CBCS Scheme

USN | | | | | | | | | |

15CS61

Sixth Semester B.E. Degree Examination, June/July 2018
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. List and explain the various types of vulnerabilities with common cyber attacks. **(08 Marks)**
   b. Encrypt the plaintext "CRYPTOGRAPHY" using hill cipher technique with key matrix
   $$K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}.$$
   (08 Marks)

OR

2 a. Distinguish between :
   i) Confusion and diffusion ciphers
   ii) Block cipher and stream ciphers. **(08 Marks)**
   b. With a neat schematic, explain the single round of DES encryption model. **(08 Marks)**

Module-2

3 a. In a RSA system, it is given p = 3, q = 11, l = 7 and M = 5. Find the cipher text 'C' and also find message 'm' from decryption. **(08 Marks)**
   b. Define Hash function. Explain the construction of generic cryptographic Hash. **(08 Marks)**

OR

4 a. With a neat sketch, explain the process of computing Hash function using SHA – 1 algorithm. **(08 Marks)**
   b. Explain the working of Diffie–Hellman key exchange protocol. **(08 Marks)**

Module-3

5 a. What is digital certificate? Explain the X-509 digital certificate format. **(08 Marks)**
   b. Distinguish shared secret–based authentication and Asymmetric key–based authentication **(08 Marks)**

OR

6 a. Assume a client 'C' wants to communicate with server 'S' using Kerberos protocol. How can it be achieved? **(08 Marks)**
   b. What is secure socket layer? Explain SSL Handshake protocol. **(08 Marks)**

Module-4

7   a.   What is intrusion detection system (IDS)? Explain different types of IDS.   (06 Mark

      b.   Explain how 802.11i provides message confidentiality and integrity.   (06 Mark

      c.   Explain the characteristics of virus and worm.   (04 Mark

OR

8   a.   What is WS-security? Explain the various types of WS – security.   (06 Mark

      b.   Explain the prevention and detection methods on DDOS attack.   (06 Mark

      c.   List and explain any two technologies used for web services.   (04 Mark

Module-5

9   a.   List and explain the objectives and scope of IT Act.   (08 Mark

      b.   Explain the process of issuing digital signature certificate and revocation of digital signatu

        certificate by a certifying authority.   (08 Mark

OR

10   a.   Explain the various offences and punishments on cyber crime.   (08 Mark

      b.   Explain the process of attribution, acknowledgment and dispatch of electronic records.

        (08 Mark

* * * *