SENG2250 System and Network Security
School of Electrical Engineering and Computing
Semester 2, 2020

Assignment 1 (100 marks, 10%) - Due: 30 August, 23:59

Aims

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

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

Questions

1. Brute-Force Attacks (20 marks)

Assume that a password consists of 7 characters. Each password character is **randomly selected** from 42 possible characters. Answer (in detail) the following questions.

a. How many different passwords can be generated? (**5 marks**)

b. Suppose that an adversary can attempt **passwords** at a rate of **one 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 the correct password? Convert the time to the number of **days**. (**7 marks**)

c. Suppose that an adversary can attempt **password characters** at a rate of **two million per second**. If an adversary can immediately know an attempted password character's correctness, what is the expected time to reveal the correct password? (**8 marks**)

2. Block Cipher and Operation Modes (25 marks)

Use an AES encryption calculator (https://www.hanewin.net/encrypt/aes/aes-test.htm) to demonstrate the CBC mode with AES (CBC-AES).

1) Give (freely choose) a **128**-bit key and a **512**-bit plaintext (all in hexadecimal).
2) Specify an Initialisation Vector (IV). An IV cannot be a trivial string like all 0s or 1s. (**5 marks**)
3) Demonstrate the process of each round in the CBC-AES. You can use the AES encryption calculator to show the block cipher encryption result without providing the encryption detail. (**15 marks**)
4) Show the entire ciphertext of 512 bits. (**2 marks**)
5) Please use the following format for your answers. (**3 marks**)

Sample Format

Key: XXXX…XXXX
Plaintext: XXXX…XXXX
IV: XXXX…XXXX
Round 1:
Input to AES: XXXX…XXXX
Output of AES: XXXX…XXXX

…

Round n:

Input to AES: XXXX…XXXX
Output of AES: XXXX…XXXX

Entire ciphertext: XXXX…XXXX

3. Hash Functions and Digital Signatures (25 marks)

a. Let H be a secure one-way hash function. Given a set $\{K_1, K_2, K_3, K_4, K_5\}$, such that

$$K_1 = H(x);\ K_2 = H(K_1);\ K_3 = H(K_2);\ K_4 = H(K_3);\ K_5 = H(K_4).$$

Suppose K_3 is known, can we compute any of others in $\{K_1, K_2, K_4, K_5\}$? If yes, show how; otherwise, explain why. (**10 marks**)

b. Alice says she comes from the future by time machine. To demonstrate her power, she will predict an event that will happen soon. Alice makes a message

$$M = Event\ ||Time\ ,$$

Where || is concatenation. Alice will tell people the $Time$, but she cannot leak the $Event$ to people before it occurs. Otherwise, history may be changed. Find a solution to satisfy the requirements as follows.

1) People can check the correctness of the prediction M at the $Time$, but not beforehand. (**5 marks**)
2) Alice has a **negligible** chance to make a correct prediction if she does not know the $Event$. (**5 marks**)
3) Alice cannot deny the prediction she made, no matter it is correct or incorrect. (**5 marks**)

Justify your solution about the above three requirements, otherwise, you may significantly lose marks.

4. Cryptanalysis on Monoalphabetic Cipher (30 marks)

The ciphertext below is generated by the monoalphabetic substitution cipher. Perform a cryptoanalysis and find the plaintext. Note that the plaintext only includes meaningful English sentence(s).

Ciphertext:

UIFSF JT B TUPSZ BCPVU UXP QFPQMF XIP EFDJEFE UP QMBZ B HBNF JO XIJDI UIF POF XIP DBMMT UIF MBSHFTU OVNCFS XJOT

Letter frequency of the ciphertext

Letter	U	I	F	S	J	T	B	P	Z	C	V	X	Q	M	E	D	H	N	O
Count	8	7	12	4	5	5	7	8	2	2	2	5	3	5	3	3	2	2	4

- Find the plaintext. (**5 marks**)
- Show your process for at least FIVE plaintext letters recovery. (**25 marks**)

Submission

All assignments must be submitted via Blackboard (Assessment tab for SENG2250). If you submit more than once, then only the latest will be graded. Your submission should be one ZIP file containing:

- Assessment item cover sheet.
- A PDF file that contains 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).