ITCS 461 Computer and Communication Security **Date :** 24/01/2022

ID :6388014 **Name :Waris Damkham** **Section : 2**

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 : **Encrypt**
2) Key : **3**
3) Character mapping : **A -> D**
4) Unknown symbols handling : **Ignore (leave unmodified)**
5) Case sensitive : (Y/N) **No**

Question 2: Examine the ciphertext and answer the following questions.
1) What is the first sentence of plaintext ?
Established in 2009, the Faculty of Information and Communication Technology (ICT) is one of the newest faculties at Mahidol University.
2) What is the first sentence of ciphertext ?
HVWDEOLVKHG LQ 2009, WKH IDFXOWB RI LQIRUPDWLRQ DQG FRPPXQLFDWLRQ WHFKQRORJB (LFW) LV RQH RI WKH QHZHVW IDFXOWLHV DW PDKLGRO XQLYHUVLWB.
3) Compare the above two answers. Are the characters mapped correctly ? (Y/N) **Y**
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) **Y**
(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 ? **DEFGHIJKLMNOPQRSTUVWXYZABC**
2) If key = 19, what will **"K"** map to ? **D**
3) If key = 25, what will **"A"** map to ? **T**

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 ? **E**
2) What letter has the second highest frequency of occurrences ? T
3) What letter has the lowest frequency of occurrences ? **Z**
4) Letter **"N"** appears **7.22** %
5) Letter **"Q"** appears **0.81** %

Question 5 : Answer the following questions.
1) What letter has the highest frequency of occurrences ? **E**
2) What letter has the second highest frequency of occurrences ? **N**
3) What letter has the lowest frequency of occurrences ? **X and Z**
4) Letter **"N"** appears **8.93** %
5) Letter **"P"** appears **2.11** %
6) Letter **"Q"** appears **0.2** %
7) Letter **"Z"** appears **0.1** %

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 **8.63** % and this should be the ciphertext of letter **T** .
2) Letter **"P"** appears **11.63** % and this should be the ciphertext of letter **E** .

Question 7 : Answer the following questions.
1) Is the attack successful ? (Y/N) **Y**
2) What is a key used to encrypt the message ? **6**
3) What are the first line of input and output of the **"Caesar Analysis"** block ?
The 1st line of input block (ciphertext) : **Uax Vn.J. ot Iusvazkx Yioktik otzkxtgzoutgr vxumxgs oy jkyomtkj zu hk g vxumxgs lux yzajktzy cnu cuarj roqk zu iutjaiz iusvazkx yioktik xkykgxin gtj zu hkiusk g iusvazkx yioktzoyz ux iusvazkx yioktik xkykgxinkxy.**
The 1st line of output block (plaintext) : **OUR PH.D. IN COMPUTER SCIENCE INTERNATIONAL PROGRAM IS DESIGNED TO BE A PROGRAM FOR STUDENTS WHO WOULD LIKE TO CONDUCT COMPUTER SCIENCE RESEARCH AND TO BECOME A COMPUTER SCIENTIST OR COMPUTER SCIENCE RESEARCHERS.**

Question 8: Answer the following questions.
1) What key is found ? **21**
2) Is the attack successful ? (Y/N) **Y**
3) Why successful/Why not successful ? **Because the key matches the encrypt from the Caesar.**

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) **Y**
1.2) What is the corresponding plaintext ? **SHE SELL SEASHELL ON THE SEASHORE**
1.3) What is the key ? **15**
2) ciphertext = **"mKw QGMJ EwFLsDALQ. osCw MH LG JwsDALQ."**
2.1) Is the attack successful ? (Y/N) **N**
2.2) What is the plaintext ? **FDP JZFC XPYELWTEJ. HLVP FA EZ CPLWTEJ.**
2.3) What is the key ? **7**
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 ? **USE YOUR MENTALITY. WAKE UP TO REALITY.**
3.2) What is the key ? **18**

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 ? **Advanced Encryption Standard**
2) Action ? **Encrypt**
3) Key size ? **128 bit**
4) Mode of operations ? **Electronic Code Book (ECB)**
5) Padding method ? **Zeros**

Question 11 :
1) Is the encrypted file successfully opened ? (Y/N) **N**
2) What do you think happening ? **Because the file is encrypted, the picture is changed to the cipher text.**
3) What is a key of encryption ? **0E AB ED 20 09 EF AC FF AA DC CA EC CE FE EE FA CE AA DE AE FE DE AE FC EC EC ED EE FA CF CE CE AD EC CE EA DE DE EC E1 98 8E DE EE FA DA EF AC EA DF AE EA EA CD CE EA CC AA DE EC EF CA CE FF AA DC CA EC DE EE AA DA DE EA BE DE CF AC**
(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) **Y**
2) Are both images different ? (Y/N) **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 ? **Changing Modes**