SOUTH EASTERN UNIVERSITY OF SRI LANKA
THIRD EXAMINATION IN BACHELOR OF INFORMATION AND COMMUNICATION TECHNOLOGY - 2018/2019
SEMESTER – I, SEPTEMBER / OCTOBER 2021

NST 31051 – Practical for Cryptography

Answer all Questions **Time Allowed: 03 hours.**

Instructions:

- **Create a folder with your Index Number and save all your files and resources in the folder.**
- **Before upload your work, convert the above folder as a .rar file and upload the single file.**
- **Write all your coding in java programming.**
  Hint: You can use any java editiors for your work
- **Upload your coding within the first 30 minutes. i.e: 12 noon to 12.30pm**

Question 01:

Imagine that you are in a warzone where you came to know that the opponent has prepared a missile to launch to demolish your location entirely and you have predicted that there will be massacre after that hit. To make a counterattack, you have to contact your high military personnel. The only possible way to contact them is through texts. Though, it is vulnerable to send plain text messages. Because the opponent may intrude on the message and see what you are up to. Hence, you have to encrypt the plain text messages and send them so that the opponent cannot understand.

To accomplish this mission, you are required to use the Caesar Cipher method for the encryption process.

a. Write a program using the Caesar Cipher method to encrypt and send the location of the missile. Use key value as 5

   Message: "*hello zero, object is at fivesixty meters south*"
   Scan the key value from the keyboard. Show the output of the encrypted message.

   (60 Marks)

b. Write a program using the Caesar Cipher method to decrypt the message from the high commander office for your message. The encrypted message from the commander is given as follows:

   Ciphertext: "*Ujwnrjyjw xjhzwji, gnwi nx ts ymj rtaj*"

   (40 Marks)

[Total 100 Marks]

Question 02:

There are situations to share some very confidential messages with one. When it comes to share via network then, the role of intruders is inevitable. They easily can see the messages and there are possibilities for the messages to be sold out. To overcome this vulnerability, we have to encrypt the data. There are various types of encryption processes are available. Among them Caesar Cipher method is weak, which can be easily decrypted.

Using the rail fence cipher method, firstly send a plaintext message containing a code word or sentence to the recipient and wait for the acknowledgement. If the acknowledgement is received as expected then the line between you and the recipient is secure. Afterwards you can continue the communication.

a. Write a program using the rail fence cipher method to encrypt the given code word to send to the receiver to establish a secure connection.

   Code word: "Cool as a Cucumber"

   (50 Marks)

b. The receiver has sent the acknowledgment to you in an encrypted form which is also encrypted using rail fence cipher technique. Write a program to decrypt the acknowledgement message to verify the secure line.

   (50 Marks)

Hint: for encryption and decryption, the key value used is 3

[Total 100 Marks]

Question 03:

Hash functions are extremely useful and appear in almost all information security applications. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but the output is always of fixed length. Values returned by a hash function are called the message digest or simply hash values.

MAC (Message Authentication Code) algorithm is a symmetric key cryptographic technique to provide message authentication. For establishing the MAC process, the sender and receiver share a symmetric key K. Essentially, a MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.

a. Write a program to create Message Digest for any message input. Use **MD5** algorithm to create the Message Digest. Your program must be able to scan any messages from the keyboard.

   Hint: You are not required to print the Hexadecimal format of the Message Digest.

   (40 Marks)

(41 Write a program to encrypt the following message using MAC (Message Authentication Code)

Message: "*My Password is 12345*"

Use "**DES**" algorithm to generate the key and "**HmacSHA256**" algorithm to create the mac object.

Your program should be able to create the MAC only for the given message.

(60 Marks)

[Total 100 Marks]

Question 04:

You and your friend have some confidential messages to share each other. You have no possible way to meet so that, decided to share the messages using a secure line communication. For this purpose, you are going to encrypt and decrypt all the messages sent and received using the asymmetric key cryptography technique.

To make the line secure both must have keys. Since you are using an asymmetric key cryptography technique, both will share different keys.

Write a program to encrypt and decrypt the given message using the asymmetric key cryptography technique.

Message: "Password is 12345"

- To generate the key pair use, "**RSA**" algorithm with **1024** key size.
- Use public key for encryption and private key for decryption processes.

Output from the program must contain the followings:

1. Encrypted text
2. Decrypted text
3. Public key and
4. Private key

[Total 100 Marks]

**** END ****