C.M.R. INSTITUTE OF TECHNOLOGY BANGALORE

CBCS SCHEME

USN □□□□□□□□□□

17CS61

Sixth Semester B.E. Degree Examination, Dec.2023/Jan.2024
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.

Module-1

1 a. Describe the main motives of launching cyber attacks. **(05 Marks)**

b. Describe the types of vulnerabilities to domain of security. **(05 Marks)**

c. Write the extended Euclidean algorithm. Use extended Euclidean algorithm to find inverse of 12 modulo 79. **(10 Marks)**

OR

2 a. Calculate the value of x using Chinese remainder theorem by given below data :
$N = 210$, $n_1 = 5$, $n_2 = 6$, $n_3 = 7$, $x_1 = 3$, $x_2 = 5$. $x_3 = 2$ **(06 Marks)**

b. Explain the Vigenere Cipher and the Hill Cipher techniques with illustration. **(06 Marks)**

c. With neat diagram, explain Fiestel structure. **(08 Marks)**

Module-2

3 a. Explain RSA algorithm with suitable example. **(10 Marks)**

b. Explain Public Key Cryptography Standard (PKCS). **(06 Marks)**

c. List the properties of cryptographic hash. **(04 Marks)**

OR

4 a. Explain the following :
(i) Hash-based MAC (ii) Digital signatures **(10 Marks)**

b. Explain Diffie-Hellman key exchange with an example. **(10 Marks)**

Module-3

5 a. Explain with neat diagram, different Public Key Infrastructure (PKI) architectures. **(10 Marks)**

b. Describe the Mutual Authentication using a shared secret. **(10 Marks)**

OR

6 a. Describe the IPsec protocols Authentication Header and Encapsulating Security Payload (ESP) in transport mode. **(10 Marks)**

b. Explain the following :
(i) SSL Record Layer protocol.
(ii) Open SSL **(10 Marks)**

Module-4

7 a. Explain the Authentication and Master Session key exchange in 802.11i with the help of diagram. **(10 Marks)**

b. List out and explain the different Worm characteristics. **(10 Marks)**

OR

8 a. Explain Firewall functionality and proxy fire wall. **(10 Marks)**

b. Explain the types of Intrusion Detection system. **(10 Marks)**

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.

VTU-13-02-2024 08:51:51am - CR - CR - CR - CR
13-02-2024 09:20:56am - CR - CR - CR - CR

Module-5

9 a. Explain the aim and objectives of IT Act. (06 Marks)

b. Define the following term with respect to IT Act 2000:

(i) Asymmetric crypto system

(ii) Certifying Authority (04 Marks)

c. Explain the important provisions of IT Act 2000 with regard to,

(i) Digital Signature

(ii) Legal recognition of Electronic Records.

(iii) Legal recognition of digital Signatures. (10 Marks)

CMRIT LIBRARY
BANGALORE - 560 037

OR

10 a. Briefly outline the any 10 functions of a controlles. (10 Marks)

b. Describe the duties of subscribes. (10 Marks)

* * * * *

VTU-13-02-2024 08:31:51am
CR - CR - CR - CR - CR - CR - CR - CR - CR
13-02-2024 09:20:56am
CR - CR - CR - CR - CR - CR - CR - CR - CR