44

B.Sc. Engg. CSE 7th Semester 03 October 2023 (Morning)

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

MID SEMESTER EXAMINATION
DURATION: 1 HOUR 30 MINUTES

WINTER SEMESTER, 2022-2023
FULL MARKS: 75

CSE 4743: Cryptography and Network Security

Programmable calculators are not allowed. Do not write anything on the question paper.
Answer **all 3 (three)** questions. Figures in the right margin indicate full marks of questions whereas corresponding CO and PO are written within parentheses.

1. a) Identify the security goals of a network and give real-life examples where each of the security goals has been breached. 3 + 3 (CO1) (PO1)

   b) Some archaeologists found a new script written in an unknown language. The archaeologists later found a small tablet at the same place that contains a sentence in the same language with Greek translation. Using the tablet, they were able to read the original script. Explain what type of cryptanalysis attack did the archaeologists use and why they used it. 5 (CO2) (PO2)

   c) Homer Simpson is trying to communicate with Marge Simpson using encryption techniques. Answer the following questions to help Homer encrypt the messages properly:

      i. Homer Simpson is building a monoalphabetic cipher using Caesar Cipher and then its output is used as an input for Multiplicative Cipher. Since Homer is very lazy, he decides to use the same key of $K = 15$ for both the ciphers. Calculate the ciphertext if the plaintext is: **shake and bake**. 6 (CO2) (PO1)

      ii. While Homer is very happy with his simple cipher, it is getting decrypted easily by his arch nemesis, Frank Grimes. So, he tries to analyze the issues with his technique. Identify the drawbacks of the Cipher used by Homer Simpson in order to keep his messages private and secured. 2 (CO2) (PO1)

      iii. Based on analysis, Homer decides to add one more layer of Cipher to increase security. He decides the ciphertext he gets in the previous case will be the key stream for his Vigenere Cipher. What should be the ciphertext with this new technique if his input plaintext is: **Marge it takes two to lie. One to lie and one to listen.** 7 (CO2) (PO1)

      iv. Homer is not risking it. He will use the output from Vigenere Cipher and pass it as an input to a Keyed Transposition Cipher with a $Key = [2, 5, 7, 6, 4, 1, 3]$. Find the final ciphertext sent by Homer to Marge. 4 (CO2) (PO1)

      v. After all these over-the-top security measures, it is observed that Homer's key is being intercepted every time by Frank. Analyze this breaching scenario and propose a solution with proper justification. 4 (CO4) (PO2)

2. a) Suppose you have a modern block cipher where the number of input bits, $n = 64$ and the number of output bits, $m = 64$. If there are ten 1's in the ciphertext, calculate how many tests you need to conduct to recover the plaintext from the ciphertext in each of the following cases: 4 × 2 (CO2) (PO1)

      i. The cipher is designed as a substitution cipher.

      ii. The cipher is designed as a transposition cipher.

   b) In the case of Question 2a, assume 1 billion tests can be conducted per second. Calculate the time to recover the plaintext in each case. 4 (CO2) (PO1)

c) The final design of a Feistel Cipher contains 2 rounds. Each of the rounds contains a mixer and a swapper. Show appropriate mathematical calculations and reasoning to derive that the plaintext can be successfully recovered in the receiver's end, i.e. $L6 = L1$ and $R6 = R1$. Assess how this design makes improvements from previous versions. 10 (CO3) (PO1)

d) With appropriate reasoning, write down the security issues and error propagation of Electronic Code Book (ECB) mode. 4 (CO3) (PO1)

3. Alias is using Blowfish encryption algorithm for sending 64 bits of data blocks. The first block is $(A4\ B3\ 97\ C4\ 77\ 66\ AB\ BA)_{16}$. The 4 expansion S-boxes in use are: 15 (CO4) (PO2)

- S-box-1: Changes all zeros to one and all ones to zero.
- S-box-2: Changes all zeros to one.
- S-box-3: Changes all ones to zero.
- S-box-4: Changes nothing.

The 32 bits of the S-boxes are made so that there are 24 zeros followed by 8 bits which are calculated as mentioned above.
The algorithm has 4 rounds. The key stream is $(A0\ 07\ 88\ 54\ A0\ 08\ 77\ 45\ 0A\ 09\ 77\ 88\ AC\ 50\ 60\ 70)_{16}$
Find out the Ciphertext.