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

Question Paper Code : X20408

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2020 AND APRIL/MAY 2021
Seventh/Eighth Semester
Computer Science and Engineering
CS6701 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Electronics and Communication Engineering/Information Technology)
(Regulations 2013)
(Also Common to PTCS 6701 – Cryptography and Network Security for B.E. Part-Time – Sixth Semester – Computer Science and Engineering – Regulations 2014)

Time : Three Hours　　　　Maximum : 100 Marks

Answer ALL questions

PART – A　　　　**(10×2=20 Marks)**

1. Calculate the cipher text for the following using single columnar transposition.
   Key : 24153 & Plain Text : ENGINEERING STUDENTS TALENT TEST

2. List various types of active attacks.

3. Write the disadvantages of ECB.

4. What are Diffie-Hellman groups ?

5. Is MD5 reversible ? Justify it.

6. Calculate the value of “r” using DSS algorithm for q = 199; p = 797; g = 81 and k = 30.

7. Mention two approaches used for intrusion detection.

8. Write the limitations of firewall.

9. Why do we need Security Association ?

10. Why do we use pseudorandom function in TLS ?

PART – B **(5×13=65 Marks)**

11. a) Find the multiplicative inverse for 550 mod 1759 using Extended Euclidean algorithm. Write the algorithm and its applications.

(OR)

b) Perform Encryption and decryption using Hill Cipher for the following :
Message : DES and Key : CONFIDENT.

12. a) Explain AES algorithm in detail.

(OR)

b) Explain various block modes of operation in detail. Compare it.

13. a) What are hash functions ? Why are they important ? How do you select a hash function ? Discuss about it.

(OR)

b) Discuss in detail about authentication protocols. Explain pros and cons for each.

14. a) What problem was Kerberos designed to address ? What are its four requirements ? How Kerberos v4 works ? Explain it.

(OR)

b) List 4 techniques used by firewalls to control access and enforce security policy. How are firewalls configured ? Illustrate it.

15. a) Why does PGP generate a signature before applying compression ? Explain PGP message generation and reception process in detail.

(OR)

b) List the principle categories of SET participants. How does SET work ? Explain it in detail.

PART – C **(1×15=15 Marks)**

16. a) Mention the advantages and disadvantages of Diffie-Hellman algorithm. Find the secret key shared between user A and user B using Diffie-Hellman algorithm for the following :
$q = 257$, α (primitive root) $= 3$, $X_A = 179$ and $X_B = 85$

(OR)

b) Write RSA algorithm and solve the following :
$p = 47; q = 71; e = 79; M = 688.$
Find public key and private key and perform encryption and decryption. Compare RSA with ECC algorithm.