U.S.N. □□□□□□□□□□

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

Autonomous Institute Affiliated to VTU

August 2022 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: 14.08.2022**

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

UNIT - I

1 a) Explain the taxonomy of attacks with relation to security goals with a neat block diagram. **8**

b) Explain cryptanalysis attacks with an example for each. **8**

c) Eve has intercepted the cipher text **"UVACLYFZLJBYL"**. Show how she can use brute-force attack to break the cipher. **4**

OR

2 a) Explain keyless transposition ciphers and keyed transposition ciphers with an example for each. **8**

b) Explain groups with an example. **8**

c) Perform the polynomial division given below. **4**
$(6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3) \div (x^5 + 3x^3 + 4)$

UNIT - II

3 a) Write about modern block ciphers and modern stream ciphers. **6**

b) Create a linear feedback shift register with four cells in which $b4 = b1 \oplus b0$. If the seed is $(1110)_2$, Show the transitions involved in 10 states. **6**

c) Explain the general structure of DES. **4**

d) Explain Shift Rows operation used in AES algorithm with an example. **4**

UNIT - III

4 a) State the Chinese Remainder Theorem and find X for the given set of congruent equations **8**
X≡4 mod 5,
X≡10 mod 11.

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.

b) Explain quadratic residues and solve the following congruence using the same **8**

i) $x^2 \equiv 4 \bmod 7$

ii) $x^2 \equiv 5 \bmod 11$

c) Explain Legendre symbol in brief. **4**

UNIT - IV

5 a) Explain locking and unlocking in asymmetric-key cryptosystem with an example. Also explain trapdoor one-way function **10**

b) In the Diffie-Hellman protocol, $g = 7$, $p = 23$, $x = 3$, and $y = 6$. **10**

i) Calculate the value of the symmetric key?

ii) Calculate the value of R1(Sender's public key) and R2(Receiver's public key)

iii) Consider the above values for Alice and Bob. Demonstrate Man in the middle attack with your own values used by Eve.

OR

6 a) Explain the taxonomy of potential attacks on RSA. **10**

b) In ElGamal cryptosystem, given the prime $p = 31$. Clearly show all the steps involved in encryption and decryption. **10**

i. Choose an appropriate values for e_1 and d, then calculate e2.

ii. Encrypt the message "HELLMAN". Use 00 to 25 for encoding. Use different blocks to make $P < p$.

iii. Decrypt the ciphertext to obtain the plaintext.

UNIT - V

7 a) Explain RSA digital signature scheme with a diagram **10**

b) Illustrate the working of Merkle-Damgard scheme with neat diagram. **4**

c) Compare and contrast a conventional signature and a digital signature. **6**

******