Assignment 1

Policy: You may discuss problems with others, but all written work submitted must be your own. *You may not copy nor solicit solutions, complete or partial, from any source.*

1. Alice and Bob want to write encrypted messages to a diary so that after decrypting the message they will know who wrote which message. They decide on the following method:
   1. All messages of Alice will start with n 0s; whereas
   2. All messages of Bob will end with n 0s; and
   3. No one will write the message containing all 0s.

   So if Alice wants to write a message m to the diary, she will encrypt the message $0^n||m$ where 0^n is a string of n 0s, and $||$ denotes concatenation. Likewise, Bob's messages will be of the form $m||0^n$. Assume that m is also of length n and $m \neq 0^n$. Note that with this encoding, each string that Alice and Bob write in the diary is of length $2n$ and it is never 0^{2n}.

   To encrypt their messages Alice and Bob agree to use the "one-time" pad and jointly select a random key k of length $2n$ which they will use to encrypt and write their messages to the diary.

   Show how to decrypt all the messages in the diary without knowing the key k as soon as both Alice and Bob written one string each in the diary. Also, show how to recover the key k. (You can assume the adversary knows who writes messages in which way.)

2. Two 8-bit strings m_1 and m_2 were sent after each being encrypted with a "one-time" pad using the same 8-bit key k. We see the resulting ciphers $c_1 = 10010010$ and $c_2 = 10110000$. We are pretty sure that either m_1 and m_2 are the ASCII binary codes for either 'M' (01001101) and 'o' (01101111) respectively; or 'I' (01001001) and 'l' (01101100) respectively. They were sending the letters of the abbreviation of Missouri (Mo) or Illinois (Il). Which is correct? What was the key k?

3. When using the one-time pad with the key $k = 0^n$, it follows that $Enc_k(m) = m$, and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^n$ (i.e. to have Gen choose k uniformly at random from the set of non-zero keys of length n). Is this an improvement? In particular, is it still perfectly secret? Prove your answer.

4. We will consider how secure the two historical ciphers in the text are. Our message space will be strings of the English alphabet.

(a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

(b) What is the largest message space $\mathcal{M} \subseteq \{a, b, \ldots, z\}^5$ (all 5-letter strings) you can find for which the mono-alphabetic substitution cipher provides perfect secrecy?

5. Prove an analogue of Shannon's Theorem for the case of "almost perfect" secrecy. That is, let $\epsilon < 1$ be a constant and say that we only require that for any distribution over $\mathcal{M}$, any $m' \in \mathcal{M}$, and any $c \in C$;

$$\left| P[m = m' \mid Enc_k(m) = c] - P[m = m'] \right| \leq \epsilon.$$

Prove a lower bound on the size of the key space $\mathcal{K}$ relative to $\mathcal{M}$ for any encryption scheme that meets this definition.

Hint 1: For simplicity, assume the uniform distribution over $\mathcal{M}$ and assume that for each k, Enc_k is deterministic. Note that the lower bound should agree with Shannon's Theorem for the case $\epsilon = 0$.

Hint 2: Note that for a given message m and a cipher c, if there is a key k such that $Enc_k(m) = c$, this key is not necessarily unique. You may want to first see what bound you can arrive at when you assume that the key would be unique, then try to drop this assumption.