BE1431

Total No. of Printed Pages: 2

**B.E. - (Computer) (Sem - VIII) (Revised Course 2019-2020)**

**EXAMINATION DECEMBER 2023**

**Cryptography Techniques for Network Security**

**[Time: 3:00 Hours]** **[Max. Marks: 100]**

**Instructions: 1. Answer any two full questions from PART A, Answer any two full questions from PART B, and any one full question from Part C**

**2. Draw neat diagram wherever necessary**

**3. Assume Suitable data if required**

## PART A

| | | | |
|---|---|---|---|
| **Q1** | **a.** | Explain the different types of attacks that can be performed on Encrypted Messages | **(10)** |
| | **b.** | Prove asymmetric key encryption can be achieved using two prime numbers 7 & 11 | **(5)** |
| | **c.** | Explain in brief different types of Steganography Techniques | **(5)** |
| **Q2** | **a.** | If the Cipher text obtained is **oeochemmormworwot** in round 2, with a key of order 4,6,1,2,5,3 apply simple columnar transposition to get the plain text back. | **(10)** |
| | **b.** | With an appropriate diagram explain AES | **(10)** |
| **Q3** | **a.** | Illustrate man in the middle attack if Alice and Bob are using Diffie Hellman Key exchange algorithm & prefers to use value of n=11 & g=7 and Tom is a attacker using values x=8 & y=6, Alice using x=3 & Bob using y=9 | **(10)** |
| | **b.** | Encrypt using Hill cipher the plain text message "retreat now" using the key phrase "backup" and a 3*3 matrix | **(10)** |

BE1431

## PART B

| | | | |
|---|---|---|---|
| **Q4** | **a.** | Explain in detail SHA 512 | **(10)** |
| | **b.** | Explain the verification and the signing process of a Digital Signature | **(10)** |
| **Q5** | **a.** | Justify the use of Hash function in a Digital Signature | **(5)** |
| | **b.** | Explain the process of exchange of public key certificates | **(5)** |
| | **c.** | Write a note on the functions and Cryptographic algorithms supported by S/MIME | **(10)** |
| **Q6** | **a.** | With a neat diagram explain MAC based on Hash function (HMAC) | **(10)** |
| | **b.** | Explain X.509 certificate format | **(5)** |
| | **c.** | State the applications of Cryptographic hash functions | **(5)** |

## PART C

| | | | |
|---|---|---|---|
| **Q7** | **a.** | Explain the Encryption and decryption process of DES | **(10)** |
| | **b.** | Explain different types of Block cipher modes | **(10)** |
| **Q8** | **a.** | Explain the following with respect to Kerberos version 4 | **(10)** |
| | | i. Authentication service Exchange to obtain ticket-granting ticket | |
| | | ii. Ticket granting service exchange to obtain service granting ticket | |
| | | iii. Client/Server Authentication exchange to obtain service | |
| | **b.** | Explain the process of PGP Message Generation and Reception | **(10)** |