Subject Code: BCS072

PAPER ID-310993

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

BTECH
(SEM VII) THEORY EXAMINATION 2025-26
CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 70**

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

SECTION A

1. Attempt *all* questions in brief. **2 x 7 = 14**

Q no.	Question	Marks	CO
a.	Compare steganography and Cryptography.	2	1
b.	State Chinese remainder theorem.	2	2
c.	Calculate Φ(35).	2	2
d.	Explain requirement of Hashing.	2	3
e.	List the function of dual signature.	2	4
f.	Write role of TGS.	2	4
g.	Write requirement of padding in ESP.	2	5

SECTION B

2. Attempt any *three* of the following: **7 x 3 = 21**

a.	Discuss Shannon's theory of confusion and diffusion. Explain.	7	1
b.	Write algorithm for primality test. How it works.	7	2
c.	State and proof digital signature standard (DSS).	7	3
d.	Compare Kerberos 4 and Kerberos 5.	7	4
e.	Explain IP security. Explain its architecture.	7	5

SECTION C

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

a.	Compare and contrast Output Feedback (OFB) and Counter mode of Block cipher.	7	1
b.	List and explain security mechanisms.	7	1

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

a.	State and prove Euler's theorem.	7	2
b.	Explain the structure single round of AES.	7	2

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

a.	Explain Hash Function? Discuss SHA- 512 with all required steps, round function & block diagram.	7	3
b.	Discuss the Message Authentication Codes. Also give the use of Authentication requirements in MAC.	7	3

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

a.	Explain Diffie-Hellman key exchange algorithm with example.	7	4
b.	Explain X.509 certificate.	7	4

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

a.	Explain the following: (i) Intrusion detection. (ii) Firewall.	7	5
b.	Explain the sequence of steps used in Secure Socket Layer Handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol.	7	5