Reg. No. : □□□□□□□□□□

Question Paper Code: 41864

B.E. / B.Tech. DEGREE EXAMINATION, MAY 2017

Sixth Semester

Information Technology

14UIT604 - CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2014)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 1 = 10 Marks)

1. In cryptography, what is cipher text

   (a) algorithm (b) encrypted message
   (c) plain text (d) none of these

2. 2 mod 17 and 2 mod 9 is

   (a) 3 (b) 21
   (c) congruent (d) Chinese Remainder theorem

3. Which of the following is prime number?

   (a) 1 (b) 2 (c) 21 (d) 321

4. Data encryption standard is

   (a) stream cipher (b) block cipher
   (c) public key cipher (d) authentication

5. 2^4 mod 17

   (a) 2 (b) 4 (c) 8 (d) 16

6. The properties of hash function is

   (a) Zero-way (b) one-way (c) two-way (d) trapdoor

7. Which one of the following is a cryptographic protocol used to secure HTTP connection?

   (a) stream control transmission protocol (SCTP)
   (b) transport layer security (TSL)
   (c) explicit congestion notification (ECN)
   (d) resource reservation protocol

8. The output of SHA is

   (a) plain text (b) cipher text
   (c) message digest (d) block text

9. IPSec in tunnel mode protects the original

   (a) TCP Header (b) IP header
   (c) UDP header (d) FTP header

10. Firewall is

   (a) just a router (b) router with filter
   (c) host (d) switch

PART - B (5 x 2 = 10 Marks)

11. Show that 3 is a primitive root of 7.

12. Define avalanche effect.

13. What are the requirements of the hash function?

14. How IPSec does offer the authentication and confidentiality services?

15. List the design goals of firewalls.

PART - C (5 x 16 = 80 Marks)

16. (a) Explain the standard security architecture and discuss the attacks that architecture can overcome. (16)

Or

(b) Explain briefly about Fermat’s and Euler’s theorems. (16)

17. (a) Draw the general structure of DES and explain the encryption and decryption process. (16)

Or

(b) Draw the general structure of AES and explain the encryption and decryption process. (16)

18. (a) Explain the working principle of RSA crypto system with an example. (16)

Or

(b) Describe how SHA logic produce message digest in detail. (16)

19. (a) What is Kerberos? Explain how it provides authenticated service. Discuss any one of its version in brief. (16)

Or

(b) Summarize the secure electronic transaction with neat diagram. (16)

20. (a) Explain about the various IDS mechanisms in detail. (16)

Or

(b) Explain how firewalls prevent intrusions and discuss its types in brief. (16)