# EECE 412, Fall 2012

## Quiz #2

Your Family name: _____

Your Given name: _____

Your student ID: _____

Name of your left neighbor: _____

Name of your right neighbor: _____

| # | Points | Out of |
|---|---|---|
| 1 | | 4 |
| 2 | | 3 |
| 3 | | 6 |
| 4 | | 6 |
| 5 | | 3 |
| TOTAL | | 22 |

_____

**1. (4 points) Suppose that Alice uses a stream cipher to encrypt plaintext P, obtaining ciphertext C, and Alice sends C to Bob. Suppose that Trudy happens to know the plaintext P, but does not know the key K that was used in the stream cipher.**

**a) Show that Trudy can easily determine the keystream that was used to encrypt P.**

**b) Show that Trudy can, in effect, replace P with plaintext of her choosing, say P'. That is, show that Trudy can create a ciphertext message C' so that when Bob decrypts C', he will obtain P'.**

**2. (3 points) Random Oracle Model.**
**Explain what the Elf needs to do with the dice and the script in order to implement a block cipher.**

**3. (6 points) Confusion and diffusion.**

**a) (2 points) Define confusion and diffusion in the context of cryptography.**

**b) (4 points) AES consists of four functions: ByteSub, ShiftRow, MixColumn, AddRoundKey. Which of these functions are primarily for confusion and which are primarily for diffusion? Justify your answer.**

**4. (6 points) Suppose that Alice and Bob use CBC mode encryption. What security problems arise if they always use a fixed initialization vector (IV), as opposed to choosing IVs at random? Explain.**

**5. (3 points) Public key cryptography is based on trap door function. Explain its properties and give an example.**