COMP 4140 Assignment 1

Question 1

Let $n \in \mathbb{Z}^+$. One time pad scheme is modified to remove the binary string 1^n from M and K. Remaining keys are chose uniformly and randomly by the key generation algo.

a) In the modified scheme, is $Pr[C=1^n]=0$?

No. Let $k=1 \cdot 0^{n-1}, m=0 \cdot 1^{n-1}$. With this key and message, the ciphertext resulting from the one-time pad scheme is 1^n. Since $k \in K, m \in M$, $Pr[M=m]>0$, and since k is uniformly distributed, $Pr[C=1^n]>0$

b) Is the modified scheme still perfectly secret? If so, prove. Otherwise, give counterexample.

It is not perfectly secret. Counterexample:
Find messages $m_1, m_2 \in M$ and ciphertext c such that $Pr[Enc_K(m_1)=c] \neq Pr[Enc_K(m_2)=c]$
Let $m_1=0^{n-1} \cdot 1, m_2=0^n$
Let $c=1^n$
$Pr[Enc_K(m_1)=c]=\frac{1}{2^n-1}$
$Pr[Enc_K(m_2)=c]=0$
Therefore the modified scheme is not perfectly secret.

Question 2.

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

With a uniform distribution, $Pr[M=0]=\frac{1}{5}=0.2$

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

(m,k) pairs such that m+k=1: 6
Total number of possible pairs: 5*6=30
Therefore $Pr[C=1]=\frac{6}{30}=0.2$.

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

(m,k) pairs such that 0+k=1: 1
Total number of possible keys: 6
$Pr[C=1|M=0]=1/6=0.1666$

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

(m,k) pairs such that 0+k=1: 1
Total number of possible keys: 6

e) Is this scheme perfectly secret? Explain.

No. The equality $Pr[M=m|C=c]=Pr[M=m]$ does not hold for this scheme.
Choose $m=1$ and $c=1$.
There are 6 (m,k) combinations for which $m+k(mod\,5)=1$. Of those, two have $m=1$. Therefore $Pr[M=m|C=c]=\frac{2}{6}=\frac{1}{3}$.

The message space has uniform distribution, so $Pr[M=m]=\frac{1}{5}=0.2$.

Therefore this scheme is not perfectly secret.

Question 3.

Prove or refute that if an encryption scheme is perfectly secret, then for every distribution over the message space M, every $m_0, m_1 \in M$ and every $c \in C$ the following statement holds: $Pr[M=m_0|C=c]=Pr[M=m_1|C=c]$.

Suppose that there is a non-uniform distribution over the message space M. Then there exists $m_0, m_1 \in M$ such that $Pr[M=m_0] \neq Pr[M=m_1]$. Since the encryption scheme is perfectly secret, by definition $Pr[M=m|C=c]=Pr[M=m]$ is true for all m. Supstituting m_0 and m_1 for m and plugging into the previous inequality gives $Pr[M=m_0|C=c] \neq Pr[M=m_1|C=c]$. Therefore $Pr[M=m_0|C=c]=Pr[M=m_1|C=c]$ does not hold for every distribution over M for a perfectly secret scheme.

Question 4.

Consider the encryption scheme that encrypts one-bit messages using a uniformly chosen one-bit key and produces a 2-bit ciphertext where $Enc_k(m)=(m \oplus k) \| b$ where $Pr[b=0]=0.75$ and $Pr[b=1]=0.25$

a) Is this encryption scheme perfectly secret?

By the second definition of perfect secrecy, the following statement must hold for every $m, m' \in M$ and $c \in C$: $Pr[Enc_K(m)=c]=Pr[Enc_K(m')=c]$.

Select arbitrary $m, m' \in M$ and ciphertext $c \in C$. Let $c=c_0 \cdot c_1$ where $c_0=m \oplus k$ and c_1 is the randomly chosen bit. For each of m and m' there is one key that will generate c_0. That key is selected with probablility 0.5. c_0 is selected independently of the message or key. Both of these selection probabilities are independent of the message, therefore $Pr[Enc_K(m)=c]=Pr[Enc_K(m')=c]$.

b) Is it true that for every ciphertexts c_1, c_2 the equality $Pr[C=c_1]=Pr[C=c_2]$ holds?

No. Let $m_1, m_2=0$ and $k=0$. Encrypting m_1 and m_2 with k will result in $c_1=00$ and $c_1=01$, where $Pr[C=c_1]=0.75$ and $Pr[C=c_2]=0.25$. Therefore $Pr[C=c_1]=Pr[C=c_2]$ does not hold for every ciphertext.

Question 5.

Let Π be the Vigenere cipher where M is the set of all 3-char lowercase english strings. A key is generated by uniformly choosing $t \in \{1,2,3\}$ and then letting the key be a uniformly chosen random string of length t.

Consider an adversary A that outputs $m_0=aab$ and $m_1=abb$. 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 of $Pr[PrivK^{eav}_{A,\Pi}=1]$

$$
\begin{aligned}
&Pr[PrivK^{eav}_{A,\Pi}=1] \\
&=\frac{1}{2} Pr[PrivK^{eav}_{A,\Pi}=1|b=0]+\frac{1}{2} Pr[PrivK^{eav}_{A,\Pi}=1|b=1] \\
&=\frac{1}{2} Pr[A \text{ outputs } 0|b=0]+\frac{1}{2} Pr[A \text{ outputs } 1|b=1]
\end{aligned}
$$

When b=0, i.e. when $m_0=aab$ is encrypted, then the first encrypted character equals the second if 1) t=1, or 2) t=2 or t=3 and the first two characters of the key are equal. The former occurs with probability $\frac{1}{3}$ and the latter with probablility $\frac{2}{3}$.

$$Pr[A \text{ outputs } 0|b=0]=\frac{1}{3}+\frac{2}{3} \cdot \frac{1}{26}=0.359$$

When b=1, i.e. when $m_1=abb$ is encrypted, then the first encrypted character equals the second if t=2 or t=3 and the first character of the key is one greater than the second character.

$$Pr[A \text{ outputs } 1|b=1]=1-Pr[A \text{ outputs } 0|b=1]=1-\frac{2}{3} \cdot \frac{1}{26}=0.974$$

$$Pr[PrivK^{eav}_{A,\Pi}=1]=\frac{1}{2}\left(\frac{1}{3}+\frac{2}{3} \cdot \frac{1}{26}+1-\frac{2}{3} \cdot \frac{1}{26}\right)=\frac{2}{3}>\frac{1}{2}$$

* Libreoffice Writer doesn’t allow formula objects to be underlined

Question 6.

Given two 40-bit ciphertexts encrypted using the same key with the one-time pad scheme:
c 1 = 11111001 01111001 11001100 00010111 10000110
and
c 2 = 11111010 01100111 11011101 00001001 10001000.

Also, given that either c1 is an encryption of ‘alpha’ and c2 of ‘bravo’ OR c1 of ‘delta’ and c2 of ‘gamma’. Anwer the following:

a) Which of the two choices is correct?
b) What is the 40-bit key used, in hex notation?

One of the two following pairs of equations must be true:
Either
$\alpha \oplus k=c_1 \Rightarrow k=c_1 \oplus \alpha$ and $\beta \oplus k=c_2 \Rightarrow k=c_2 \oplus \beta$ which combines into $c_1 \oplus \alpha=c_2 \oplus \beta$
or
$\delta \oplus k=c_1 \Rightarrow k=c_1 \oplus \delta$ and $\gamma \oplus k=c_2 \Rightarrow k=c_2 \oplus \gamma$ which combines into $c_1 \oplus \delta=c_2 \oplus \gamma$

I wrote a python script to answer this. Here is the output:

```
alpha: 01100001 01101100 01110000 01101000 01100001
bravo: 01100010 01110010 01100001 01110110 01101111
delta: 01100100 01100101 01101100 01110100 01100001
gamma: 11111001 01111001 11001100 00010111 10000110
c1   : 11111010 01100111 11011101 00001001 10001000
c2   : 01100111 01100001 01101101 01101101 01100001

c1 xor alpha
key  : 10011000 00010101 10111100 01111111 11100111

c2 xor bravo
key  : 10011000 00010101 10111100 01111111 11100111

c1 xor delta
key  : 10011101 00011100 10100000 01100011 11100111

c2 xor gamma
key  : 10011101 00000110 10110000 01100100 11101001
```

The keys for
$c_1 \oplus \delta$ and $c_2 \oplus \gamma$ do not match! Only $c_1 \oplus \alpha=c_2 \oplus \beta$ holds. Therefore c1 is an encryption of ‘alpha’ and c2 is an encryption of ‘bravo’.

The key is:
9D 06 B0 64 E9