**USC UPSTATE**

**CSCI 455: Computer Security**

**Spring 2019**

**Homework Assignment 2**

**Problem 1**

1. Describe how an attacker can obtain the one-time pad that is used to encrypt a message, given both the message and the ciphertext, and explain why your method works.
2. Suppose that two equal-sized messages *M*1 and *M*2 are encrypted with the *same* one-time pad and let *C*1 and *C*2 be the resulting ciphertexts. Suppose further that an attacker captures both ciphertexts *C*1 and *C*2, and knows one of the two messages, say *M*1. Based on Part a), describe how the attacker can obtain the other message *M*2, and explain why your method works.
3. Let’s think about a more realistic situation than part b) that the attacker captures both ciphertexts *C*1 and *C*2, but does not know message *M*1. Based on part b), can you provide an example showing that the attacker can still obtain the message *M*2 ? You can do research online and find approaches. By answering this question, you can have an idea on how an attacker can do in practice and why the one-time pad cannot be used more than once.