CBCS SCHEME

USN □□□□□□□□□□ **17CS61**

Sixth Semester B.E. Degree Examination, June/July 2023

Cryptography Network Security and Cyber Law

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Module-1

1 a. Discuss common attacks on cyber security. **(10 Marks)**

b. Explain Extended Euclidean algorithm for computing the multiplicative inverse of a given integer mod n. Apply the same for evolving multiplicative inverse of 15 mod 26. **(06 Marks)**

c. Calculate the value of x, using CRT for the following congruent equations:

$x \equiv 3 \bmod 5$

$x \equiv 5 \bmod 6$

$x \equiv 2 \bmod 7$. **(04 Marks)**

OR

2 a. Discuss about Rings and Fields. **(08 Marks)**

b. Find the number of generators in the integer group $\langle Z_{17}^{*}, *_{17} \rangle$. **(02 Marks)**

c. Consider the following table where each letter is represented by a number modulo 26.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Apply encryption and decryption using Hill Cipher method, for the message block {Q, P} using the key matrix $K = \begin{bmatrix} D & H \\ P & M \end{bmatrix}$. **(04 Marks)**

d. With the relevant diagram, explain DES block cipher generation algorithm. **(06 Marks)**

Module-2

3 a. Describe the working of RSA algorithm apply RSA to encrypt the text message M. Consider p = 3, q = 7 and M = 0010100100. **(10 Marks)**

b. Write a short note on Birthday paradox. **(04 Marks)**

c. Explain HMAC algorithm. **(06 Marks)**

OR

4 a. Explain the construction of SHA-1 to generate MAC. **(10 Marks)**

b. Explain Diffie Hellman key exchange algorithm. Compute shared secret key 'K' between user-A and user-B when p = 13, g = 2, a = 7, b = 5. **(10 Marks)**

Module-3

5 a. Explain shared secret based mutual authentication. **(06 Marks)**

b. Illustrate SSL record layer protocol. **(04 Marks)**

c. Explain the working of Needham Schroeder protocol for authentication. **(10 Marks)**

OR

6 a. Explain KERBEROS authentication protocol. **(10 Marks)**

b. Explain IP security in tunnel and transport mode for AH and ESP. **(10 Marks)**

Module-4

7 a. Explain the working of WEP. Discuss its major drawbacks. **(10 Marks)**

b. Explain different types of intrusion detection systems. **(10 Marks)**

OR

8 a. Explain data protection mechanism in TKIP using 2-way key mixing. **(10 Marks)**

b. Explain following worm. Propagation models:

i) Simple Epidemic Model.

ii) Kermack-McKendrick Model. **(10 Marks)**

Module-5

9 a. What is Information Technology Act? Discuss its aims and objectives. **(10 Marks)**

b. Who is a controller? Outline his functions and powers. **(10 Marks)**

OR

10 a. Describe the provisions of the IT-Act as regards the following:

i) Legal recognition of electronic records.

ii) Publication rules in the electronic gazette. **(10 Marks)**

b. Describe the duties of subscribers. Discuss the penalties and adjudications under section 43 of IT-Act, 2000 for

i) Damage to computer or computers system etc.

ii) Failure to furnish information return. **(10 Marks)**

* * * * *