CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 1

Question 1

You intercept the following 2 transmissions (each byte represents an ASCII character).

Transmission 1:

```
01101110 00000100 11010100 11100100 01010000
01010001 11110110 00100011 01010100 10001000
00010110 00001100 01011111
```

Transmission 2:

```
01101110 00000100 11010100 11100100 01010000
01010001 11110110 00100011 01010100 10001001
00011000 00001100 00011011
```

You find out that both transmissions were encrypted with the same one-time pad.

1. Without any additional information, what can you say about the plaintext of the two transmissions?
2. You find out that the plaintext of the first transmission was "breaking code". Using this, recover the plaintext of the second transmission. (You may wish to use an online text-to-ASCII converter.)

Question 2

Why is the decryption algorithm for one-time pads the same as the encryption algorithm?

Question 3

Consider a symmetric cryptosystem where we split the plaintext P into two halves, P_1 and P_2. We also have a key K, which has the same length as P_1 and P_2. The ciphertext C is given by $C_1||C_2$, where we have:

$$C_1 = P_1 \oplus K$$
$$C_2 = P_2 \oplus C_1 \oplus K$$

(Here || denotes *concatenation*, so "a" || "b" = "ab").

1. Write a decryption algorithm to recover P given K and C.
2. Is this system semantically secure? Why or why not?
3. Is this system IND-CPA secure? Why or why not?

Question 4

A programmer wants to use the IP address of his computer's most recent network request as the seed for a CSPRNG. Explain why this is a bad idea.

Contributors:

- Ryan Cottone, Will Giorza