PAPER ID-310050

Subject Code: KCS074

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

BTECH
(SEM VII) THEORY EXAMINATION 2024-25
CRYPTOGRAPHY AND NETWORK SECURITY

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

Note: Attempt all Sections. In case of any missing data; choose suitably.

SECTION A

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

Q no.	Question	CO	Level
a.	Outline the key principles of security.	1	K1
b.	Distinguish between active and passive attacks.	1	K2
c.	Determine GCD of (1970, 1066) using Euclid's algorithm.	2	K3
d.	Compute Φ(55).	2	K3
e.	Discuss Public Key Infrastructure (PKI).	3	K2
f.	Explain Birthday attack	3	K2
g.	Explain E-mail security.	4	K2
h.	List out some functions of PGP.	4	K1
i.	Differentiate transport and tunnel mode in IPsec.	5	K2
j.	Distinguish between Logic Bomb and Trojan Horse	5	K2

SECTION B

2. Attempt any *three* of the following: **10 x 3 = 20**

Q no.	Question	CO	Level
a.	Illustrate Substitution techniques and Transposition techniques under classical encryption.	1	K4
b.	Explain the Advanced Encryption Standard (AES) algorithm, providing a clear diagram that illustrates its architecture.	2	K2
c.	Illustrate the idea of Digital Signature for authentication. Discuss signing & verifying process of Digital Signature Algorithm (DSA) in detail with suitable steps.	3	K4
d.	Explain the full-service Kerberos environment. Determine the principal differences between version 4 and version 5 of Kerberos.	4	K2
e.	Explain the concept of IP security. Explain the role of AH and ESP.	5	K2

SECTION C

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

Q no.	Question	CO	Level
a.	Illustrate the DES algorithm with the help of block diagram. List the strength of DES. Discuss the requirement of Double and Triple DES.	1	K4
b.	Explain Vigenère cipher and encrypt the following message "Life is full of surprises" using the key – "HEALTH".	1	K4

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

Q no.	Question	CO	Level
a.	Compute the multiplicative inverse of 11 mod 26. Also state the Extended Euclidian Algorithm.	2	K3
b.	Apply Miller-Rabin primality test to test the primality of the number n=37. Write the pseudo code for Miller Rabin primality testing.	2	K3

Subject Code: KCS074

PAPER ID-310050

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

BTECH
(SEM VII) THEORY EXAMINATION 2024-25
CRYPTOGRAPHY AND NETWORK SECURITY

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

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

Q no.	Question	CO	Level
a.	Explain the concept of MAC. Discuss the working of MAC with suitable block diagram.	3	K2
b.	Discuss SHA- 512 with all required steps, round function & block diagram.	3	K2

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

Q no.	Question	CO	Level
a.	Determine the role of X.509 certificate in cryptography. Discuss X.509 certificate in detail.	4	K3
b.	Illustrate the various services supported by S/MIME. Explain how S/MIME supports these services.	4	K3

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

Q no.	Question	CO	Level
a.	Discuss the concept of dual signature in context of Secure Electronic Transaction (SET). Briefly describe the sequence of events that are required for a SET transaction.	5	K2
b.	Discuss the difference between SSL connection and SSL session. Discuss SSL protocol architecture.	5	K2