PAPER ID-310323

Roll No: | | | | | | | | | | | | | |

**BTECH**
**(SEM VII) THEORY EXAMINATION 2023-24**
**CRYPTOGRAPHY AND NETWORK SECURITY**

**TIME: 3 HRS** **M.MARKS: 100**

**Note: 1.** Attempt all Sections. If require any missing data; then choose suitably.

## SECTION A

**1. Attempt *all* questions in brief.** **2 x 10 = 20**

| Q no. | Question | Marks |
|---|---|---|
| a. | Define steganography with example. | 2 |
| b. | Explain cryptanalysis. | 2 |
| c. | Compute GCD (24120,1640) using Euclid's algorithm. | 2 |
| d. | Find all primitive roots of 13. | 2 |
| e. | Explain birthday attack. | 2 |
| f. | Write the services provided by digital signature. | 2 |
| g. | Define X.509 certificates. | 2 |
| h. | List the any four services provided by Pretty good privacy. | 2 |
| i. | Discuss intrusion detection. | 2 |
| j. | Explain firewall and its usage. | 2 |

## SECTION B

**2. Attempt any *three* of the following:**

| | | |
|---|---|---|
| a. | Discuss the working of DES in detail with suitable diagram. | 10 |
| b. | Explain RSA algorithm with suitable steps. Let p= 17, q=11, e=7 and d=23. Calculate the public key & private key and show encryption and decryption for plain text M= 77 by using RSA algorithm. | 10 |
| c. | Explain Digital Signature. Discuss signing & verifying process of Digital Signature Algorithm (DSA) in detail with suitable steps. | 10 |
| d. | Discuss Diffie-Hellman key exchange in detail with suitable diagram. | 10 |
| e. | Explain secure electronic transaction (SET) protocol with suitable diagram. | 10 |

## SECTION C

**3. Attempt any *one* part of the following:** **10 x 3= 30**

| | | |
|---|---|---|
| a. | Discuss cryptography and its types with suitable example. | 10 |
| b. | Define block cipher. Also discuss any two block cipher modes of operation with advantages and disadvantages of each with block diagram. | 10 |

**4. Attempt any *one* part of the following:** **10 x 1= 10**

| | | |
|---|---|---|
| a. | State and prove Fermat's theorem. Use Fermat theorem to find a number 'a' between0 and 72 with a≡9794 mod 73. | 10 |
| b. | State Chinese remainder theorem (CRT). Solve the following congruent equations by CRT<br>i. X=2 mod 3<br>ii. X=3 mod 5 | 10 |

PAPER ID-310323

Roll No: | | | | | | | | | | | | | |

**BTECH**
**(SEM VII) THEORY EXAMINATION 2023-24**
**CRYPTOGRAPHY AND NETWORK SECURITY**

**TIME: 3 HRS** **M.MARKS: 100**

**5. Attempt any *one* part of the following: 10 x 1= 10**

| | | |
|---|---|---|
| a. | Discuss message authentication code (MAC).Also give the use of authentication requirement in MAC. | 10 |
| b. | Explain Hash Function. Discuss SHA- 512 with all required steps, round function with block diagram. | 10 |

**6. Attempt any *one* part of the following: 10 x 1= 10**

| | | |
|---|---|---|
| a. | Explain Kerberos protocol for key distribution with suitable diagram. | 10 |
| b. | Discuss X.509 certificates in detail. Write the role of X.509 certificates in cryptography. | 10 |

**7. Attempt any *one* part of the following: 10 x 1= 10**

| | | |
|---|---|---|
| a. | Discuss authentication header and encapsulating security payload in detail with packet format. | 10 |
| b. | Explain working of intrusion detection system (IDS) and its types with suitable diagram. | 10 |