System and Network Security

Quiz 1 (Spring 2021)

International Institute of Information Technology, Hyderabad

Time: 60 Minutes Total Marks: 40

Instructions: This is online examination.

Write at the top of your answer book with the following information:

System and Network Security (CS 5470)

Quiz - 1 (Spring 2021)

Date: 2-February-2021

Name:

Roll Number:

Submit your scanned hand-written answer script in the moodle with the file name: RollNo_Quiz1_2Feb2021.pdf

1. Answer the following ten objective-type questions.

   (a) Does a perfectly secure algorithm exist in the real life encryption world? If so, name a cipher here _____.

   (b) Can FCS be implemented using Hardware? If yes, give an example here _____.

   (c) The probability that a key can be either a weak key, a semi weak key or a possibly weak key in DES is _____.

   (d) Name two OSI layers where error detection or correction happen on the payload _____.

   (e) Hill cipher is an example of _____.

   (f) Is the Diffie Hellman key exchange prototocol an end-to-end encryption algorithm? Why? _____.

   (g) The difference between DES encryption and decryption algorithm is _____.

   (h) Like DES, does AES also use Feistel structure? _____.

   (i) Which has a key length of 128 bits?

   a) IDEA

   b) Triple-DES

   c) IDEA and Triple-DES

   d) None of the mentioned ciphers

   (j) The differences between Message Authentication Code (MAC) function and one-way cryptographic hash function are _____.

$[10 \times 1 = 10]$

2. (a) External error control is better than internal error control- Justify your answer.

   (b) Better security can be provided by combining both Link-by-Link Encryption (LLE) and End-to-End Encryption (EEE) - Justify. Explain this combined approach with an example.

   [4 + 6 = 10]

3. In the Diffie-Hellman key exchange protocol, what happens if X_A and X_B have the same value, that is, Alice and Bob have accidentally chosen the same private key? Are Y_A and Y_B the same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.

   [8]

4. (a) Explain why the password management scheme used in UNIX is vulnerable to the password guessing attacks?

   (b) Improve the the password management scheme used in UNIX using biometric verification with the help of fuzzy extractor technique. Explain its security particularly from the password guessing attacks points of view.

   [4 + 8 = 12]

********** **End of Question Paper** **********