COMP5631/CSIT5710: Cryptography and Security
2019 Fall – Written Assignment Number 1
Handed out: on September 18 for COMP5631 students and
September 20 for CSIT5710 students
Due: on Sept. 26 for COMP5631 students and
Sept. 27 for CSIT5710 students at the *beginning* of the lecture

Assignments handed in during class will lose marks. No assignments will be accepted after class. No email submission will be accepted.

Q1. Find the multiplicative inverse of 29 modulo 1137. Write down all steps of your computation. Please use the extended Euclidean algorithm, which is a slight modification of the Euclidean algorithm. 20 marks

Q2. You are given a piece of ciphertext with 10000 English letters whose original plaintext is a piece of English writing. You are told that the encryption was with either a transposition cipher or a simple substitution cipher. How do you detect the type of the cipher used for the encryption? 20 marks

Q3. There are ten pieces of ciphertext in the following URL:
[Click here]
Each of them is obtained by encrypting an English article with a simple substitution cipher. According to the last digit in your student ID number, please choose the corresponding ciphertext and recover the original message.

You may use the following online software to compute the frequencies of single letters, digraphs and trigraphs in the ciphertext for you:

[Click here]

Please write down details of your decryption process.

Programming project: Those who would like to do programming may write a computer program for computing the frequencies of single letters, digraphs and trigraphs in any ciphertext. This is not compulsory. It is your own decision whether you use the online software or write your own programs.

20 marks

Q4. Problem 1: We identify each English letter with an integer between 0 and 25 as follows:

A	B	C	$\cdots$	Y	Z
0	1	2	$\cdots$	24	25

Take any pair (k_0, k_1) of integers such that $\gcd(k_0, 26) = 1$ and $0 \leq k_i \leq 25$, and define the 1-to-1 mapping f by

$$f(x) = (xk_0 + k_1) \bmod 26.$$

So f is a permutation (substitution) of the English alphabet.

A **simple substitution cipher** based on f is a 5-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$, where

- $\mathcal{M}$ and $\mathcal{C}$ are the set of all finite strings of English letters;
- $\mathcal{K}$ is the set of all possible f;
- $k = (k_0, k_1) \in \mathcal{K}$ is the encryption and decryption key.
- For a message $m = m_0 m_1 m_2 \cdots$,

$$E_k(m) = f(m_0) f(m_1) f(m_2) \cdots$$

- For a ciphertext $c = c_0 c_1 c_2 \cdots$,

$$D_k(c) = f^{-1}(c_0) f^{-1}(c_1) f^{-1}(c_2) \cdots$$

Use the secret key $(k_0, k_1) = (3, 1)$ to encrypt the message "cryptography" (25 marks)

Q5. Consider the 8-bit CFB mode of DES, where $n = 64$ and $t = 8$. If a bit error occurs in the transmission of a ciphertext character (i.e., a block of one byte), how far does the error propagate in the decrypted plaintext characters? Justify your answer. (20 marks)