JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2024

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARKS: 35

COURSE NAME: Information Security

COURSE INSTRUCTORS: Dr. Nancy Singla MAX. TIME: 2 Hours

Note: *(a) All questions are compulsory.*
(b)Marks are indicated against each question in square brackets.
(c) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

---

Q1. Alice wants to securely send a confidential document to Bob via email. She decides to use digital signatures to ensure the integrity and authenticity of the document. Describe the steps Alice should take to sign the document and explain how Bob can verify the digital signature upon receiving the email. [5] [CO4]

Q2. (a) Jack is sending Tommy a message with RSA algorithm. The public key is 3, while N is 55. What is the value of 'd' that Tommy must use to decrypt the message? [5+5] [CO2]

(b) Can RSA algorithm be broken if the private exponent 'd' is relatively small compared to the modulus N? Explain.

Q3. A company is developing a new web application that requires user registration and authentication. The development team is implementing a secure method for storing user passwords to protect them from unauthorized access. Describe the approach the team should take to securely store passwords using hash values. Discuss the advantages of this approach in comparison to storing passwords in plain text. [5] [CO1]

Q4. A group of friends wants to divide the access code to their secret clubhouse using Shamir's Secret Sharing scheme. They decide to split the 2-digit access code into 3 shares, requiring any 2 shares to reconstruct the code. Considering 3 shares as (1, 90), (2, 107) and (3, 124), reconstruct the 2-digit access code. [5] [CO4]

Q5. Explain the Rabin encryption and decryption scheme in cryptography. Discuss the security implications associated with Rabin encryption. [5] [CO2]

Q6. (a) Why must a symmetric key cryptographic algorithm generate a mapping that is one-to-one? [2+3] [CO3]

(b) Why is Diffie-Hellman susceptible to man-in-the-middle attacks? How such attacks can be prevented?