U.S.N.										

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

Autonomous Institute Affiliated to VTU

September / October 2023 Supplementary 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

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) List and define five security services. **6**

b) Analyze the type of security attack in each of the following cases: **6**

i) An employee breaks into manager's office to obtain a copy of confidential data.

ii) A student gives a cheque for \$10 to buy a used book. Later she finds that the cheque was cashed for \$100.

iii) A student sends hundreds of e-mails per day to another student using a phony return e-mail address.

c) Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$. Note that we use the symbol $\otimes$ to show the multiplication of two polynomials. **4**

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

OR

2 a) Explain RC4 showing the idea of this stream cipher with a figure. **6**

b) Demonstrate with a suitable example how monoalphabetic substitution cipher is vulnerable to frequency analysis attack. **6**

c) Given a = 161 and b = 28, find gcd (a, b) using Extended Euclidean algorithm and the values of s and t. **4**

d) Use the Vigenere cipher with keyword "**health**" to encipher the message "life is full of surprises". **4**

UNIT - II

3 a) Draw and explain ShiftRows transformation in AES with an example **6**

b) Draw the P-box with the following permutation table and analyze the type of the same **6**

i) P-Box (8 inputs) - O/P : 8 1 2 3 4 5 6 7

ii) P-Box (7 inputs) - O/P : 1 3 5 6 7

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.

c) Write pseudocode for the split and exclusiveOr routines used in DES cipher with the following signatures. **8**

i) split (n, m, inBlock[n], leftBlock[m], rightBlock[m])
ii) exclusiveOr (n, firstInBlock[n], secondInBlock[n], outBlock[n])

UNIT - III

4 a) Using quadratic residues, solve the following congruences: **6**
i) $x^2 \equiv 4 \bmod 7$
ii) $x^2 \equiv 5 \bmod 11$

b) Apply Euler's theorem to find the multiplicative inverse of the following: **6**
i) $12^{-1} \bmod 77$
ii) $16^{-1} \bmod 323$

c) Apply Chinese Remainder Theorem to find the integer x which leave a remainder of 6, 13, 9 and 19 when divided by 11, 16, 21 and 25 respectively. **8**

UNIT - IV

5 a) Write the procedure used for generating private and public keys and encryption in elliptic curve cryptography. **6**

b) Alice uses Bob's RSA public key (e = 7, n = 143) to send the plaintext P = 8 encrypted as ciphertext C = 57. Show how Eve can use the chosen-ciphertext attack if she has access to Bob's computer to find the plaintext. **6**

c) In ElGamal, given the prime p = 31 **8**
i) Choose an appropriate e1 and d, then calculate e2.
ii) Encrypt the message "HELLO"; use 00 to 25 for encoding. Use different blocks to make P < p.
iii) Decrypt the ciphertext to obtain the plaintext.

OR

6 a) Explain the idea behind the RSA cryptosystem. **6**
i) What is the one-way function in this system?
ii) What is the trapdoor in this system?
iii) Define the public and private keys in this system

b) Assume that Alice uses Bob's ElGamal public key (e1 = 2 and e2 = 8) to send two messages P = 17 and P′ = 37 using the same random integer r = 9. Eve intercepts the ciphertext and somehow, she finds the value of P = 17. Show how Eve can use a known-plaintext attack to find the value of P′. **6**

c) In the Diffie-Hellman protocol, g = 7, p = 23, x = 3, and y = 6. **8**
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.

UNIT - V

7 a) Discuss the influence of preimage resistance on the attacks on RSA signed digests. **6**

b) With a neat diagram, explain HMAC. **6**

c) Using the RSA Digital Signature scheme, let p = 809, q = 751 and d = 23. Calculate the public key e. Then do the following: **8**

i) Sign and verify a message with M1 = 100 Calculate the signature S1.

ii) Sign and verify a message with M2 = 50. Calculate the signature S2.

iii) Show that if M = M1 × M2, then S = S1 × S2.

****