



Roll No:

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

**BTECH-HONOURS  
(SEM V) THEORY EXAMINATION 2024-25  
DATA ENCRYPTION AND COMPRESSION**

**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.	Discuss the need of IT security.	1	K1
b.	Elaborate CIA triangle as the principle of security.	1	K2
c.	Differentiate active and passive attacks with suitable example.	1	K3
d.	Define the encryption and decryption process.	2	K1
e.	Differentiate digital signature and physical signature.	2	K2
f.	Show the process of message authentication with suitable example.	2	K3
g.	Define IP spoofing with example.	3	K2
h.	Demonstrate the importance of key management in cryptography.	3	K1
i.	Illustrate the techniques used in data compression.	4	K2
j.	Describe the significance of compression ratio.	4	K3

**SECTION B****2. Attempt any three of the following:****10 x 3 = 30**

Q no.	Question	CO	Level
a.	Elaborate substitution cipher and transposition cipher with suitable examples.	1	K3
b.	Differentiate private key cryptography and public key cryptography with suitable examples.	2	K3
c.	Demonstrate the function of firewall and discuss various types of firewalls.	3	K3
d.	Discuss Huffman coding for data compression. Given a message M of 100 characters where frequencies of each character are a=50, b=10, c=30, d=5, e=3, f=2. Find the Huffman code and number of bits required to store this message	4	K3
e.	Explain the working of knapsack encryption algorithm with suitable example.	2	K2

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

Q no.	Question	CO	Level
a.	Describe the types of DoS attack with suitable examples.	1	K2
b.	Elaborate the various security techniques used to protect the data and digital resources.	1	K1



Roll No:

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

**BTECH-HONOURS**  
**(SEM V) THEORY EXAMINATION 2024-25**  
**DATA ENCRYPTION AND COMPRESSION**

**TIME: 3 HRS****M.MARKS: 100****4. Attempt any one part of the following: 10 x 1 = 10**

Q no.	Question	CO	Level
a.	Write the steps of RSA encryption algorithm. In a RSA cryptosystem a particular A uses two prime numbers $p=13$ and $q=17$ to generate his public key. If the public key of A is 35. Find the private key of A.	2	K2
b.	Explain the function of IDEA encryption algorithm with suitable diagram.	2	K3

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

Q no.	Question	CO	Level
a.	Take a suitable example and explain the arithmetic coding technique of data compression.	3	K3
b.	Discuss the various techniques used for lossless and lossy data compression.	3	K3

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

Q no.	Question	CO	Level
a.	Show the working of DES and AES algorithm with well labeled diagram.	4	K3
b.	Describe the steps of Lempel-Ziv encoding technique of data compression with suitable example.	4	K3

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

Q no.	Question	CO	Level
a.	Explain the architecture of digital signature by taking suitable example.	2	K2
b.	Demonstrate the working of cryptographic hash function. Also discuss MD5 and SHA-1.	2	K3