Assignment Two (CS 435/890BN, Spring/Summer 2019)

(Weight: 3%, Due: July 30, 5:30pm)

1. (10 points) Finish the following table:

Mode	Encrypt	Decrypt
ECB	$C_j = E(K, P_j)$ $j = 1, \ldots, N$	$P_j = D(K, C_j)$ $j = 1, \ldots, N$
CBC	$C_1 = E(K, [P_1 \oplus IV])$ $C_j = E(K, [P_j \oplus C_{j-1}])$ $j = 2, \ldots, N$	
CFB		
OFB		
CTR		

2. (15 points)

Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key k. To encrypt a message m, consisting of a string of bits, the following procedure is used.

1. Choose a random 80-bit value v
2. Generate the ciphertext $c = \text{RC4}(v \| \text{k}) \oplus m$
3. Send the bit string $(v \| c)$

a. Suppose Alice uses this procedure to send a message m to Bob. Describe how Bob can recover the message m from $(v \| c)$ using k.
b. If an adversary observes several values $(v_1 \| c_1), (v_2 \| c_2), \ldots$ transmitted between Alice and Bob, how can he/she determine when the same key stream has been used to encrypt two messages?
c. Approximately how many messages can Alice expect to send before the same key stream will be used twice? Use the result from the birthday paradox described
d. What does this imply about the lifetime of the key k (i.e., the number of messages that can be encrypted using k)?

3. (10 points)

Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

a. XOR of subkey material with the input to the f function
b. XOR of the f function output with the left half of the block
c. f function
d. permutation P
e. swapping of halves of the block

4. (10 points)
   In AES, show the first eight words of the key expansion for a 128-bit key of all zeros.

5. (20 points)

Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101}:

a. Show the original contents of **State**, displayed as a 4×4 matrix.
b. Show the value of **State** after initial AddRoundKey.
c. Show the value of **State** after SubBytes.
d. Show the value of **State** after ShiftRows.
e. Show the value of **State** after MixColumns.

6. (15 points) Perform encryption and decryption using the RSA algorithm, for the following:

   a. $p = 3; q = 11, e = 7; M = 5$
   b. $p = 5; q = 11, e = 3; M = 9$
   c. $p = 7; q = 11, e = 17; M = 8$

   d. $p = 11; q = 13, e = 11; M = 7$
   e. $p = 17; q = 31, e = 7; M = 2$

   Hint: Decryption is not as hard as you think; use some finesse.

7. (10 points) In the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe?

8. (10 points) In using the RSA algorithm, if a small number of repeated encodings give back the plaintext, what is the likely cause?