ENEE 457
One-Time Pad Class Exercise

1. What happens if we use the same one-time pad to encrypt two messages? What information will be leaked about the messages?

2. In a brute-force search, an attacker tries decrypting a ciphertext with each possible key until the correct key is discovered. Does a brute-force search attack work for the one-time pad? Why or why not?