**ITCS 461 Computer and Communication Security Date : ­­\_\_\_\_\_\_\_\_\_**

**ID : Name : Section :** \_\_\_\_\_\_\_\_\_\_

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

When you get your lab done, save this answer sheet using file name including your student ID as “ **Lab1-6188xxx.docx**” or “ **Lab1-6188xxx.pdf**”, for example. Submit this file to a lab folder in ***MyCourses*** website (or other channel as instructed) according to your section.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lab 1 : Introduction to Cryptography**

Follow Lab 1 direction (**Lab1\_Explanatory\_slides.pdf**) and answer the following questions.

**Part 1-1: Classical Symmetric Cryptography**

**Encryption using Caesar Cipher**

**Question 1:** See the default settings of Caesar Cipher.

What are the values of these settings ?

1) Action :

2) Key :

3) Character mapping :

4) Unknown symbols handling :

5) Case sensitive : (Y/N) \_

**Question 2:** Examine the ciphertext and answer the following questions.

1) What is the first sentence of plaintext ?

2) What is the first sentence of ciphertext ?

3) Compare the above two answers. Are the characters mapped correctly ? (Y/N)

4) Copy ciphertext from the text output window then paste it to the text input window. Change Action to **“Decrypt”** then click **“Play”**. Do you get the plaintext back ? (Y/N)

(If not, try until you get the correct plaintext back.)

**Question 3:** Clear all input text, then type **“ABCDEFGHIJKLMNOPQRSTUVWXYZ”**,

change Action to **“Encrypt”**, change Key to **13** and click **“Play”**.

1) What is the output ciphertext ?

2) If key = 19, what will **“K”** map to ?

3) If key = 25, what will **“A”** map to ?

**Part 1-2: Classical Symmetric Cryptography (cont.)**

**Attack the Caesar Cipher using frequency analysis**

**Question 4 :** Open“Frequency Analysis.cwm”, “Play”, then “Stop”. Observe the output graph.

Answer the following questions.

1) What letter has the highest frequency of occurrences ?

2) What letter has the second highest frequency of occurrences ?

3) What letter has the lowest frequency of occurrences ?

4) Letter **“N”** appears %

5) Letter **“Q”** appears %

**Question 5 :** Answer the following questions.

1) What letter has the highest frequency of occurrences ?

2) What letter has the second highest frequency of occurrences ?

3) What letter has the lowest frequency of occurrences ?

4) Letter **“N”** appears %

5) Letter **“P”** appears %

6) Letter **“Q”** appears %

7) Letter **“Z”** appears %

**Question 6 :** Apply Caesar encryption with **Key = 11** to this message. Then use the result

ciphertext as an input to plot the letter frequency graph again. Observe the shifting in each bar.

1) Letter **“E”** appears % and this should be the ciphertext of letter .

2) Letter **“P”** appears % and this should be the ciphertext of letter .

**Question 7 :** Answer the following questions.

1) Is the attack successful ? (Y/N)

2) What is a key used to encrypt the message ?

3) What are the first line of input and output of the **“Caesar Analysis”** block ?

The 1st line of input block (ciphertext) :

The 1st line of output block (plaintext) :

**Question 8:** Answer the following questions.

1) What key is found ?

2) Is the attack successful ? (Y/N)

3) Why successful**/**Why not successful ?

**Question 9 :** Try to break (attack) the following Caesar cipher using **“Caesar\_Analysis.cwm”**.

1) ciphertext = **“hwt HtAA HtpHwtAA DC Iwt HtpHwDGt”**

1.1) Is the attack successful ? (Y/N)

1.2) What is the corresponding plaintext ?

1.3) What is the key ?

2) ciphertext = **“mKw QGMJ EwFLsDALQ. osCw MH LG JwsDALQ.”**

2.1) Is the attack successful ? (Y/N)

2.2) What is the plaintext ?

2.3) What is the key ?

3) If above cipher is failed to attack by Caesar Analysis, try attacking using brute force attack (try all possible keys).

3.1) What is the plaintext ?

3.2) What is the key ?

**Part II: Modern Symmetric Cryptography**

**Advanced Encryption Standard (AES)**

**Question 10 :** Observe the default settings. What are the default values for this encryption ?

1) Cryptographic Algorithm ?

2) Action ?

3) Key size ?

4) Mode of operations ?

5) Padding method ? \_\_\_\_\_\_\_\_\_\_\_\_

**Question 11 :**

1) Is the encrypted file successfully opened ? (Y/N)

2) What do you think happening ?

3) What is a key of encryption ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(While playing, move mouse pointer over the arrow head of input to AES window.)

**Question 12:** Display ***picture\_1.jpg*** and ***picture\_1\_decrypted.jpg*** together, and compare both images.

1) Can **“*picture\_1\_decrypted.jpg*”** be opened and displayed successfully ? (Y/N)

2) Are both images different ? (Y/N)

3) If yes, specify what is the noticeable difference ?

4) What do we need to change in the workspace in order to perform **AES** encryption

with **OFB** mode of operations ?