# CSci 4554 Assignment 8

### Due Friday, April 4 in class

**Problem 1 (8 points).** Supposed a block cipher is used to encrypt two different messages that happen to have the same block in the same position in the middle but differ in the beginning. Consider the four modes of block cipher operations (CBC, CFB, OFB, and CTR). If the two messages are encrypted with the same key and the same IV (nonce for CTR), would the two identical blocks result in the same ciphertext? Please show your computations for each mode.

**Problem 2 (5 points).** Consider a Diffie-Hellman key exchange protocol with two different prime values of $p$, both on the order of 200 bits:

- with the largest prime factor of $p - 1$ on the order of $2^{160}$
- with the largest prime factor of $p - 1$ on the order of $2^{40}$

Compare the number of tries needed to solve the discrete logarithm problem in these two cases.

**Problem 3 (6 points).** Suppose we chose $p = 11$, $q = 23$, and $e = 3$ for an RSA module. Compute $d$, encrypt $m = 20$ and decrypt the result to check the answer. Show all your computations.

**Problem 4 (6 points).** Suppose you need to encrypt $m = 80$ using the same RSA module as in problem 3. Show how you can use the result from the previous problem to simplify the computation.