Reg. No. : | | | | | | | | | | |

Question Paper Code: 59216

B.E./B.Tech. DEGREE EXAMINATION, SEP 2020

Elective

Computer Science and Engineering

15UCS916-CRYPTOGRAPHY

(Regulation 2015)

Duration: One hour Maximum: 30 Marks

PART A - (6 x 1 = 6 Marks)

(Answer any Six of the following Questions)

1. What will be the plain text corresponding to cipher text "PROTO" if vigenere cipher is used with keyword as "HELLO"? CO1- U

   (a) SANFOUNDRY (b) WORLD (c) INDIA (d) AMERICA

2. An asymmetric-key (or public-key) cipher uses CO1- U

   (a) 1 Keys (b) 2 Keys (c) 3 Keys (d) 4 Keys

3. Which are the most frequently found letters in the English language? CO1-U

   (a) e,a (b) e,o (c) e,t (d) e,i

4. An encryption algorithm transforms the plaintext into CO1-U

   (a) Cipher text (b) Simple Text (c) Plain Text (d) Empty Text

4. For a key 25D5 and PT input A479 what is the output we obtain after the "add round key" function? CO2- R

   (a) F34D (b) 81AC (c) 79DF (d) 327D

5. The DES algorithm has a key length of CO2- R

   (a) 128 Bits (b) 32 Bits (c) 64 Bits (d) 16 Bits

6. In DES algorithm, if the input of an s-box is 110011 then we look for the ____ th row of the S-box to obtain the output. CO2- R

   (a) 0 (b) 1 (c) 2 (d) 3

7. n = 35; e = 5; C = 10. What is the plaintext (use RSA)? CO3- A

(a) 3 (b) 7 (a) 3 (b) 7

8. Which are necessary for an agent to solve an online search problem? CO3- R

(a) Actions (b) Step-cost function (c) Goal-test (d) All of the above

9. What is the size of W (in bits) in the SHA-512 processing of a single 1024- bit block? CO4- U

(a) 64 (b) 128 (c) 512 (d) 256

9. What is the value of ipad in the HMAC structure? CO4- U

(a) 00111110 (b) 00110010 (c) 10110110 (d) 01110110

10. What is the maximum length of the message (in bits) that can be taken by SHA-512? CO4- R

(a) 2^{128} (b) 2^{256} (c) 2^{64} (d) 2^{192}

PART – B (3 x 8 = 24 Marks)

(Answer any Three of the following Questions)

11. Explain about Fermat and Euler Theorem. CO1- U (8)

12. In AES, how the encryption key is expanded to produce keys for the 10 rounds. CO2- App (8)

13. Briefly describe the idea behind Elliptic Curve Cryptosystem and describe the key management of public key CO3- U (8)

14. Explain about Authenticated Encryption. CO4- U (8)

15. Discuss about the objectives of HMAC and it security features. CO4- U (8)