Candidate Seat no............

CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY

Sixth Semester of B.Tech. (IT) Examination
May 2022

IT348 Cryptography and Network Security

Date: 07/05/2022, Saturday **Time: 10:00 a.m. to 01:00 p.m.** **Maximum Marks: 70**

Instructions:

1. The question paper comprises of two sections.
2. Section I and II must be attempted in separate answer sheets.
3. Make suitable assumptions and draw neat figures wherever required.

SECTION – I

Q - 1 **Do as directed.** **[07]**

(a) Differentiate cryptanalytic attacks and non-cryptanalytic attacks. **[02]**

(b) Generate the ciphertext for the following plain text with the help of auto key cipher "Attack is delayed". Use initial key = 'M'. **[05]**

Q - 2 (a) Draw and explain the encryption and decryption structure of Electronic Codebook (ECB) mode. **[05]**

Q - 2 (b) Why only prime numbers are used in RSA, Justify your answer. **[02]**

OR

Q - 2 (a) Draw and explain the encryption and decryption structure of Cipher Block Chaining (CBC) Mode **[05]**

Q - 2 (b) Which technique (Cryptography or Steganography) is used in each of the following cases for confidentiality? **[02]**

1. A student writes the answer to a test on a small piece of paper, rolls up the paper, and inserts in a ball-point pen, and passes the pen to another student.
2. To send a message, an officer replaces each character in the message with a symbol that was agreed upon in advance as the character replacement.

Q - 3 (a) Answer the following questions. **[ANY TWO]** **[10]**

i) Apply a brute-force attack to break the cipher "UVACLYFZLJBYL". Note that the ceaser cipher algorithm is used for encryption.

ii) Explain the key expansion process in AES cipher

iii) Define multiplicative inverse in modular arithmetic. Calculate the multiplicative inverse of 89 in Z_{300}.

Q - 3 (b) Describe the chosen cipher text attack in RSA. **[04]**

Q - 4 (a) Calculate 9^{667} mod 780 using fast exponential algorithm **[04]**

Q - 4 (b) Discuss three basic requirements of any cryptographic hash function **[03]**

Candidate Seat no............

SECTION – II

Q - 4 **Answer the following question** [07]

(a) Draw the block diagram of the DES function and explain the working of it [04]

(b) What is X.509 recommendation? Explain the signature field of X.509 certificate format. [03]

OR

(a) Generate 8-bit round keys for round 1 and round 2 in S-DES for a given 10-bit cipher key as 1011100110. [04]

Straight P box: 3 5 2 7 4 10 1 9 8 6

Compression P box: 6 3 7 4 8 5 10 9

(b) Calculate the padding bit (SHA512) require for the messages having below-mentioned length: [03]

1. 1
2. 896
3. 897

Q - 5 (a) Find the Greatest Common Divisor of 2740 and 1760 using Euclidean Algorithm. [05]

OR

Q - 5 (a) Use the Vigenere Cipher with the keyword "HEALTH" to encipher the message "Life is full of surprises". Find the cipher text. [05]

Q - 5 (b) Find 20^{62} mod 77 using Euler's theorem. [05]

Q - 5 (c) List out and explain the invertible and non-invertible components used in Feistel cipher. [04]

Q - 6 (a) Explain key generation process in DES. [05]

OR

Q - 6 (a) List out and explain the fields of X.509 digital certificate. [05]

Q - 6 (b) Explain security service and security mechanism. [03]

Q - 6 (c) Write a short note on any TWO of the following [06]

1. Master Key Generation in SSL 2. Trust calculation in Preety Good Privacy
3. Secure MIME

*****