CBCS SCHEME

USN | | | | | | | | | | |

15CS61

Sixth Semester B.E. Degree Examination, Feb./Mar. 2022
Cryptography, Network Security and Cyber Law

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Briefly discuss the defense strategies and techniques to prevent intrusions. **(06 Marks)**

b. What is Chinese remainder theorem? Explain. Further, compute f^{-1} (3, 5, 2), given N = 210, $n_1 = 5$, $n_2 = 6$, $n_3 = 7$ and $x_1 = 3$, $x_2 = 5$ and $x_3 = 2$ (compute x). **(10 Marks)**

OR

2 a. Define Hill Cipher. Consider a Hill Cipher using block size of 2 (m = 2). Calculate the Hill Cipher for a block and plaintext (H, I), given $K = \begin{pmatrix} 3 & 7 \\ 15 & 12 \end{pmatrix}$ **(08 Marks)**

b. With the help of a neat diagram explain the construction of DES. **(08 Marks)**

Module-2

3 a. Explain RSA algorithm with steps. Using RSA technique perform the encryption and decryption. For the given data: p = 3, q = 11, e = 3 and m = $(00111011)_2$. **(08 Marks)**

b. What do you mean by weak collision resistance and strong collision resistance? Discuss the attack complexity of both of these collision resistances. **(08 Marks)**

OR

4 a. With regard to cryptographic hash, explain the followings:
i) Hash-based MAC
ii) Digital signatures. **(08 Marks)**

b. Explain E_L Gamal Encryption. A block of plaintext has been encrypted using E_L Gamal encryption. Assume that p = 131, g = 2 and the recipients public key = 97. What is the plain text corresponding to the cipher text, $C_1 = 103$ and $C_2 = 51$? **(08 Marks)**

Module-3

5 a. What is Identity-based encryption? Explain the working of it. **(06 Marks)**

b. Write a note on certificate-based authentication. **(04 Marks)**

c. With the help of a diagram, discuss the sequence of messages exchanged between the client and Kerberos. **(06 Marks)**

OR

6 a. Briefly explain the Internet Key Exchange (IKE) protocol. Also discuss the various things accomplished in IKE phase 1. **(08 Marks)**

b. Show the sequence of messages and their contents involved in SSL handshake. **(08 Marks)**

Module-4

7 a. Write a note on E-mail worms. **(04 Marks)**

b. Briefly discuss the four main functions of a firewall. **(06 Marks)**

c. With a functional diagram indicate the tasks performed by an Intrusion Detection System (IDS). **(06 Marks)**

OR

8 a. What is SOAP? Briefly explain. **(04 Marks)**

b. With regard to web services security, discuss the followings:

i) WSDL and UDDI

ii) XML signatures

iii) SAML

iv) WS-Trust. **(12 Marks)**

Module-5

9 a. Enlist the objectives of IT Act. **(03 Marks)**

b. List any ten functions of the controller in IT Act. **(10 Marks)**

c. In which situations, the digital signature certificate is suspended? Briefly explain. **(03 Marks)**

OR

10 a. Discuss the penalties and adjudications under section 43 of the IT Act 2000 for damage to a computer, computer system etc. **(08 Marks)**

b. What is the punishment for cyber terrorism? Explain. **(04 Marks)**

c. As per IT Act, what is the constitution of advisory committee? Discuss. **(04 Marks)**

* * * * *