THE UNIVERSITY OF NEWCASTLE AUSTRALIA

SCHOOL OF INFORMATION AND PHYSICAL SCIENCES

SENG2250 System and Network Security
School of Information and Physical Sciences

SENG2250/6250 System and Network Security

Assignment 1

This assignment is to be done individually.

*Due on **Sunday, 20 August 23, 11:59pm**, electronically via the "Assignment 1" submission link in Canvas.*

Total 100 marks

Aims

This assignment aims to establish a basic familiarity with security primitives and attacks by analysing, demonstrating solutions using cryptography.

Guidelines

For each of the following questions, you are allowed to use programming methods to answer questions. Additionally, you may use Large Language AI models (e.g., ChatGPT), although if you do so, please refer to the "Using Generative AI.pdf" file found on Canvas, this document provides advice to better use the toolset and formatting advice for answering questions.

Questions

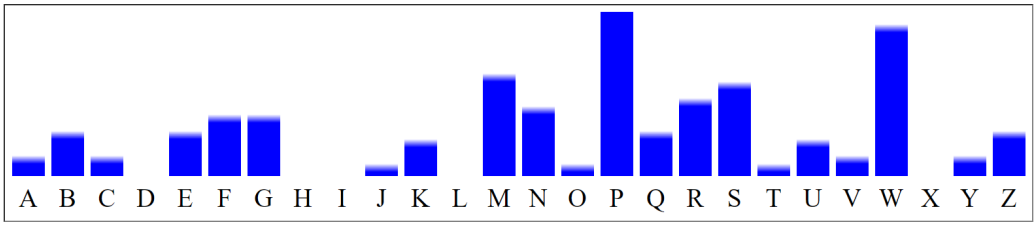
1. (20 Marks) Cryptanalysis on Substitution Ciphers

A monoalphabetic substitution cipher generates the ciphertext below. Perform cryptanalysis and find the plaintext. Note that the plaintext only includes meaningful English word(s)/sentence(s).

Ciphertext

wep umpp rgmusfp br znj rwmpwfepk ngw wn s qsmyp powpzw agw sffnmkbzy wn ngm srrgvcwbnz wep vswpmbsqr grpk smp cpmupfwqt rwmpwfesaqp.

Ciphertext letter frequency



a. (**5 Marks**) Find the plaintext.
b. (**15 Marks**) Show your process of finding (at least) FIVE plaintext letters.

2. (80 Marks) Block Cipher and Operation Modes

For this question, you will demonstrate your understanding of block cipher modes operation by using an AES encryption calculator and demonstrating the Counter (CTR) mode of operation.

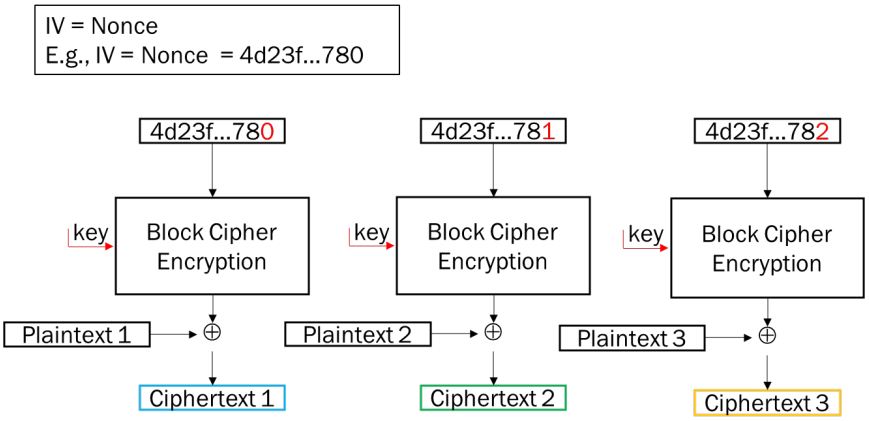


Figure: CTR Encryption

You may either answer by using hand calculations of the mode of operations functionalities assisted by an AES encryption (as a Block Cipher Encryption) calculator:
https://www.hanewin.net/encrypt/aes/aes-test.htm

or develop a program that takes an underlying AES cryptosystem in ECB-mode and uses it to implement the CTR mode. In the latter case, you will need to find how to use the AES cryptosystem for your language of choice (e.g., AES is in java's standard java.security, while python requires an external library such as PyCryptoDome), ensure that it is used in the ECB mode of operation.

a. (**10 Marks**) Create a 256-bit key and a 512-bit plaintext (all in hexadecimal).
The key should start with your student ID. For example, if your student ID is C1234567, then your key can be:

C1234567EDEEEFF0F2F3F4F5F7F8F9FAC1234567EDEEEFF0F2F3F4F5F7F8F9FA

b. (**10 Marks**) Specify an Initialisation Vector (IV). An IV cannot be a trivial string like all 0s or 1s. An IV is a nonce and a nonce often includes a timestamp.
c. (**30 Marks**) Demonstrate the encryption process of each block in the CTR-AES. You can use the AES encryption calculator to show the block cipher encryption result without providing the encryption detail.

d. (**5 Marks**) Show the entire ciphertext of 512 bits.
e. (**5 Marks**) Please use the following format for your answers. Note that the Result of XOR may need to be moved depending on the mode of operation in use.

Sample Input/Output Format:

Entire Plaintext: XXXX…XXXX
Key: XXXX…XXXX
IV: XXXX…XXXX

Block 1:
Input of AES: XXXX…XXXX
Output of AES: XXXX…XXXX
Result of XOR: XXXX...XXXX

Block 2:

Input of AES: XXXX…XXXX
Output of AES: XXXX…XXXX
Result of XOR: XXXX...XXXX

…

Entire Ciphertext: XXXX…XXXX

f. (**20 Marks**) The avalanche effect is a property of some block cipher cryptosystems where a small change to the plaintext leads to a major change to the resulting ciphertext. Choose a 128-bit plaintext and encrypt it using a single block of AES (in normal ECB mode) with the key chosen earlier, also produce ciphertext the same way with **five unique 1-bit flips** of the plaintext (e.g., if the plaintext is 101, then a 1-bit flip could be 111, 100, or 001). Does AES have the avalanche effect? Use your calculated ciphertexts as evidence.

Submission

All assignments must be submitted via Canvas. If you submit more than once, then only the latest submission will be graded. Your submission should be a **PDF** file containing answers to all questions, including any code and output used to answer any questions. Also, follow the instructions on “Using Generative AI.pdf” file found on Canvas if you have used any AI tool.

The mark for an assessment item submitted after the designated time on the due date, without an approved extension of time, will be reduced by 10% of the possible maximum mark for that assessment item for each day or part day that the assessment item is late. **Note: this applies equally to week and weekend days.**

Plagiarism

A plagiarised assignment will receive ZERO marks (and be penalised according to the university rules).

Note: Handwritten submission will NOT be accepted for this assignment.