



Roll No:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

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

TIME: 3 HRS

M.MARKS: 70

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

SECTION A

1. Attempt all questions in brief.

02 x 7 = 14

Q no.	Question	CO	Level
a.	Define cryptography and state any two security services.	1	K1
b.	What is the difference between stream cipher and block cipher?	1	K2
c.	State Fermat's Little Theorem.	1	K1
d.	What is the purpose of a digital signature?	2	K2
e.	What is Diffie-Hellman key exchange used for?	2	K2
f.	Define Public Key Infrastructure (PKI)	2	K2
g.	Mention any two functions of a firewall.	5	K2

SECTION B

2. Attempt any three of the following:

07 x 3 = 21

a.	Explain substitution and transposition ciphers with suitable examples.	1	K2
b.	Explain modular arithmetic and Extended Euclidean Algorithm with example.	1	K3
c.	Explain authentication requirements and hash functions. Discuss birthday attack.	2	K4
d.	Explain symmetric key distribution methods and Diffie-Hellman key exchange.	2	K3
e.	Explain IP Security architecture and its components.	5	K2

SECTION C

3. Attempt any one part of the following:

07 x 1 = 07

a.	Describe the Feistel structure and explain the working of DES.	1	K3
b.	Discuss block cipher modes of operation and explain Triple DES.	1	K4

4. Attempt any one part of the following:

07 x 1 = 07

a.	Describe the AES encryption and decryption process.	1	K3
b.	Explain RSA algorithm along with its security considerations.	1	K4

5. Attempt any one part of the following:

07 x 1 = 07

a.	Describe Secure Hash Algorithm (SHA) and its security features.	2	K2
b.	Explain ElGamal Digital Signature technique and Digital Signature Standard (DSS).	2	K3

6. Attempt any one part of the following:

07 x 1 = 07

a.	Describe X.509 certificates and Public Key Infrastructure (PKI).	2	K2
b.	Explain Kerberos authentication protocol and electronic mail security using PGP.	2	K4

7. Attempt any one part of the following:

07 x 1 = 07

a.	Describe SSL and Secure Electronic Transaction (SET).	5	K3
b.	Discuss intrusion detection systems, viruses, and the role of firewalls in network security.	5	K6