SENG2250 System and Network Security
School of Information and Physical Sciences
Semester 2, 2022

Assignment 1 (100 marks, 10%) - Due: 21 August, 23:59

Aims

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

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

Questions

1. Block Cipher and Operation Modes (30 marks)

Use an AES encryption calculator (e.g., https://www.hanewin.net/encrypt/aes/aes-test.htm) to demonstrate the **Counter** mode (CTR) with **AES** (CTR-AES).

a. Create a 256-bit key and a 512-bit plaintext (all in hexadecimal). (**5 marks**)

The key should start with your student ID. For example, if your student ID is C1234567, then your key can be:

C1234567EDEEEFF0F2F3F4F5F7F8F9FAC1234567EDEEEFF0F2F3F4F5F7F8F9FA

b. Specify an Initialisation Vector (IV). An IV cannot be a trivial string like all 0s or 1s. (**5 marks**)

c. Demonstrate the process of each round in the CTR-AES. You can use the AES encryption calculator to show the block cipher encryption result without providing the encryption detail. (**15 marks**)

d. Show the entire ciphertext of 512 bits. (**2 marks**)

e. Please use the following format for your answers. (**3 marks**)

Sample Format

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

Round 1:
Input of AES: XXXX…XXXX
Output of AES: XXXX…XXXX

Round 2:
Input of AES: XXXX…XXXX
Output of AES: XXXX…XXXX

…

Entire Ciphertext: XXXX…XXXX

2. Brute-Force Attacks (25 marks)

Suppose that a language "X" has **28** different letters. Answer the following questions.

a. Alice wants to use a 10-letter password (case insensitive). Each password character is **randomly selected** from **28** possible letters. How many different passwords can be generated? (**5 marks**)

b. Suppose that an adversary can attempt passwords at a rate of **four million per second**. If an adversary can immediately know an attempted password's correctness, what is the **expected** time (i.e., average time) to reveal Alice's password generated above? Convert the time to the number of seconds. (**8 marks**)

c. Suppose that Bob uses a monoalphabetic substitution cipher (regarding the language "X") to encrypt a message. Assume the redundancy of the plaintext "X" is **4.5**. How many ciphertext characters are needed to identify a unique key? (**12 marks**)

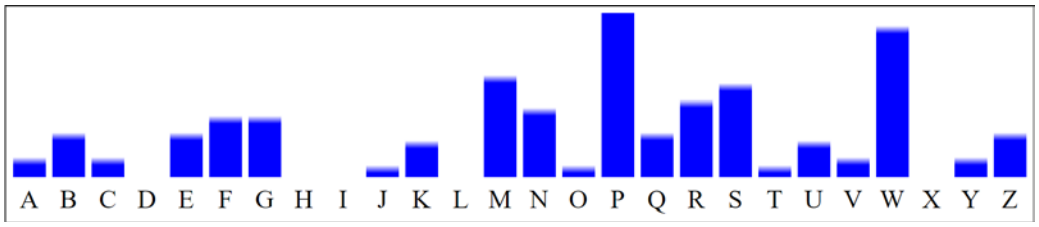
3. Cryptanalysis on Monoalphabetic Cipher (25 marks)

A monoalphabetic substitution cipher generates the ciphertext below. Perform cryptanalysis and find the plaintext. Note that the plaintext only includes meaningful English 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. Find the plaintext. (**5 marks**)

b. Show your process of finding (at least) FIVE plaintext letters. (**20 marks**)

4. Hash Functions (20 marks)

a. Let h be a secure one-way hash function. Given a set $\{v_1, v_2, v_3, v_4, v_5\}$, such that

$$v_1 = h(x);\ v_2 = h(v_1);\ v_3 = h(v_2);\ v_4 = h(v_3);\ v_5 = h(v_4).$$

Suppose v_3 is known, can we compute any of the others in $\{v_1, v_2, v_4, v_5\}$? If yes, show how; otherwise, explain why. (**10 marks**)

b. Let (e, n) be an RSA public key, and (p, q, d) be the corresponding private key. The public key (e, n) is known to everyone, but NO ONE knows the private key (p, q, d). Consider a message m,

1) If $0 < m < n$, can we use the RSA encryption algorithm as a one-way hash function? Justify your answer (**5 marks**)
2) If $m > n$, can we use the RSA encryption algorithm as a cryptographic hash function? Justify your answer. (**5 marks**)

Submission

All assignments must be submitted via Canvas. If you submit more than once, then only the latest will be graded. Your submission should be a **PDF** file containing answers to all questions.

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).