Reg. No. :

Question Paper Code : X10328

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2020
Seventh Semester
Computer Science and Engineering
CS8792 – CRYPTOGRAPHY AND NETWORK SECURITY
(Common to Information Technology and Computer and Communication Engineering)
(Regulations 2017)

Time : Three Hours | Maximum : 100 Marks

Answer ALL questions

PART – A **(10×2=20 Marks)**

1. Compare active and passive attack.
2. Encrypt the plaintext tobeornottobe using the vigenere cipher for the key value Now.
3. Give the five modes of operation of block cipher.
4. Define field and ring in number theory.
5. Find the GCD of (2740,1760) using Euclid's Algorithm.
6. For p = 11 and q = 19 and choose d = 17. Apply RSA algorithm where Cipher message = 80 and thus find the plain text.
7. What is MAC ? Mention the requirement of MAC.
8. State birthday problem.
9. List out the applications of SSL.
10. What do you mean by IP Security policy ?

PART – B **(5×13=65 Marks)**

11. a) i) What is monoalphabetic cipher ? Examine how it differs from Caesar cipher. **(7)**

ii) Encrypt the message "this is an exercise" using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext. **(6)**

(OR)

b) i) Explain OSI Security Architecture model with neat diagram. **(7)**

ii) Describe the various security mechanisms. **(6)**

12. a) i) Demonstrate that the set of polynomials whose coefficients forms a field is a ring. **(5)**

ii) For each of the following elements of DES, indicate the comparable element in AES if available :

a) XOR of subkey material with the input to the function. **(4)**

b) f function. **(4)**

(OR)

b) What do you mean by AES ? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example. **(13)**

13. a) i) With a neat sketch, explain the Elliptic curve cryptography with an example. **(8)**

ii) Alice and Bob use the Diffie – Hellman key exchange technique with a common prime number 11 and a primitive root of 2. If Alice and Bob choose distinct secret integers as 9 and 3, respectively, then compute the shared secret key. **(5)**

(OR)

b) State Chinese Remainder theorem and find the value of X for the given set of congruent equations using Chinese Remainder theorem. **(13)**

$X \equiv 1 \pmod 5$
$X \equiv 2 \pmod 7$
$X \equiv 3 \pmod 9$
$X \equiv 4 \pmod{11}$

14. a) Briefly explain the steps of message digest generation in Whirlpool with a block diagram. **(13)**

(OR)

b) Explain PKI management model and its operations with the help of a diagram. **(13)**

15. a) With the help of a neat diagram, explain wired and wireless TLS architecture. **(13)**

(OR)

b) Assume when an attacker tries to modify the database content by inserting an UPDATE statement. Identify this SQL injection attack method and justify. Detail the methods used to prevent SQL injection attack. **(13)**

PART – C **(1×15=15 Marks)**

16. a) Discuss examples from real life, where the following security objectives are needed :

i) Confidentiality. **(5)**

ii) Integrity. **(5)**

iii) Non-repudiation. **(5)**

Suggest suitable security mechanisms to achieve them.

(OR)

b) Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer.

Transfer amount	**Cryptography functions required**
1 – 2000	Message digest
2001 – 5000	Digital signature
5000 and above	Digital signature and encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations. **(15)**

———————