JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS-2022

B.Tech-III Semester (CS/IT)

COURSE CODE (02): 19B1WC1632 CS-IT MAX. MARKS: 35

COURSE NAME: Information Security

COURSE INSTRUCTORS: Dr Pankaj Dhiman MAX. TIME: 2 Hours

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

Q1. Consider the following: Plaintext: "PROTOTYPE", Secret key: "HELLO", what is the corresponding cipher text using Hill cipher method? **[4 Marks]**

Q2. Discuss the ethical Concepts in information security and the prevention to illegal and unethical behaviors? **[3 Marks]**

Q3. Find out the plain text corresponding to cipher text "INSTRUCTION" if Rail Fence Cipher is used with keyword as "NAME"? **[4 Marks]**

Q4. AES uses a _____ bit block size and a key size of _____ bits. **[3 Marks]**

a) 128; 128 or 256

b) 64; 128 or 192

c) 256; 128, 192, or 256

d) 128; 128, 192, or 256

Q5. What are the message authentication functions? What are its requirements? **[3 Marks]**

Q6. Explain the principle of RSA algorithm by taking an example. **[3 Marks]**

Q7. How many rounds does the AES-256 perform ? Explain with example? **[3 Marks]**

Q8. On Encrypting "thepepsiisintherefrigerator" using Vignere Cipher System using the keyword "HUMOR" we get cipher text ? **[4 Marks]**

Q9. Using P=3, q=13, d=7 and e=3 in the RSA algorithm, what is the value of cipher text for a plain text 5? **[4 Marks]**

Q10. What is maximum length of the message (in bits) that can be taken by SHA-512? Explain with example? **[4 Marks]**