Assignment – 2 Date: August 19, 2016

Submission Deadline: September 2, 2016

No assignment will be evaluated after the deadline.

1. Implement the Auto-key Cipher.
2. Implement the following classic polyalphabetic ciphers (Generate the keys pseudo-randomly, check validity of the key, and store it into a key-file):
    a. Vigenere Cipher
    b. Hill Cipher
    c. Keyed Transposition Cipher (Assume the block size to be 5.)

3. Modify the Hill Cipher program you wrote for above Q. 2b, so as to implement the following *Permutation Cipher*: (Following π is a permutation of plain text letters positioned at {1, …, 8})

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

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

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