CSE 325 (R-15)

Total No. of Questions :09] [Total No. of Pages : 02

III/IV B.Tech. DEGREE EXAMINATIONS, NOVEMBER- 2019

Second Semester

COMPUTER SCIENCE ENGINEERING

FOUNDATIONS OF CRYPTOGRAPHY

Time: Three Hours **Maximum marks:60**

Answer Question No.1 Compulsory **6X2=12 M**

Answer ONE Question from each Unit **4X12=48 M**

1. a) Define the three security goals?

b) Why random numbers are used in security

c) Find decryption key, if encryption key in a transposition cipher is [3 1 5 4 2]

d) What is weak collision resistance? Mention its use.

e) Define trapdoor one-way function. Give an example

f) What is hash function?

UNIT-I

2. a) What is importance of discrete logarithms in cryptography? Explain in detail. What is the difference between an index and a discrete logarithm?

b) What is Euler's Totient Function? Find the value of ¤ (37).

(OR)

3. a) Define threat and attack. What is the difference between both? List some examples of attacks which have arisen in real world cases.

b) Use Euler's theorem to find a number X between 0 and 28 with X^{83} congruent to 6 modulo 35 (You should not need to use any brute force searching)

UNIT-II

4. a) Define one-way function/one-way permutation.

P.T.O

b) Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root ~ =2.

i) Show that 2 is primitive root of 11

ii) If user A has public key Y_A=9, what is A's private key X_A?

iii) If user B has public key Y_B=3, What is the shared secrete key K, shared with A

(OR)

5. Explain cipher block modes of operations in detail.

UNIT-III

6. a) Write notes on Elgamal digital signature scheme.

b) Explain CCA2 Secure Encryption Scheme.

(OR)

7. Explain the Random-Oracle Model (ROM). Elaborate on Public-Key encryption secure against chosen-ciphertext attacks in the ROM.

UNIT-IV

8. a) What is the purpose of digital signature? Explain its properties and requirements.

b) List the generally accepted requirements for a cryptographic hash function. Explain each requirement.

(OR)

9. a) What are the services provided by digital signatures? Explain if the following are provided?

i)Source Authentication, (ii) Data Integrity and (iii) Source Non-Repudiation

b) Give a brief on Zero-Knowledge Proofs. Explain Fiat-Shamir Identification Scheme.

CSE 325 (R-15)

Total No. of Questions :09] [Total No. of Pages : 02

III/IV B.Tech. DEGREE EXAMINATIONS, APRIL- 2019

Second Semester

COMPUTER SCIENCE ENGINEERING

FOUNDATIONS OF CRYPTOGRAPHY

Time: Three Hours **Maximum marks:60**

Answer Question No.1 Compulsory 6X2=12 M

Answer ONE Question from each Unit 4X12=48 M

1. a) Pairing function

b) Find decryption key, if encryption key in a transposition cipher is [3 1 4 5 2]

c) List the categories of potential attacks on RSA

d) What do you mean by man-in-the-middle attack?

e) How will you decrypt a message using elliptic curve cryptosystem?

f) Define Perfect Zero-Knowledge proof

UNIT-I

2. a) Explain various logarithms used for modular arithmetic operations with example.

b) Differentiate the cipher properties of confusion and diffusion.

(OR)

3. a) What is importance of Chinese Remainder Theorem in cryptography? Explain.

b) What is an elliptic curve? Explain encryption in this context.

UNIT-II

4. a) Explain the RSA algorithm. Compute cipher text for M=88, p=17 and q=11.

b) In detail explain different possible approaches for attacking RSA algorithm.

(OR)

5. a) Give a brief on Computational indistinguishability and pseudorandom generators (PRGs) and explain One-wayness of PRGs

b) With an example explain how to Build PRG from a one-way permutation.

P.T.O

UNIT-III

6. a) Explain the security notations for public-key encryption: IND-CPA/IND-CCA

   b) Use Fermats theorem to find a number a between 0 and 72 with a congruent to 9794 modulo 73.

(OR)

7. a) Give the definition of CPA/CCA1/CCA2 security. Explain CPA/CCA1 Secure Encryption Scheme.

   b) Explain Miller Rabin test for primality.

UNIT-IV

8. "Identification schemes (ID-schemes) are very powerful in some areas of cryptography". Justify and prove the equivalence between non-interactive trapdoor commitment schemes and a natural class of identification schemes.

(OR)

9. a) What is Birthday Attack on Digital Signatures? Can it be performed by an 'Outsider'? Explain.

   b) Explain in detail Digital Signature Standard approach and its algorithm