| U.S.N. | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|

# B.M.S. College of Engineering, Bengaluru-560019

**Autonomous Institute Affiliated to VTU**

## July 2023 Semester End Main Examinations

**Programme: B.E.** **Semester: VI**
**Branch: Computer Science and Engineering** **Duration: 3 hrs.**
**Course Code: 20CS6PCCNS** **Max Marks: 100**
**Course: Cryptography and Network Security** **Date: 10.07.2023**

**Instructions**: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

**Important Note:** Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

| | | | UNIT - I | *CO* | *PO* | Marks |
|---|---|---|---|---|---|---|
| 1 | a) | | With the help of a neat diagram, list different types of security attacks. | *CO2* | *PO2* | **6** |
| | b) | | Apply Extended Euclidean algorithm to find the inverse of 12 modulo 79. | *CO1* | *PO1* | **6** |
| | c) | | Given that $Z_7 = \{1, 2, 3, 4, 5, 6\}$ * mod 7 is a group, write all the cyclic subgroups of different orders of $Z_7$. Is $Z_7$ a cyclic group? | *CO1* | *PO1* | **8** |
| | | | **OR** | | | |
| 2 | a) | | Analyze how secure communication is achieved using Shannon's perfect secrecy. List the requirements for achieving perfect secrecy according to Shannon's theory. | *CO2* | *PO2* | **7** |
| | b) | | Briefly explain the following terms:<br>i) Choosen Message Attack (CMA)<br>ii) Choosen Plain Text Attack (CPA)<br>iii) Choosen Cyber Text Attack (CCA) | *CO1* | *PO1* | **6** |
| | c) | | Show how to multiply $(x^3 + x^2 + x + 1)$ by $(x^2 + 1)$ in GF($2^4$) using the efficient algorithm for multiplication using irreducible polynomial:$(x^4 + x^3 + 1)$. | *CO1* | *PO1* | **7** |
| | | | **UNIT - II** | | | |
| 3 | a) | | Distinguish between Block ciphers and Stream ciphers. | *CO2* | *PO2* | **6** |
| | b) | | Analyze the process of AES encryption algorithm with a neat diagram. | *CO2* | *PO2* | **8** |
| | c) | | Compare the following with respect to AES and DES:<br>i) Substitution<br>ii) Permutation<br>iii) Round key | *CO2* | *PO2* | **6** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | **UNIT - III** | | | |
| | 4 | a) | Apply Chinese Remainder theorem to solve the following congruent equations:<br>$x_1 \equiv 3 \bmod 5$<br>$x_2 \equiv 5 \bmod 6$<br>$x_3 \equiv 2 \bmod 7$ | *CO1* | *PO1* | **8** |
| | | b) | Apply Fermat's Little theorem to find the values for the following:<br>i) $5^{15} \bmod 13$<br>ii) $15^{18} \bmod 17$ | *CO1* | *PO1* | **6** |
| | | c) | Apply Miller Rabin primality testing and check if the following numbers are prime or not:<br>i) 201<br>ii) 341 | *CO1* | *PO1* | **6** |
| | | | **UNIT - IV** | | | |
| | 5 | a) | Illustrate Diffie-Hellman key exchange algorithm with example. | *CO3* | *PO3* | **7** |
| | | b) | Explain ElGamal encryption. A block of plaintext has been encrypted using ElGamal encryption. Assume that p=131, g=2 and the recipient's public key=97, What is the plain text corresponding to the ciphertext C1=103 and C2=51. | *CO3* | *PO3* | **8** |
| | | c) | Demonstrate cycling attack on RSA algorithm with an example. | *CO3* | *PO3* | **5** |
| | | | **OR** | | | |
| | 6 | a) | With the help of a neat diagram, explain Elliptic curve arithmetic rules with an example. | *CO3* | *PO3* | **8** |
| | | b) | Consider RSA encryption scheme with public key N=55 and e=3. Suppose the encryption of an unknown message m=6, find the encrypted value of 2m mod N. | *CO3* | *PO3* | **6** |
| | | c) | Perform encryption and decryption using RSA if p=7, q=11, e=13 and Message/Plain text=5. | *CO3* | *PO3* | **6** |
| | | | **UNIT - V** | | | |
| | 7 | a) | Analyze how cryptographic hash can be used for Digital signature generation. | *CO2* | *PO2* | **6** |
| | | b) | Compare and contrast a conventional signature and a digital signature. | *CO2* | *PO2* | **6** |
| | | c) | Discuss the idea behind RSA digital signature scheme with a neat diagram. | *CO2* | *PO2* | **8** |



**********