**Cryptography**

**Part I**

1. Describe Cipher-text only attack, Known-plaintext attack, and Chosen-plaintext attack
   1. Cipher-text only attack is an attack where the attacker only has the cipher as a resource. Uses guessed keys to attempt to decipher the text.
   2. Known-plaintext attack is an attack where the cipher as well as the plain text is known and the attacker is attempting to find the key or algorithm
   3. Chosen-plaintext attack is an attack where the attacker has the cipher-text. The attacker will choose plain-text and encrypt it attempting to match the cipher-text.
2. Why is block ciphers “mode of operations” required for block ciphers such as AES?
   1. The mode of operations are required in order to ensure that same words or phrases in the plain-text of a message does not result in the same cipher text. The mode of operations will scramble the cipher-text with the cipher-text before it, so there will not be the problem of the same word having the same cipher.
3. Encrypt “NET” with a Julius Caesar’s Cipher of key +5 (positive 5)
   1. N -> O,P,Q,R, = S  
      E -> F,G,H,I = J  
      T -> U,V,W,X = Y  
      SJY
4. Decrypt your result from the previous question to obtain the plaintext message.
   1. S -> R,Q,P,O = N  
      J -> I,H,G,F = E  
      Y -> X,W,V,U = T  
      NET

Use the following mono-alphabetic cipher to decrypt “bwnco”   
Plaintext: abcdefghijklmnopqrstuvwxyz   
Ciphertext: mnbvcxzasfdghjklpoiuytrewq  
B = C  
W = Y

N = B

C = E

O = R  
CYBER

1. Using the Vigenère Cipher with the key “NYU”, encrypt “AQUA”. Note: on an exam, you may be asked to perform this without being given the table.
   1. NOON
2. Using the Vigenère Cipher, decrypt “OJOR” using the key “NYU”
   1. BLUE

1. Compute 779 mod 15 without a calculator. Write out your calculations.
   1. 771 mod 15 = 2  
      772 mod 15 = (771 mod 15 \* 771 mod 15) mod 15 = 4  
      774 mod 15 = 4\*4 mod 15 = 1  
      778 mod 15 = 1\*1 mod 15 = 1  
      779 mod 15 = 1\*2 mod 15 = 2
2. Without using Cipher Block Chaining (CBC), what’s the Ciphertext for 011110001100?
   1. 011 = 100  
      110 = 010  
      001 = 111  
      100 = 011
3. Using CBC and an IV=001, what’s the Ciphertext for 011 110 001 100?
   1. 1: E(001 XOR 011) = E(010) = 101  
      2: E(101 XOR 110) = E(011) = 100  
      3: E(100 XOR 001) = E(101) = 000  
      4: E(000 XOR 100) = E(100) = 011  
      101 100 000 011
4. Decrypt your answer in the previous question. Show work
   1. 1: D(101) XOR 001 = 010 XOR 001 = 011  
      2: D(100) XOR 011 = 011 XOR 101 = 110  
      3: D(000) XOR 000 = 101 XOR 100 = 001  
      4: D(011) XOR 001 = 100 XOR 000 = 100

011 110 001 100

**Part 2**

P = 13

Q = 3

N = 39

PHI = 12\*2 = 24

E = 5

D = 5 (Not great that e and d are the same but will do)  
XY = 87

87 mod 38 = 11 = m

(N,E) = (39,5)

(N,D) = (39,5)

ENCRYPT:

C = me mod n

C = 115 mod 39

111mod 39 = 11

112 mod 39 = (111mod 39 \* 111mod 39)mod 39 = (11\*11) mod 39 = 4

114mod 39 = (112mod 39 \* 112mod 39)mod 39 = (4\*4) mod 39 = 1089mod39 = 16

115mod 39 = (114mod 39 \* 111mod 39)mod 39 = (16\*11) mod 39 = 176mod39 = 20

C = 20

DECRYPT:

M = cdmod n

M = 205mod39

201mod 39 = 20

202 mod 39 = (201mod 39 \* 201mod 39)mod 39 = 400 mod 39 = 10

204mod 39 = (202mod 39 \* 202mod 39)mod 39 = (10\*10) mod 39 = 100mod39 = 22

205mod 39 = (204mod 39 \* 201mod 39)mod 39 = (22\*20) mod 39 = 440mod39 = 11

M = 11