Assignment – 2 Date: August 08, 2018

Submission Deadline: August 22, 2018

No assignment will be evaluated after the deadline.

1. a. Implement Vigenere Cipher.

   b. Use Kasiski Analysis to guess the block size (*m*) used in generating the following code using Vigenere Cipher:
   "VHVSSPQUCEMRVBVBBBVHVSURQGIBDUGRNICJQUCERVUAXSSR"
   HINT: Create a list of all the sets of repeating 4-letters and 3-letters. For each of these, find the distance between the two repeating units, and then consider all the factors of this distance, as probable values of m.

2. a. Implement the Auto-key Cipher.

   b. Perform a brute force attack to break the following code encrypted using Auto-key cipher:
   "YRRQKYTMTCMCLHBWONB"
   Show all sequences generated till you get the actual plaintext, along with corresponding keys.

3. a. Implement a Keyed Transposition Cipher, also called Permutation Cipher, where you will specify the transposition key yourself.

   b. Hence use the following key to transpose your plaintext characters:

X	1	2	3	4	5	6	7	8
Π(x)	4	1	6	2	7	3	8	5

   where π represents the permutation of plain text letters positioned {1, …, 8}

   c. Test the operation of your encryption and decryption programs using the above π and its corresponding π^{-1}.
   Hence decrypt the following cipher text, which was encrypted using the above π:
   "TGEEMNELNNTDROEOAAHDOETCSHAEIRLM"

4. a. Modify the Hill Cipher program you wrote in Assignment 1, so as to implement the Permutation Cipher of Q. 3b., that is:

x	1	2	3	4	5	6	7	8
Π(x)	4	1	6	2	7	3	8	5

   HINT: The key of a transposition cipher may be represented as a matrix of zeros and ones.

****