**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.

**Answer 1**

1. If the key is truly random, at least as long as the plaintext, never reused in whole or in part, and kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. Since the key can only have 2 possible values for each instance (Ki = (0 xor 1), you can use the message and ciphertext to determine what key was generated for each value in the plaintext. This will require some brute force but would eventually recover enough plaintext to intelligently fill out the rest. You would use M1 and C1 to determine K1 and so on.

<https://en.wikipedia.org/wiki/One-time_pad>

1. If you have C1 and C2 along with M1, you can use M1 and C1 to determine K and apply the key to decryption of C2. If the two encrypted messages are using the same cipher and the same key, C1 xor C2 results in M1 xor M2 where C1 and C2 are the respective ciphertext and M1 and M2 are the corresponding plaintext. Claude Shannon's "Communication Theory of Secrecy Systems.” You just continue this technique until you recover enough of the plaintext to intelligently fill out the rest. By comparing the ciphertext to the message, we could also draw some conclusions through testing and brute force approach to piece the key together.
2. If the two encrypted messages are using the same cipher and the same key, C1 xor C2 results in M1 xor M2 where C1 and C2 are the respective ciphertext and M1 and M2 are the corresponding plaintext. Claude Shannon's "Communication Theory of Secrecy Systems.” You just continue this technique until you recover enough of the plaintext to intelligently fill out the rest.

<https://crypto.stackexchange.com/questions/59/taking-advantage-of-one-time-pad-key-reuse>