Subject Code: HTCS401

PAPER ID-410934

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

BTECH-HONS
(SEM IV) THEORY EXAMINATION 2023-24
INFORMATION THEORY FOR CYBER 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	CO
a.	Explain the provable security in the context of cryptographic systems.	02	
b.	Define the term 'entropy' in the context of information theory.	02	
c.	Explain the concept of perfect secrecy.	02	
d.	Explain the concept of unconditional security.	02	
e.	Provide examples of cryptographic systems that achieve information-theoretic security.	02	
f.	Describe the role of side information at receivers in secure communication systems.	02	
g.	How does strong secrecy differ from weak secrecy?	02	
h.	Provide examples of cryptographic schemes that achieve partial secrecy.	02	
i.	Explain the principles of digital forensics	02	
j.	Explain how PKI works.	02	

SECTION B

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

a.	Consider a source generating four symbols A,B,C,D with probabilities P(A)=0.4,P(B)=0.3,P(C)=0.2,P(D)=0.1. Calculate the entropy of the source. If we use a binary encoding scheme, what is the minimum average code length according to Shannon's entropy?	10	
b.	Describe the process of secret key agreement between two parties. Discuss the Diffie-Hellman key exchange protocol and provide a step-by-step numerical example.	10	
c.	Explain the Advanced Encryption Standard (AES). Describe its structure and key features. Provide a detailed example of the AES encryption process for a 128-bit block of plaintext.	10	
d.	Describe the rate-distortion theory for secrecy systems. Provide a detailed explanation of how it is used to optimize secure source coding.	10	
e.	Describe the concept of lightweight cryptography. Why is it important for resource-constrained environments? Provide examples of lightweight cryptographic algorithms and discuss their applications.	10	

SECTION C

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

a.	Define and explain Shannon’s entropy. How does it relate to the uncertainty of a random variable? Provide an example involving a discrete random variable with three possible outcomes to illustrate your explanation.	10	
b.	Consider a cryptographic system where the key size is 128 bits. Discuss the lower bounds on key size for secrecy and authentication. How does increasing the key size affect the security of the system?	10	

PAPER ID-410934

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

BTECH-HONS
(SEM IV) THEORY EXAMINATION 2023-24
INFORMATION THEORY FOR CYBER SECURITY

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

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

a.	Define randomized ciphers. Explain their role in enhancing the security of cryptographic systems. Provide an example of a randomized cipher and discuss its advantages and disadvantages.	10	
b.	Describe the Hamming and Lee metrics. How are they used to measure the distance between codewords in block codes? Provide an example involving a simple block code.	10	

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

a.	Discuss the concept of side-channel attacks. Provide examples of different types of side-channel attacks and explain how they can be mitigated in cryptographic systems.	10	
b.	Explain the concept of semantic security. How does it relate to the strength of a cryptographic system? Provide a detailed explanation with examples.	10	

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

a.	Discuss the principles of rate-distortion theory for secrecy systems. Explain how it is used to optimize secure source coding. Provide a detailed example.	10	
b.	Discuss the principles of distributed channel synthesis. Explain how it is used to achieve secure communication in distributed systems. Provide a detailed example.	10	

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

a.	Discuss the role of network forensics in investigating cybercrimes. Explain the process of capturing and analyzing network traffic to detect malicious activities. Provide an example of a network forensics investigation.	10	
b.	Explain the role of PKI in digital signatures. How do digital signatures work and what are their applications? Provide a detailed example involving the use of digital signatures in securing email communications.	10	