**Georgia Gwinnett College**

**School of Science and Technology**

**ITEC 3300: Information Security**

**Homework Assignment 1**

**Problem 1 [20 Points]**

Implement the one-time pad encryption scheme in Microsoft Excel. Your worksheet should look as follows: ***see my Excel file <3***

* For Encryption:
  + Have the message occupy adjacent cells in one row, with one bit of the message in each cell.
  + Align the key (the one-time pad) with the message in the next row. Note that the key should be of the same length as the message.
  + In the next row, enter a formula that computes the ciphertext.
* Decryption is similar:
  + Have the ciphertext occupy adjacent cells in one row, with one bit of the ciphertext in each cell.
  + Align the key (the one-time pad) with the ciphertxt in the next row. Note that the key should be of the same length as the ciphertext.
  + In the next row, enter a formula that computes the plaintext (message).

**Problem 2**

1. **[15 Points]** 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. Because the cyphertext itself is the result of an exclusive or between the plaintext and the one-time pad, given both the cyphertext and the plaintext, the one time pad can be found by taking the exclusive or between the cyphertext and the plaintext:  
    **M ⊕ OTP = C, therefore C ⊕ M = OTP**  
     
    See my Excel file for my applied logic!
2. **[15 Points]** 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.

Like in part a., the attacker can find the same one-time pad by taking the exclusive or of C1 and M1, and then take the exclusive or of C2 and the shared one-time pad to gain M2, the second plaintext message. See my Excel file for my logic!

**Problem 3 [20 Points]**

Suppose that FJAV is the ciphertext of a *common English word* produced by the Shift Cipher, but the secret key is unknown. Can you determine the secret key and the plaintext (i.e. the original English word)? If so, give the secret key and the plaintext, and describe how you find them. **Secret Key: 9, Plaintext: WARM, found by brute-forcing the 25 possibilities of the value of the shift.**

**Problem 4**

Suppose that the Shift Cipher is modified so that for *each* letter of the message, a fresh random key is chosen and applied to shift just that letter.

1. **[30 Points]** Implement the modified scheme in Microsoft Excel. The implementation should be similar to that for the one-time pad scheme in Problem 1.  **See Excel Sheet <3**
2. **[20 Points]** (**For Extra Credit**) Does the modified scheme satisfy Shannon’s notion of perfect secrecy? Justify your answer. (**Hint**: Compare the modified scheme with the *one-time pad* scheme.)  
   **Because Shannon’s Notion of Perfect Secrecy is satisfied only if a.) the ciphertext has no statistical correlation with the plaintext, b.) for any ciphertext, its plaintext is equally likely to be any possible message, and c.) the ciphertext contains no information about the plaintext, and because this modified scheme does not mask the length of the original message, it technically does not satisfy the third rule of Shannon’s Notion. Compared to the One-time Pad method, the One-time Pad method does satisfy perfect secrecy SO LONG AS the one-time pad is used…. You guessed it…… One time. Leave it to computer scientists to make things so complicated! ;D**