**CIS 3362 Homework #5a**

**Due: 11/3/2014 at the beginning of class**

1) Let the round 7 key for AES be the following in hexadecimal:

 8910 4DFA A275 BBCD F011 184E 976D 5DB3

Determine the first 4 bytes of the round 8 key. Please give your answer in hexadecimal.

2) Let the round 4 key for AES be the following in hexadecimal:

 1234 5678 9ABC DEFF EDCB A987 89AB CDEF

Determine the first 4 bytes of the round 5 key. Please give your answer in hexadecimal.

3) What is the remainder when 1214753  is divided by 399?

4) What is the remainder when 22221387 is divided by 871?

5) What is the remainder when 15417822 is divided by 589?

6) Consider an RSA system where n = 221 and e = 125. What are p, q, φ(n) and d?

7) Consider an RSA system where n = 437 and e = 137. What are p, q, φ(n) and d?