05/01/2024 - FN

Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 20336

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2023.

Fifth Semester

Computer Science and Engineering

CB 3491 – CRYPTOGRAPHY AND CYBER SECURITY

(Common to : Computer Science and Engineering (Artificial Intelligence and Machines Learning) and Computer and Communication Engineering)

(Regulations – 2021)

Time : Three hours | Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Encrypt the plain text "miss Carlet with the knife in the library" with the key = 3201 using row Transposition technique.

2. Differentiate between an unconditionally secure cipher and a Computationally secure cipher.

3. In AES, how the encryption key is expanded to produce keys for the 10 rounds?

4. What are the properties hold by a good random number generator?

5. Does Fermet's theorem hold for p = 5 and a = 2? Justify.

6. What is Message Authentication Code? How it differ from Hash function?

7. List the applications of X.509 Certificate.

8. Write the schemes for the distribution of public keys.

9. How to prevent SQL Injection Attacks?

10. What are the classifications of Cyber Crimes?

PART B — (5 × 13 = 65 marks)

11. (a) (i) Describe OSI security architecture and derive a relativity matrix between security, Attacks, Services, and Mechanisms. (8)

(ii) Using play fair cipher algorithm encrypt the plaintext = ATTACK POSTPONED using the key = EMERGENCY. (5)

Or

(b) Perform Encryption and Decryption on the plain text "CAT" using Hill Cipher with the Key K1.

$$K1 = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

12. (a) Perform SDES Encryption using the following

Plain text = 11000011; Key: 1010101101; P10: 3,5,1,7,9,2,6,4,8,10

P8: 3,2,6,5,8,7,1,4; E/P: 41232341; P4:4321; IP:1,3,8,7,6,4,5,2

Where

P10: permutation order for 10 bits

P8: permutation order for 8 bits

E/P: expansition permutation order

P4: permutation order for 4 bits

IP: Initial permuation order

S0, S1: substitution boxes

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \qquad S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

Or

(b) Explain Block cipher mode of operation: Electronic Code Book, Cipher Block Chaining and Counter mode with neat sketch.

13. (a) Determine the plaintext text from the cipher text C=106, N=143, e=11 using RSA algorithm.

Or

(b) Assume the client C (sender) wants to communicate with another client C1 (Receiver) using Diffie - Hellman procedure. How can it be achieved? Explain with numerical example.

14. (a) Write down the steps involved in Schnorr digital signature standard. Provide numerical example for the same.

Or

(b) What are the properties of Hash? Show how the 512 bit input message blocks are converted into 160 bit message digest using SHA-1 Algorithm?

15. (a) Discuss various security challenges in cloud computing and depict the complete Elgamal cryptosystem procedure in detail.

Or

(b) Explain various attacks on kerberos and depict how it could withstand from all such violations with neat sketch.

PART C — (1 × 15 = 15 marks)

16. (a) Alice and Bob exchange a shift cipher key using the Diffie-Hellman key exchange. They agree to use the prime p = 11 for their cyclic group Z_{11} and g = 7 as the generator.

(i) Assume Alice uses the secret value a=6 and Bob the secret value b=8. Compute the public values and the final key that Alice and Bob exchange.

(ii) Assume Alice and Bob exchange the values $X = g^a = 5 \bmod 11$ and $y = g^b = 10 \bmod 11$. Determine the secret key they both exchanged! Describe your computation steps to determine the key.

Or

(b) The ECC cryptosystem defined by $y^2 = x^3 + x + 6$ over F_{11} and $G = (2,7)$. B's secret key is 3. A wishes to encrypt the message Pm=(10, 9) and chooses the random value k=2. Find B's public key and determine the cipher text Cm.

———————