Dr. Pankaj Dhiman

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS-2022

B.Tech-III Semester (CS/IT/ECE/Civil/BT)

COURSE CODE: 19B1WC1632 CS-IT

MAX. MARKS: 25

COURSE NAME: Information Security

COURSE CREDITS: 2 MAX. TIME: 1 Hour 30 Min

***Note:** All questions are compulsory. Marks are indicated against each question in square brackets.*

T2 Examinations April 2022

Q1. Consider a block cipher using 8-bit blocks that is based on the basic DES architecture (Feistel network) with two rounds and no initial or final permutation. The scrambling function for round i is fi(x, K) = (2i · K) x mod 15, for i = 1, 2, where the key K is a member of Z15. If K = 7 and the ciphertext is 00111111, what is the plaintext? Draw the picture of the Feistel Cipher network to help you, and show your intermediate results. **3 marks**

Q2. Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2.

a) If user, A" has public key YA=9, what is A"s private key XA.

b) If user, B" has public key YB=3, what is shared secret key K. **3 marks**

Q3. Consider the Following properties.

R-i) Closure under multiplication R-ii) Associativity of multiplication

R-iii) Distributive Law R-iv) Commutativity of multiplication

R-v) Multiplicative Identity R-vi) No zero divisors R-vii) Multiplicative Inverse.

a) Abelian group satisfies which of the properties from above options? 1 marks

b) A Ring satisfies which of the properties from above options? 1 marks

c) a.(b.c) = (a.b).c, Find out the representation from above options? 1 marks

d) A Ring is said to be commutative if it also satisfies which of the above property. 1 marks

Q4. Difference between attack and vulnerability? List and explain any seven attacks. 3 marks

Q5. What is SSL session? Can a session be shared among multiple connections? 3 marks What are the parameters that define a session state?

Q6. Consider the following: Plaintext: "PROTOCOL", Secret key: "NETWORK", what is the corresponding cipher text using Play fair cipher method? 3 marks

P.T.O

Q7. What will be cipher text if the string "JAVAPOINT" is given as input to the code of Vigenere cipher with key as "BEST". 2 marks

Q8 How many number of tests required breaking the DES algorithm? 2 marks

Q9.Compare substitution ciphers with transposition ciphers. 2 marks

T2 Examinations April 2022

**P.T.O**