EECE 412, Fall 2014

Quiz #2

Your 412 alias: ________________________

Your Family name: ________________________

Your Given name: ________________________

Your student ID: ________________________

Name of your left neighbor: _________________

Name of your right neighbor: _________________

#	Points	Out of
1		2
2		2
3		2
4		4
5		10
6		8
TOTAL		28

____

1. **(2 points) State the Kerckhoff's principle (in your own words)?**

2. (2 points) Explain why Kerckhoff's is paramount to security of the crypto-systems? Provide some examples.

3. (2 points) Why is it important to reconsider design assumption every so often? Provide an example.

4. (4 points) Draw random oracle models for block and stream ciphers below. Describe how these ciphers work according to the models.

5) (10 points) Consider the following example: Alice encrypts a plaintext P with AES in CBC mode to using key K get a ciphertext C. Lets also limit size of P to exactly 3 blocks and, hence, C to 3 blocks too. Thus, E(P, K) = E({P_0, P_1, P_2}, K) = {IV, C} = {IV, C_0, C_1, C_2}, where C_i = E(P_i XOR C_{i-1}, K). Then Alice sends C to Bob and Bob uses the same key K to decrypt the message.

5.1) (5 points) Demonstrate how Trudy can use this knowledge to change the C so that corresponding P changes as well.

5.2) (5 points) Propose and explain changes to the mode of operation of encryption that will mitigate the vulnerabilities:

6) (8 points). For each mode of operation (OFB, CTR, CBC and ECB) state it's pros and cons. For each of the modes, also, provide an example where would you use it.