Hi-Tech Institute of Engineering & Technology

Department Of Computer Science

B.Tech. Subject Code: KCS-074H

Model Paper

(Sem – VII), THEORY EXAMINATION-2023-24,

Subject Name: Cryptography and Network Security

Time: 3 Hours *Total Marks: 100*

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

SECTION-A

1. Attempt all question in brief. 2x 10 = 20

Q. No	Question	Marks	CO
a.	**Explain active and passive attack.**	2	1
b.	**Apply the Caesar Cipher (p=D(3,C)) and Decrypt the cipher text "PHHW PH"**	2	2
c.	**Specify the benefits of IPSec.**	2	5
d.	**Find gcd(1970,1066) using Euclid's algorithm.**	2	2
e.	Distinguish between an active and passive attack.	2	1
f	What requirements should a digital signature scheme satisfy?	2	1
g	What do you mean by email security?	2	4
h	What is Kerberos?	2	4
i	Explain role of compression function in hash function.	2	3
j	Differentiate between public key and private key.	2	4

SECTION-B

2. Attempt any Three of the following: 10x3 =30

Q. No	Question	Marks	CO
a.	Describe RSA algorithm, encryption and decryption function. In RSA, given e=07 and n=3. Encrypt the message "ME" using 00 to 25 for letter A to Z.	10	2
b.	Define ring and field. Give an example of ring which is not a field.	10	2
c.	Analyze various types of virus and its counter measures.	10	5
d.	Explain symmetric and asymmetric cryptography with the help of diagrammatic representation. And how to symmetric cryptography is different from asymmetric cryptography.	10	4
e.	Write the pseudo code for Miller Rabin primality testing. Test whether 61 is prime or not using the same Miller Rabin test.	10	2

SECTION-C

3. Attempt any one **part of the following: 10x1 = 10**

Q.No	Question	Marks	CO
a.	What are the requirements of a Message Authentication code (MAC)? Discuss the logical structure, components and algorithmic steps of MD5 algorithm.	10	3
b.	Draw block diagram of DES encryption. Also, discuss the strengths of DES.	10	1

4. Attempt any one **part of the following: 1x10 = 10**

Q. No	Question	Marks	CO
a.	Explain the Chinese Remainder Theorem with example. How Chinese remainder theorem provide the security to online information sharing transactions.	10	2
b.	Explain the concept of Digital signature algorithm with key generation and verification in detail.	10	3

5. Attempt any one **part of the following:** **1x10 = 10**

Q. No	Question	Marks	CO
a.	Define Primality Test and also explain Miller Rabin Algorithm using base 2 to test whether the number 341 is composite or not?	10	2
b.	Explain AES algorithm. What is the difference between the AES decryption algorithm and the DES algorithm?	10	2

6. Attempt any one part of the following

Q.No	Question	Marks	CO
a.	Describe how Diffie-Hellman algorithm used for key exchange is vulnerable to man in middle attack? Determine the shared secret key in a Diffie-Hellman scheme with a common prime 71 and primitive root 7. Given private keys of the communicating parties A and B are 5 and 12 respectively.	10	4
b.	Explain the full service of Kerberos environment. What are the principle differences between version 4 and 5 of Kerberos?	10	4

7. Attempt any one part of the following

Q.No	Question	Marks	CO
a.	Explain Secure Electronic Transaction (SET) in internet protocol security in detail.	10	4
b.	What do you mean by system security? Also discuss viruses and related threats to system security?	10	5