ID: **640315** **Name:** สิทธิกร เฉลิมกิตติชัย **Section :** 01

- Save this answer sheet as " **Lab1-YourID.pdf**" (Removing all figures will help reduce the file size).
- Submit this file to the lab folder in e-learning website according to your session.

Lab 1 : Symmetric Cryptography

Follow Lab 1 document (Lab1.pdf) and answer these questions:

Part I: Classic 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

5) Case sensitive (y/n): n

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

1) What is the first line of plaintext?

The Faculty of Engineering, Mahidol University was established in 1989, in response to Thailand's need for engineers as a newly industrialized country. The Faculty aims to produce graduates with knowledge and excellence in engineering, who value ethics and feel responsible to the profession and to society. Over the past 23 years, the faculty has shown its excellence in teaching and research in various fields of engineering including chemical, civil, computer, electrical, industrial, and mechanical engineering, as well as in interdisciplinary fields such as biomedical engineering.

2) What is the first line of ciphertext?

WKH IDFXOWB RI HQJLQHHULQJ, PDKLGRO XQLYHUVLWB ZDV HVWDEOLVKHG LQ 1989, LQ UHVSRQVH WR WKDLODQG'V QHHG IRU HQJLQHHUV DV D QHZOB LQGXVWULDOLCHG FRXQWUB. WKH IDFXOWB DLPV WR SURGXFH JUDGXDWHV ZLWK NQRZOHGJH DQG HAFHOOHQFH LQ HQJLQHHULQJ, ZKR YDOXH HWKLFV DQG IHHO UHVSRQVLEOH WR WKH SURIHVVLRQ DQG WR VRFLHWB. RYHU WKH SDVW 23 BHDUV, WKH IDFXOWB KDV VKRZQ LWV HAFHOOHQFH LQ WHDFKLQJ DQG UHVHDUFK LQ YDULRXV ILHOGV RI HQJLQHHULQJ LQFOXGLQJ FKHPLFDO, FLYLO, FRPSXWHU, HOHFWULFDO, LQGXVWULDO, DQG PHFKDQLFDO HQJLQHHULQJ, DV ZHOO DV LQ LQWHUGLVFLSOLQDUB ILHOGV VXFK DV ELRPHGLFDO HQJLQHHULQJ.

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? z

Question 4: 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 occurrence? z

4) Letter **"N"** appears 7.22 %?

5) Letter **"Q"** appears 0.81 %?

Part I: Classic Cryptography

Attack the Caesar cipher using frequency analysis

Question 5: Answer the following questions

1) What letter has the highest frequency of occurrences? i

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

3) What letter has the lowest frequency of occurrence? q x z

4) Letter **"N"** appears 9.39 %?

5) Letter **"P"** appears 1.2 %?

6) Letter **"Q"** appears 0.11 %?

7) Letter **"Z"** appears 0.11 %?

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 5.35 % and this should be the ciphertext of letter p

2) Letter **"P"** appears 3.71 % and this should be the ciphertext of letter a

Question 7: Answer the following questions

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

2) What is the key used to encrypt the message? 6

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

1 st line of input block (ciphertext):

Uax Vn.J. ot Iusvazkx Yioktik otzkxtgzoutgr vxumxgs oy jkyomtkj zu hk g vxumxgs lux yzajktzy cnu cuarj rogk zu iutjaiz iusvazkx yioktik xkykgxin gtj zu hkiusk g iusvazkx yioktzoyz ux iusvazkx yioktik xkykgxinkxy. Lgiarze skshkxy ul znk Lgiarze ul OIZ iaxxktzre iutjaiz xkykgxin ot g tashkx ul xkykgxin gxkgy otirajotm haz tuz rosozkj zu gxzoloiogr otzkrromktik, jgzghgyk gtj qtucrkjmk-hgykj yeyzks, iusvazkx tkzcuxg gtj ykiaxoze, iusvazkx mxgvnoiy, gtj yulzcgxk ktmotkkxotm. Grr gjsozzkj yzajktzy xkikobk larr lotgtiogr yavvuxz znxuamn Vn.J. yinurgxynov vxumxgs, gtj znke

gxk kdvkizkj zu vgxzoiovgzk ot lgiarze gizobozoky larr-zosk ut-igsvay znxuamnuaz znk vxumxgs.

1 st 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. FACULTY MEMBERS OF THE FACULTY OF ICT CURRENTLY CONDUCT RESEARCH IN A NUMBER OF RESEARCH AREAS INCLUDING BUT NOT LIMITED TO ARTIFICIAL INTELLIGENCE, DATABASE AND KNOWLEDGE-BASED SYSTEM, COMPUTER NETWORK AND SECURITY, COMPUTER GRAPHICS, AND SOFTWARE ENGINEERING. ALL ADMITTED STUDENTS RECEIVE FULL FINANCIAL SUPPORT THROUGH PH.D. SCHOLARSHIP PROGRAM, AND THEY ARE EXPECTED TO PARTICIPATE IN FACULTY ACTIVITIES FULL-TIME ON-CAMPUS THROUGHOUT THE PROGRAM.

Question 8: Answer the following questions

1) What key is found? 25

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

3) Why successful/Why not successful? not

Question 9: Try to break the following Caesar ciphers using **"Caesar_Analysis.cwm"**.

1) ciphertext= **"hwt HtAA HtpHwtAA DC lwt HtpHwDGt"**

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

1.2) What is the 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 bruteforce 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 Cryptography

AES

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

1) Cryptographic Algorithm? AES

2) Action? encrypt

3) Block size? 128 bit

4) Key size? 128 bit

5) Mode of operation? Electronic code book (ECB)

6) Padding method? Zeros

Question 11:

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

2) What do you think happen?
Cann't open this file.jpg

Question 12: Display logo-title.jpg and logo2.jpg together, and compare both images.

1) Can **"logo2.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) How to change the settings in current workspace to perform AES encryption **with OFB mode of operation**?

AES encryption is work to encryption but AES decryption’s not work