe two common MAC algorithms. Why is HMAC preferred over a basic hash function for message authentication ?

(b) Find the gcd of the given polynomial :

$a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$.

(c) Explain the purpose of statistical tests in cryptography and describe two common statistical tests used to evaluate randomness.

(d) Compare DES, 3DES, and AES based on Key Size, Block Size, Number of Rounds, Encryption Mechanism, Security Strength, and Performance Efficiency.

(6+6+4+2)

4. (a) How does the ShiftRows operation work in AES ?

(b) Given an RSA algorithm where $p = 13$, $q = 5$, and $e = 7$, what are the values of d (the private key exponent) and the ciphertext for the plaintext message '6' using the public key (e, n) ?

(c) Explain the Next-bit Test and its significance in cryptographic security. How does it help in evaluating Pseudo-Random Number Generators (PRNGs) ?

(6+8+4)

5. (a) Given 2 as a primitive root of 29, construct a table of discrete logarithms and use it to solve the following congruences.

(i) $17x^2 \equiv 10 \pmod{29}$

(ii) $x^2 - 4x - 16 \equiv 0 \pmod{29}$

(b) How do digital signatures ensure message integrity? Explain the role of cryptographic hash functions in maintaining integrity. What happens if the message is altered during transmission ?

(c) Explain the Birthday Attack in cryptography. How does it impact the security of hash functions ? Provide an example of birthday attack.

(6+6+6)

6. (a) Consider a Diffie-Hellman scheme with a common prime $q = 13$, and a primitive root $\alpha = 7$.

(i) Show that 7 is a primitive root of 13.

(ii) If Alice has a public key $Y_A = 5$, what is Alice's private key X_A ?

(iii) If Bob has a public key $Y_B = 12$, what is the secret key shared with Alice ?

(b) Consider a Blum-Blum-Shub (BBS) generator with the following parameters :

- Two large prime numbers : $p = 11$ and $q = 19$
- The initial seed $x_0 = 2$

Generate the first 5 bits of the random sequence using the BBS algorithm.

(9+9)

7. (a) Explain the working of SHA-256 in detail. How does it ensure collision resistance ?

(b) What is a digital signature ? List and explain three common attacks on digital signature. Explain how it works with the help of a cryptographic algorithm.

(c) Define the following with one example of each.

(i) finite field GF (p).

(ii) Fermat's Little Theorem.

(7+7+4)

- o O o -

SPACE FOR ROUGH WORK