

Dr R. Singh Alr

21/11/2023 (65)

National Institute of Technology Hamirpur (H.P.)

End Semester Theory Examination – November-2023

Title of the Course: <Cryptography and Information Security >

Class: B.Tech (Mathematics and Computing)

Course Code: MA-411

Duration: 3 Hour

Semester: 7

Max. Marks: 50

**Instructions:**

- All Questions are compulsory.
- Marks are given against each question.

1. Define the three Security goals. Define the security services and mechanisms in Cryptography. [03+05 Marks]
2. Explain the additive and multiplicative ciphers with suitable examples. [04 Marks]
3. Discuss the Affine Cipher. Using the Affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26. [03 Marks]
4. Write the statement and procedure of Euclidean Algorithm. Find the greatest common divisor of 2740 and 1760. [04 Marks]
5. Define the multiplicative inverse. Find the multiplicative inverse of 8 in  $Z_{10}$ . [02 Marks]
6. Discuss the Chinese Remainder Theorem (CRT). Find the value of X using CRT  
 $X \equiv 1 \pmod{5}$ ,  $X \equiv 2 \pmod{7}$ ,  $X \equiv 3 \pmod{9}$ ,  $X \equiv 4 \pmod{11}$  [04 Marks]
7. Explain the general structure of DES algorithm in detail with neat diagram. [05 Marks]
8. Describe RSA algorithm.
  - (i) In a public-key system using RSA, you intercept the cipher text  $C = 10$  sent to a user whose public key is  $e = 5$ ,  $n = 35$ . What is the plaintext?
  - (ii) In an RSA system, the public key of a given user is  $e = 31$ ,  $n = 3599$ . Determine the private key of this user? [05 Marks]
9. Discuss the Diffie-Hellman key exchange algorithm. Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime  $q = 83$  and a primitive root  $\alpha = 5$ .
  - (i) If Alice has a private key  $X_A = 6$ , what is Alice's public key  $Y_A$ ?
  - (ii) If Bob has a private key  $X_B = 10$ , what is Bob's public key  $Y_B$ ?
  - (iii) Construct the shared secret key. [05 Marks]
10. Write a short note on virus, worms and intruders. Describe in detail about SSL/TLS. [06 + 04 Marks]

\*\*\*\*\*ALL THE BEST\*\*\*\*\*