CSCI 4174/CSCI 6708 NETWORK SECURITY
ASSIGNMENT NO.3

Date given: March 9, 2017
Due: Friday, March 20, 2017, 11.55 p.m.

NOTE: For programming questions, you may use Java, Python. C or C++. Please do not use any other programming languages. Furthermore, submit source code as well as sample runs of the output. Failure to do so will result in loss of points.

1. Write a program to encrypt and decrypt strings of characters using the following ciphers:
a) Caesar cipher
b) Vigenere cipher
c) Matrix transposition cipher

Your program should contain functions/methods to encrypt a given plaintext string of characters and a key and generate the corresponding ciphertext. It should also contain functions/methods to decrypt a ciphertext string of characters and generate the corresponding plaintext. Submit the source codes and sample runs of the program.

2. We discussed DES in detail in the lectures. An important standard that has superseded DES in recent years is the Advanced Encryption Standard (AES), which is based on the Rijndael algorithm. Find out information on AES and write a 2-page summary (12 point font, single line spacing, diagrams can be included) on AES – overview, key generation, encryption process, etc.

3. In each of the following, the two prime numbers p and q, and the message M to be encrypted using RSA are given. For each case, determine the private and public keys and the encrypted message.

a) p = 7, q = 11, M = 6
b) p = 11, q = 13, M = 9
c) p = 17, q = 31, M = 5

4. Write a program that will take a message m (an integer) and key (e,n) – two integers, and generate the ciphertext c (another integer), using the RSA algorithm. Use the examples in question 1 above to test your program.

Note: Use the mod equation discussed in class to derive the ciphertext.