EECE 412, Fall 2012

Quiz #2 Key

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.
K=C ^ 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'.

Once K is known (obtained as shown in part a), C'=K^P'=C^P^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.

Input:

- Fixed size short string of plaintext M
- Key K

Output: Fixed size short string of ciphertext C

For each value of K, the Elf keeps a separate part of his script, in which he rolls dice for each value of M in order to generate C. If the elf has already seen the pair of M and K, then he just looks up the corresponding C from his script.

3. (6 points) Confusion and diffusion

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

confusion -- obscuring the relationship between the plaintext and ciphertext

diffusion -- spreading the plaintext statistics through the ciphertext.

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.

ByteSub and AddRoundKey are primarily for confusion, as each byte is substituted with another byte obtained through a table lookup or XOR (with the key material) operation.

ShiftRow is for diffusion only, as it does nothing but shifting each row by a variable number of bytes (from 0 to 3).

MixColumn can be considered as doing diffusion and confusion. So, any of the two answers (or both) would be considered as correct for MixColumn.

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.

If IV is fixed than the following issues arise:

1) The same plain text will always result in the same cipher text.
2) Given that many modern protocols have structured headers, which could be known to the attacker, by obtaining many first blocks of the cipher can put the key into depth, i.e., make it easier for an attacker to obtain the key.

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

- Easy to compute in one direction
- Hard to compute in other direction
- "Trap door" used to create keys

Example: Given large numbers p and q, product $N=pq$ is easy to compute, but given N, it is hard to find p and q.