CSCI 2070 – Introduction to Ethics/ Cyber Security

Spring 2017

HW2

Due Date 03/28/2017

Instruction: This is an individual assignment, sharing your answers with other students is not allowed. Write your answers on a separate sheet and make sure you include your name on each of the sheet that you will be submitting. Submit your answers through D2L.

1. Given that the Caesar’s cipher was used, find the plaintext that corresponds to the following ciphertext:
   VSRQJHEREVTXDUHSDQWV

(20 points)

2. Find the plaintext and the key, given the ciphertext
   CSYEVIIXIVQMREXIH

   Hint: The Key is a shift of the alphabet

(20 points)

3. The weak ciphers used during the election of 1879 employed a fixed permutation of the words for a given length sentence. To see that this is weak, find the permutation of (1, 2, 3, 4, …., 10) that was used to produce the scrambled sentences below, where “San Francisco” is treated as a single word. Note that the same permutation was used for all three sentences.

   FIRST TRY TRY IF YOU AND DON’T AGAIN AT SUCCEED
   ONLY YOU YOU YOU AS BELIEVE OLDAREAREAS
   WINTER WAS IN THE I SUMMER EVER SAN FRANCISCO COLDEST SPENT

(20 points)

4. Encrypt the message
   We are all together
   using a double transposition cipher (of the type I described in the class) with 4 rows and 4 columns, using the row permutation

   (1, 2, 3, 4) → (2, 4, 1, 3)

   And the column permutation

   (1, 2, 3, 4) → (3, 1, 2, 4)

(20 points)

5. Decrypt the ciphertext
   IAUTMOCSMNIMREBOTNELSTRHEREOAEVMWIHTSEEATMAEOHWHSYCEELTTEOHMUOUFEHTRFT

   This message was encrypted with a double transposition using a matrix of 7 rows and 10 columns.
   Hint: the first word is “there”

(30 points)