47

SRN | | | | | | | | | |

REVA UNIVERSITY
Bengaluru, India

Sixth Semester B Tech C3 Examination June 2017
Course (Subject): Cryptography & Network Security
Course Code:BTCS15F6300

Time: 3 hours **Max. Marks: 100**

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

SECTION-I (UNIT –I)

1. a) When do you say the attack is active attack? Discuss briefly about the active attacks. 5
   b) Elaborate on the Fiestel Cipher Structure used for symmetric key cryptosystems 10
   c) Discuss the various security mechanisms 10

OR

2. a) Differentiate between active & passive attacks. 6
   b) Elaborate the DES round function in detail with a neat diagram. 9
   c) Explain the different Security Services and Mechanisms. 10

SECTION-II (UNIT – II)

3. a) Perform the encryption & decryption using RSA algorithm on the data given p=3, q=11, e=7 & M=5 8
   b) Illustrate the three ways in which message can be authenticated using one –way Hash function 7
   c) Briefly describe the properties of hash function that must have to be useful for message authentication 5
   d) How a secret key is exchanged securely using Diffie Hellman Key Exchange algorithm 5

OR

4. a) Explain the RSA encryption & decryption process with an example 10
   b) Consider a Diffie Hellman scheme with common prime q=11 & primitive root alpha=2 6
      i. If user A has public key YA=9, what is A's private key?
      ii. If user B has public key YB=3, what is the shared secret key?
   c) Explain the process of message digest generation using SHA-512 9

SECTION-III (UNIT – III)

5. a) Elaborate on the steps performed by sending & receiving PGP entity when the message is to be both signed & encrypted 10
   b) List & explain the header fields defined in MIME 5
   c) Differentiate between tunnel mode & transportmode functionalities 5
   d) Discuss the benefits of IPSec 5

OR

6. a) Illustrate the confidentiality & authentication service provided by pretty good privacy 10
   b) Briefly explain the content types of MIME specified in RFC 2046 10
   c) Differentiate between two approaches to intrusion detection. 5

SECTION-IV (UNIT – IV)

7. a) How is salt generated in a scheme used on UNIX? What are the purposes that salt serves? 5
   b) Explain the phases encountered by computer virus during its lifetime. 5
   c) Elaborate on filtering rules based on information contained in a network packet of a packet filtering firewall. 5

PTO

d) Illustrate the typical steps in digital immune system operation. 10

OR

8. a) Define the following terms with respect to malicious software programs 6
   i. Virus
   ii. Downloaders
   iii. Trojan horse
   iv. Flooders
   v. Zombie
   vi. Adware

b) Summarize the general techniques firewalls use to control access and enforce site's security policy. 5

c) Explain the packet firewall with a block diagram. 9

d) Elaborate on the Nimda attack and its distribution methods in the context of blended attacks. 5

***