22

SRN

REVA UNIVERSITY
Bengaluru, India

Sixth Semester B.Tech CSE Semester-End Examination May/June 2018
Course (Subject): Cryptography and Network Security
Course Code: BTCS14F6300

Time: 3 Hours Max. Marks: 100

Note: *Answer ONE FULL question from each unit.*

UNIT – I

1. a) Alice wants to take a home loan and approaches ICICI bank. In order to approve the home loan, bank officials requested him to send his Aadhar card via an e-mail. For, a secure transmission they have agreed on the following terms and conditions 10
   i. They both use a symmetric encryption algorithm,
   ii. Agreed to use 128-bitkey.

   Identify the algorithm used for communication. Explain encryption and decryption process for the same with a neat diagram.

   b) OSI Security Architecture is a systematic approach of providing security. It focuses on Security attacks, services and Mechanisms. Explain with suitable diagram the various Security attacks, Security services and Security Mechanisms. 15

OR

2. a) As per U.S government's policy, the grade of students has to be disclosed only to the student and their parents. So, the faculty uses a 56-bit symmetric block encryption to send the student's grade. Identify the algorithm used for communication. Explain encryption and decryption process for the same with a neat diagram. 10

   b) Identify and explain the operations used for transforming plaintext to cipher text in 3DES. 6

   c) Hospitals has to maintain the patient's medical record securely by ensuring data confidentiality, Integrity and Availability. Explain how these terminologies are used in maintaining patient's records. 6

   d) Few Encryption algorithms uses Block Cipher whereas others use Stream Cipher. List the differences between block cipher and stream cipher? 3

UNIT – II

3. a) Indiangovernmentprotectsitsofficialdatafromhackersusingpublickey cryptography with two prime numbers. Identify and explain the algorithm. Apply the same to encrypt and decrypt the message M=2with p=3 and q=11. 10

   b) A common application of SHA is to encrypt passwords, Outline briefly the requirements of hash functions? Discuss the processing of SHA-512 algorithm? 15

OR

4. a) Alice and Bob wants to exchange their cryptographic keys on an insecure channel. Identify and explain the key exchange algorithm. Explain how the algorithm is vulnerable to man-in-middle attack. 10

b) HMAC has been chosen mandatory-to-implement MAC in IP Security. Explain briefly HMAC message authentication functions withneat Diagram. 7

c) A way of implementing Public key cryptography is Digital Signatures. Explain the working of Digital Signatures with suitable diagram? 5

d) List the differences between MAC and Hash function? 3

UNIT – III

5. a) Explain how PGP provides services like authentication, confidentiality, compression and Email compatibility. Also Draw and explain the transmission and reception of PGP messages 10

b) Write the certificate format of X.509. Illustrate the concept of 'certificate chain' for verification of digital signature on X.509 certificate. 10

c) PGP provides a pair of data structures at each node referred as private key ring and public key ring. Explain the procedure how the private key is encrypted and stored in private key ring. 5

OR

6. a) In an unprotected network, any client can send a request for any server for service. Explain the Kerberos V4 authentication dialogue with a suitable diagram to securely transmit data in an unprotected network. 12

b) Explain briefly the Transport mode and Tunnel modes? Also explain about the scope of AH and ESP in these modes? 7

c) Whenever the Intrusion prevention system fails, the second line of defense is Intrusion detection system. Explain the methods used for statistical anomaly detection 6

UNIT – IV

7. a) Identify the network security system designed to prevent unauthorized access to or from a private network. Explain the various types of the network security systems with suitable diagram. 12

b) A computer virus is a type of malicious software program. Classify the different types of Viruses? 7

c) In UNIX based systems, the passwords are never stored in clear. Illustrate the UNIX password scheme? 6

OR

8. a) Antivirus computer software used to prevent, detect and remove malicious software. Outline the four generations of anti-virus softwares? Illustrate the steps involved in a digital immune systemwith a neat diagram? 12

b) Eve can easily guess the password set by Alice to access his e-mail. Help Alice by defining the four techniques that were user to avoid guessable passwords. 5

c) Malicious software is intentionally included in the system for a harmful purpose. Explain briefly the following Backdoor, Logic Bomb, Trojan Horses and Mobile code? 8