LAB 1:
INTRODUCTION TO *CRYPTOGRAPHY*

[ITCS461]

Computer and Communication Security

Mahidol University

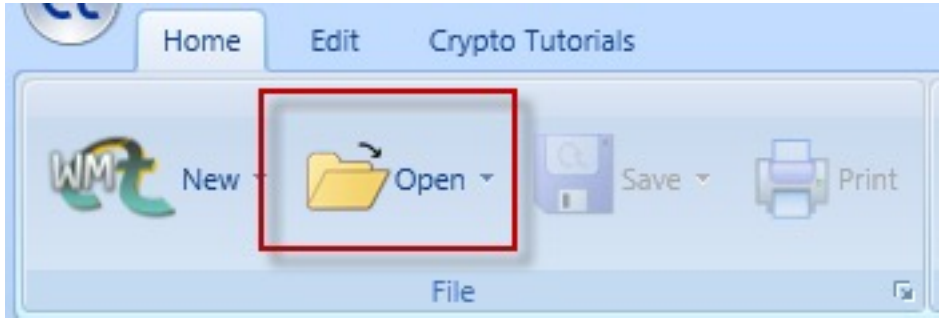
Mahidol University

SETUP: BEFORE YOU START

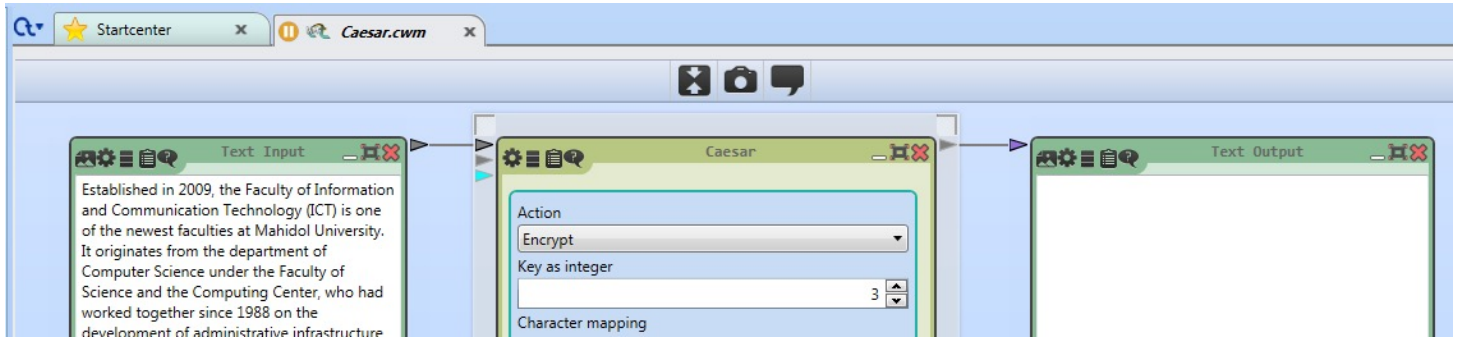
1) Download and install Cryptool 2 (stable ver.) from https://www.cryptool.org
2) Download and unzip Lab_1.zip from MyCourse (or other channel as instructed)
3) Use the MS Word file “Lab1_answer_sheet.docx” for answering questions in this lab
4) Good Luck Have Fun (GLHF) :D

PART 1: CLASSICAL CRYTOGRAPHY

1) Open Cryptool 2 and load the workspace “Caesar.cwm” from the extracted files in Lab 1.zip



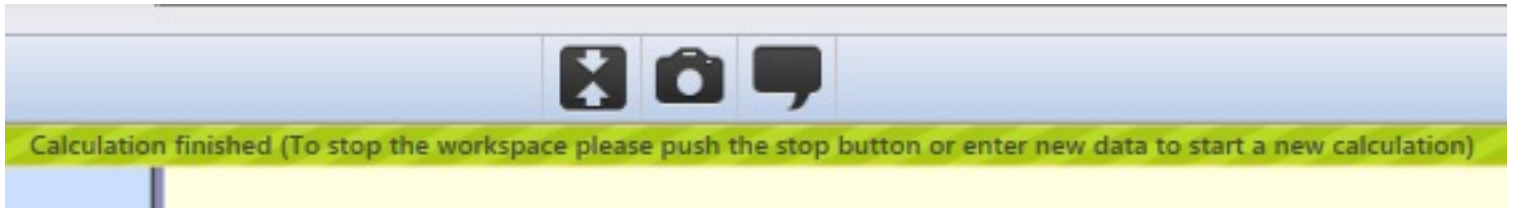
2) The workspace is configured such that the plaintext will be encrypted using Caesar Cipher.



PART 1-1: CLASSICAL CRYTOGRAPHY

- Click “Play” to see the result of this encryption on the text output window

- When the program says “Calculation finished”, click “Stop” and examine the result.



- **>> Answer question 1-3**

PART 1-2: CLASSICAL CRYTOGRAPHY

1) Load a workspace called “Frequency Analysis.cwm”
2) Click “Play”, let the program finishes, and click “Stop”. Then, observe the output graph.
3) **>> Answer question 4**

PART 1-2: CLASSICAL CRYTOGRAPHY

1) Open the Internet browser and go to the link https://www.ict.mahidol.ac.th/history/
2) Copy the text on history page (red area)
3) Paste the text into the input box in Cryptool abd click “Play” then observe the result.
4) **>> Answer question 5-6**

Established on 20th May 2009, the Faculty of Information and Communication Technology stems from the Department of Computer Science under the Faculty of Science and Computing Center, which have cooperatively worked together in the development of computing infrastructure and software for university administration and in computing research since 1988. Recognizing the significance of information and communication technology development in Thailand, Mahidol University has established the Faculty of ICT with the mission to meet the growing domestic and global needs for qualified human resources in computer technology.

Areas in Information and Communication Technology have grown to encompass many aspects of computing technologies, and it now covers many emerging technologies such as cloud computing, data analysis embedded systems, software engineering, and intelligent systems.

Today the demand for ICT professionals is greater than ever, and graduates are required to have both background in theoretical concepts and practical experience. The main mission of the Faculty of ICT is to produce computer scientists and ICT professionals having high research and development caliber.

PART 1-2: CLASSICAL CRYTOGRAPHY

1) Load “Caesar_Analysis.cwm” workspace. This workspace illustrates cryptanalysis of Caesar cipher using frequency analysis. Click “Play” to attack this ciphertext then “Stop”.
   >> Answer question 7

2) Switch back to “Caesar.cwm” workspace. Try encrypt current text with Key=21 then copy the result ciphertext and paste to text input box of “Caesar_Analysis.cwm”. Run the attack again.
   >> Answer question 8

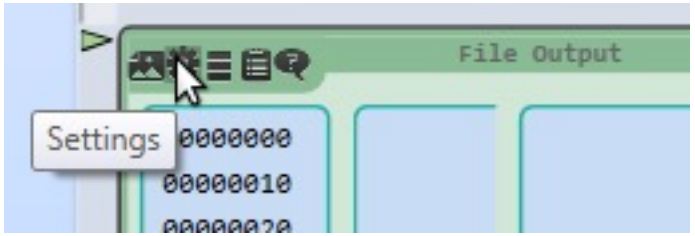
3) Try solving the **challenge in question 9**

PART 2: MODERN CRYTOGRAPHY

- Go to the history page again and save an image inside this page (or any JPEG image as instructed) to your computer, and name it "picture_1.jpg"
- **>> Answer question 10**

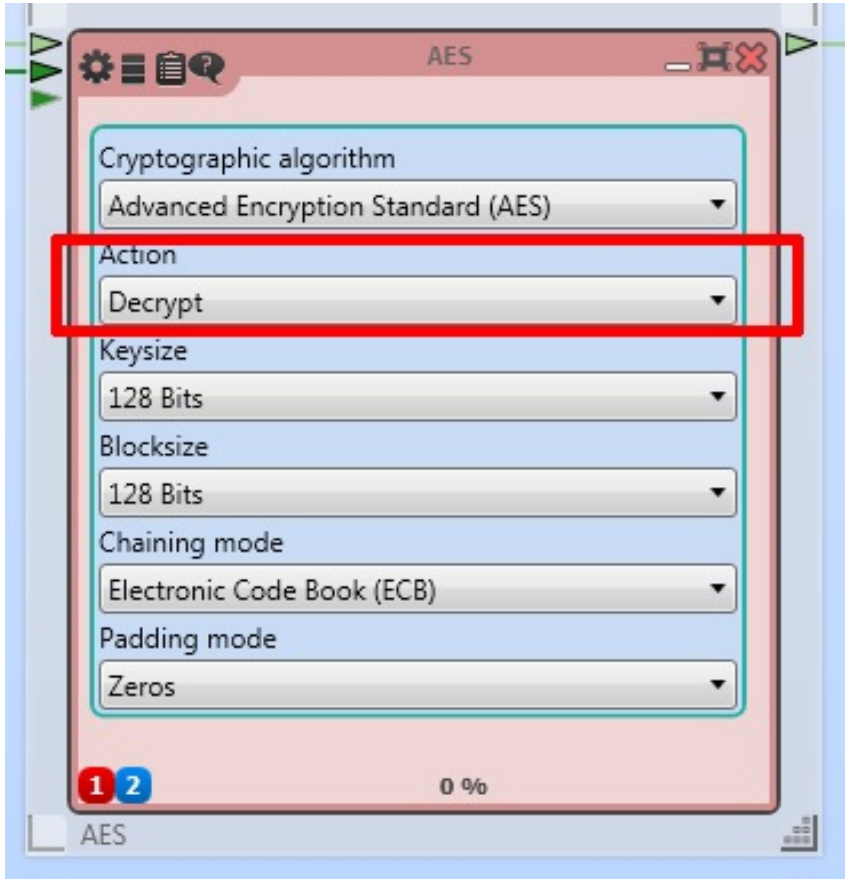
PART 2: MODERN CRYTOGRAPHY

- Try to encrypt the saved file (picture_1.jpg) on your computer by selecting the location of the input file (clicking at the setting icon of the File input window) and the output file (e.g., "picture_1_encrypted.jpg") and then click "**Play**".
- Locate the output file and try to display the encrypted file.
- **>> Answer question 11**



PART 2: MODERN CRYTOGRAPHY

- Now, let's decrypt the "picture_1_encrypted.jpg" file that we just created, back to the original format.
- To do that, we can use the same workspace. First, change the "Action" to "Decrypt". Then select the input file to be the encrypted file ("picture_1_encrypted.jpg") and output file to be a file with any name different from the original file name (don't forget to put the format .jpg after the name, e.g. picture_1_decrypted.jpg).
- **>> Answer question 12**



BEFORE YOU LEAVE

- Write your **name** and **student ID**
- Don't forget to save the answer file in **PDF format**
- And submit it to MyCourse website (or any channel as instructed by the lecturer) in the folder according to your section