**Matthew Austin**

**Principles of Cryptography (CIS-405)**

**Homework Assignment 2.**

**Question 1**

Complete Exercise 1 of Module 7: Transposition Ciphers Discussion Activity. For part 14 answer questions a through d

**Points: 4** (1 point each for steps a through d).

1. Now answer the following questions.
   1. Explain what is meant by a known plaintext attack?
      1. known-plaintext attack is an attack model for cryptanalysis where the attacker has access to both the plaintext and its ciphertext.
   2. What is the plaintext in this case?
      1. ITHASHANDSBUTCANNOTCLAPX
   3. What is the key? You can specify as either common separated numbers or letters.
      1. 1,2,3,4,5,6
   4. Given your knowledge of the key, manually encrypt the message that you just decrypted and show the step-by-step procedure you used to produce the cyphertext= TWTOHEICERSKAIAXNSCXSILX.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T | H | E | A | N | S |
| W | E | R | I | S | I |
| T | I | S | A | C | L |
| O | C | K | X | X | X |

TWTO HEIC ERSK AIAK NSCX SILX

**Question 2**

Complete Exercise 1 of Module 8: Polyalphabetic Ciphers Discussion Activity.

(**Points: 4** (2 point each for parts a and b).

1. Consider a Vigenere encryption **C = E(k, msg)**.
2. Assuming you are given a ciphertext and the length **p** of the key, what is an upper bound on the number of keys you must test before you are guaranteed to break the key? Assume the size of the alphabet is **n**.
   1. n \* 26
3. Consider double encryption where the two Vigenere keys are of the same length, i.e., **C = E(k1, E(k2, msg))** where **length(k1) = length(k2)**. What is an upper bound on the number of cases you must test before you are guaranteed to break the key?
   1. n \* 26 \* 26

**Question 3**

Complete Exercise 3 of Module 8: Polyalphabetic Ciphers Discussion Activity.

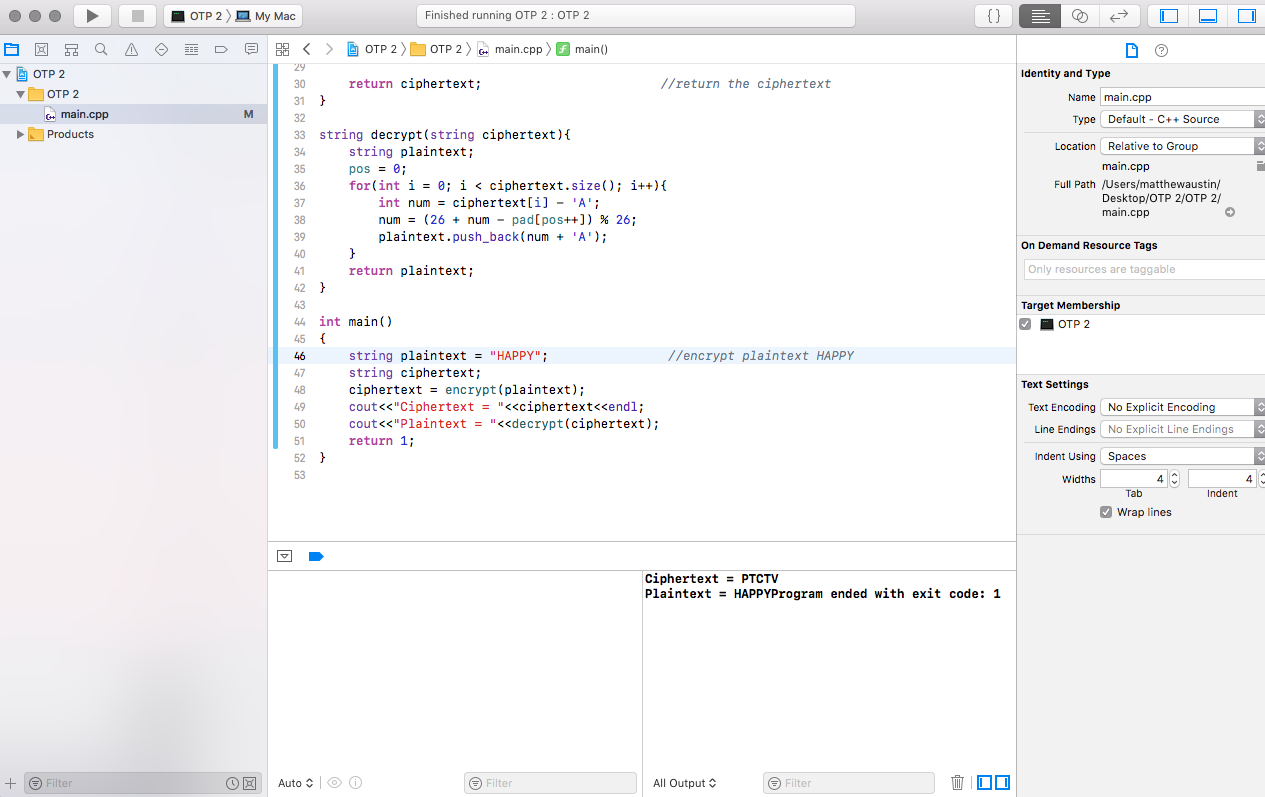
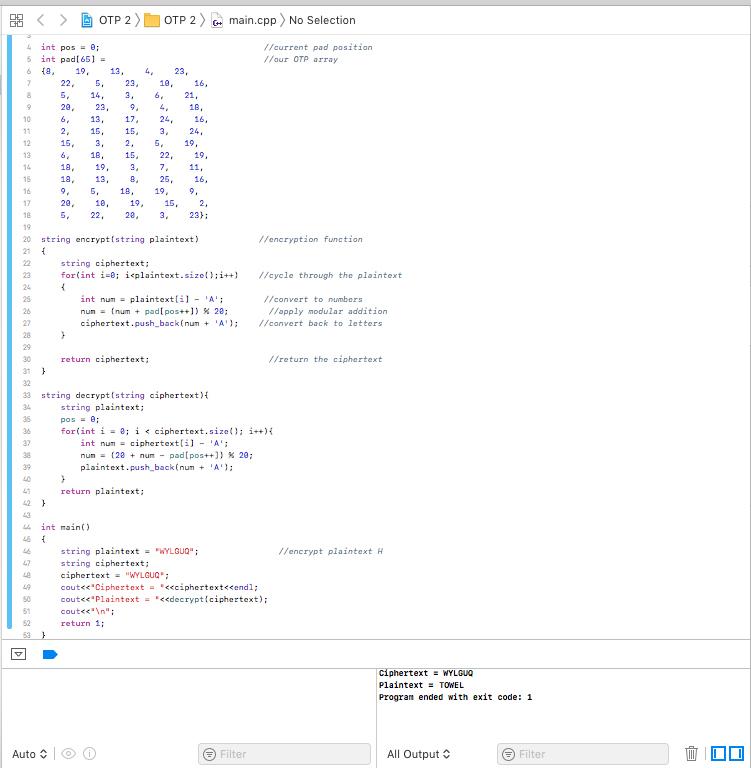
(**Points: 4** (2 point each for stating the key and the plaintext).

1. Key:
   1. DWARF
2. Plaintext:
   1. IWASATALOSSWHATTODOFORIDURSTNOTRETURNTOTHESAMELANDINGPLACEBUTSTOODTOTHENORTHANDWASFORCEDTOPADDLEFORTHEWINDTHOUGHVERYGENTLEWASAGAINSTMEBLOWINGNORTHWESTASIWASLOOKINGABOUTFORASECURELANDINGPLACEISAWASAILTOTHENORTHNORTHEASTWHICHAPPEARINGEVERYMINUTEMOREVIS

**Question 4**

Complete Exercise 2 of Module 9: One Time Pad Discussion Activity. You must provide a screenshot of the code and console window as evidence that you programmatically arrived at the right solution.

(**Points: 4** (2 points for screenshot of code and console displaying the answer to the riddle). TOWEL

1. 
2. 

**Question 5**

Complete Exercise 3 of Module 9: One Time Pad Discussion Activity.

(**Points: 2** (2 points for providing an answer to the riddle).

Using the book cipher key 126-3-4 for the Vernam/OTP algorithm solve the following riddle. *What invention lets you look right through a wall?* The encrypted answer is **#2/!6\*.**

WINDOW

**Question 6**

Attempt steps 1 through 8 of Module 10: Electromechanical Cipher Machines Discussion activity. There has been a discussion board created for this part of the homework. Post your answer to parts a and b on the discussion board.

**Points: 2** (1 point for correctly encrypting a message and posting the relevant information on the discussion board.  1 points for correctly decoding a classmate's encrypted message.)

MY CIPHERTEXT:

**Model:** Default (Wehrmacht – UKW = B)

**Rotors:** I, IV and III.

**Plugboard:** WR HM

OCTVP VMIAG CVQIQ APSIA SQEDX ZOWC

PLAINTEXT: IF YOU ARE READING THIS ITS TOO LATE

Sean Ulrich:

Rotors: V, III, II (default model)

Plugboard: JA RK

Ciphertext: MSBKQ ZKNVZ PABVV MTRCN UZOFX LIQAE XJDCM G

Plaintext: I AM THE FIRST NO HARD FEELINGS BUT GET REKTED