

SECR3443 INTRODUCTION TO CRYPTOGRAPHY (Lab 1)

Name : _____
 Student ID : _____
 Name : _____
 Student ID : _____
 Section / Group : _____

Marks

INSTRUCTIONS:

Watch the following 10-minutes short video about the Polyalphabetic Cipher using Vigenere Encryption, and the Kasiski analysis used in cryptography. Then, complete the following tasks in group A or B.

Link: <https://youtu.be/LsewLHTAmsA>

TASK 1 : VIGENERE CIPHER

Based on Vigenere Cipher:

(a)	Encrypt "CYBER DEFENSE SHIELD" using the first 5 characters of your name. Show your encryption table as shown in the video (Deliverable: One table for each member).	[5 marks]
(b)	Write any English text with 100 length, encrypt with 5 to 7 characters of your own chosen keyword. (Deliverable: One encrypted text for each group A or B).	[5 marks]
(c)	Exchange the encrypted text in (b) with another pair of your group (exchange between group A and B). Keep secret your keyword and plaintext from other group.	

TASK 2 : KASISKI ANALYSIS

(d)	Based in task 1(c), calculate the factors of the keyword used. Show the occurrence table . (Deliverable: One table for each group A or B).	[5 marks]
(e)	Find the keyword used and the plaintext. Show the decrypted table . (Deliverable: One decrypted table for each group A or B).	[5 marks]

Note: You may use MS Excel to perform the encryption and decryption. Show your detail working.