COMP 4140 (Fall 2022) Assignment 1

This assignment covers materials from weeks 1 and 2 of the lectures.

Instructions:

- Answer all questions.
- If a question has multiple parts, please label these parts appropriately. Eg. Question 1, Part a.
- Please underline your final answer(s).
- Show your work. Your grade will depend not only on the final answer provided, but also on the calculations and work provided to reach the your final answer.
- Your submission can be either hand-written or typed. If you submit hand-written solutions, ensure they are legible.
- Ensure that your submission to crowdmark is correctly oriented.

Due date: Thursday September 29, by 11:59 PM (CST). Late assignments will be accepted up to 1 hour after due date/time without penalty. After that, assignmets will not be accepted.

NOTE: This pdf copy of the assignment questions is provided for your convenience only. Your assignment submission must be done using Crowdmark. You will be emailed a link to crowdmark once it's available.

Assumptions:

1. Unless otherwise explicility stated, you may assume keys in $\mathcal{K}$ are uniformly distributed in the questions below. That is, the key generation algorithm Gen selects each key in $\mathcal{K}$ with probability $1/|\mathcal{K}|$.
2. Unless otherwise explicility stated, you may assume for any distributions on $\mathcal{M}, \mathcal{C}$ that $\Pr[M = m] > 0, \Pr[C = c] > 0$ for all $m \in \mathcal{M}, c \in \mathcal{C}$ in the questions below.

Question 1: (4 marks)

Let n be a positive integer and consider the minor modification of the n-bit one-time pad scheme: The message space $\mathcal{M}$ and keyspace $\mathcal{K}$ are modified by removing the string 1^n (the binary string of n 1's) from them. The remaining keys are chosen uniformly and randomly by the key generation algorithm. Answer the following parts.

a. In this modified scheme, is $\Pr[C = 1^n] = 0$? Why or why not?

b. Is this (slightly) modified version of the one-time pad still perfectly secret? If it is perfectly secret, give a proof using one of the three equivalent definitions. If it is not perfectly secret, give a counterexample.

Question 2: (5 marks)

Consider the encryption scheme with $\mathcal{M} = \{0, 1, 2, 3, 4\}$ with some probability distribution on $\mathcal{M}$ where Gen returns a uniform key from the key space $\mathcal{K} = \{0, 1, 2, 3, 4, 5\}$ (note that there are **6** keys in $\mathcal{K}$). The algorithms $\mathsf{Enc}_k(m)$ returns $m + k \pmod 5$ and $\mathsf{Dec}_k(c)$ returns $c - k \pmod 5$.

If the message space is given the uniform distribution, answer the following questions:

a. Compute $\Pr[M = 0]$.

b. Compute $\Pr[C = 1]$.

c. Compute $\Pr[C = 1 | M = 0]$.

d. Compute $\Pr[M = 0 | C = 1]$.

e. Is this scheme perfectly secret? Explain.

Question 3: (4 marks)

Consider the following statement.

If an encryption scheme is perfectly secret, then for every distribution over the message space $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$ and every $c \in \mathcal{C}$, the following equality holds:

$$\Pr[M = m_0 | C = c] = \Pr[M = m_1 | C = c].$$

Is this statement true? Prove or refute the statement.

Question 4: (4 marks)

Consider the following encryption scheme that encrypts a one-bit message using a uniformly chosen bit as the key and produces a 2-bit ciphertext as follows:

Let m be the 1-bit plaintext message and k be the 1-bit key. Define $\mathsf{Enc}_k(m) = (m \oplus k)||b$ where b is 0 with probability 3/4 and 1 with probability 1/4. The symbol $||$ means concatenation.

a. Is this encryption scheme perfectly secret? *Hint*: Use the second definition of perfectly secret.

b. Is it true that for every (2-bit) ciphertexts c_1, c_2, the equality $\Pr[C = c_1] = \Pr[C = c_2]$ holds?

Question 5: (4 marks)

Let Π be denote the Vigenere cipher where the message space consists of all 3-character strings (over the English lowercase alphabet), and a key is generated by first choosing the period t uniformly from $\{1, 2, 3\}$ and then letting the key be a uniformly chosen random string of length t.

Consider the following adversary $\mathcal{A}$ that outputs $m_0 = \mathsf{aab}$ and $m_1 = \mathsf{abb}$. When the adversary is given ciphertext c, it outputs 0 if the first character of c is the same as the second character of c. Otherwise, it outputs 1.

Compute the value $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]$.

Question 6: (4 marks)

Suppose you have in your possession two 40-bit ciphertexts c_1, c_2 as given

$c_1 =$ 11111001 01111001 11001100 00010111 10000110

and

$c_2 =$ 11111010 01100111 11011101 00001001 10001000.

The spacing between bits is provided for readability only.

You also know that both generated using the one-time pad scheme using the *same* key. In addition, you know that exactly one of the following is true:

1. c_1 is an encryption of the string alpha and c_2 is an encryption of the string bravo, or
2. c_1 is an encryption of the string delta and c_2 is an encryption of the string gamma.

The 40-bit plaintext messages are obtain by taking the ASCII code of a character and converting it to its binary representation. Eg. the character a is represented in the plaintext message by 01100001.

The questions are:

a) Which of the two possible choices (1. or 2.) given above is correct?

b) What is the 40-bit key used? Give final answer using hexadecimal notation.

Question 7: (Not Graded)

Decrypt the following ciphertext generated by a substitution cipher. Spaces and punctuations have been included to aid the cryptanalysis process. This datafile is available as *a1-data.txt* on UMLearn page.

yh stn hxe uenh gf hypen, yh stn hxe sgonh gf hypen, yh stn hxe tbe gf syncgp, yh stn hxe tbe gf fggqynxdenn, yh stn hxe ewgax gf ueqyef, yh stn hxe ewgax gf ydaoecjqyhl, yh stn hxe netngd gf qybxh, yh stn hxe netngd gf ctordenn, yh stn hxe nwoydb gf xgwe, yh stn hxe sydheo gf cenwtyo, se xtc eieolhxydb

uefgoe jn, se xtc dghxydb uefgoe jn, se seoe tqq bgydb cyoeah hg xetied, se seoe tqq bgydb cyoeah hxe ghxeo stl — yd nxgoh, hxe weoygc stn ng fto qyre hxe woenedh weoygc, hxth ngpe gf yhn dgynyenh tjhxgoyhyen ydnynhec gd yhn ueydb oeaeyiec, fgo bggc go fgo eiyq, yd hxe njweoqthyie ceboee gf agpwtoyngd gdql.