JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION-2022

B.Tech-III Semester (CS/IT)

COURSE CODE (CREDITS): 18B1WC1734 MAX. MARKS: 35

COURSE NAME: Cryptography and Network 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. Suppose Alice and Bob use *an Elgamal scheme* with a common prime $q=157$ and a primitive root $\alpha = 5$. [CO-4] [Marks-6]

a) If Bob has public key $Y_B=10$ and Alice chose the random integer $k=3$, what is the cipher-text of $M=9$.

b) If Alice now chooses a different value of k so that the encoding of $M=9$ is $C= (25, C_2)$, what is the integer C_2.

Q2. Use the Caesar Cipher technique to encrypt and decrypt the message "JUIT IS BEST UNIVERISTY", key shift value of this message is 3. [CO-2] [Marks-4]

Q3. Explain the generation *Sub key and S-Box* from the given *32-bit* key by Blowfish. In AES, how the encryption key is expanded to produce keys for the *10* rounds. [CO-4] [Marks-5]

Q4. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement. [CO-1] [Marks-5]

Q5. Assume the client *(C)* wants to communicate server *(S)* using Kerberos procedure. How can it be achieved? Write the complete authentication procedure. [CO-5] [Marks-5]

Q6. Encode the text "Ciphertext" using the following techniques. Assume characters are stored in *8-bit ASCII* with zero parity. [CO-6] [Marks-5]

A) Base-64

B) Quoted-printable

Q7. What is *DHCP*? How useful is it to help achieve security of IP addresses. [CO-6] [Marks-5]