EECE 412, Fall 2010

Quiz #2 Key

Your Family name: _____

Your Given name: _____

Your student ID: _____

#	Points	Out of
1		2
2		8
3		6
4		6
TOTAL		22

Name of your left neighbor: _____

Name of your right neighbor: _____

Questions:

1. (2 points) The basic assumption in cryptography (a.k.a. Kerckhoff's Principle) states which of the following? (select one most appropriate)

[x] The system design should be assumed publicly known but the key(s) can be assumed secret.

[ ] Security should be achieved through secrecy.

[ ] The key(s) should be assumed publicly known but the system design can be assumed secret.

[ ] Both system design and the keys can be assumed secret.

[ ] Neither system design or the keys can be assumed secret.

2. (8 points) Explain what the Elf needs to do with the dice and the script in order to implement a stream cipher.

Input:

- **short string (key)**
- **length of the output**

Output: long random stream of bits (keystream)

The Elf keeps a listing of key to keystream mapping on his scroll. If a request comes in with a specific key, the Elf checks his scroll for the mapping of the key to keystream bits, and returns it if found. If the key is not listed yet, the Elf will need to roll the dice and generate the requested length of output keystream. The keystream bits can then be used to XOR with the plaintext to generate the cipher text.

3. (6 points) Explain the difference between backward and forward secrecy and give at least two examples of key refreshing techniques that have either one or both of these properties.

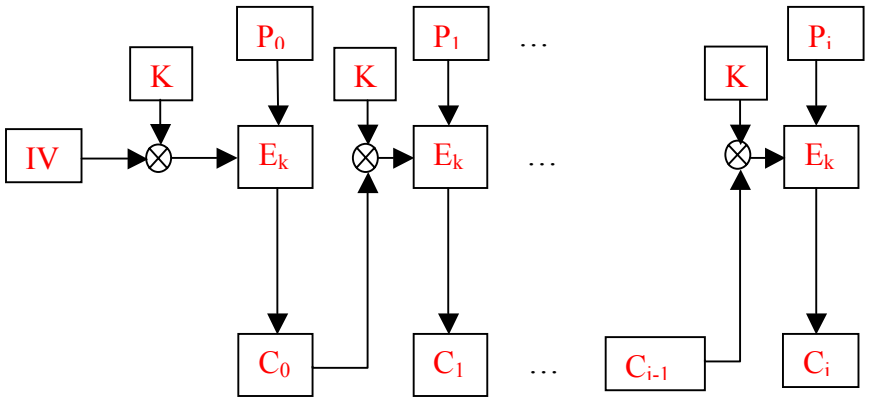
Backward secrecy means that a compromise should not compromise any earlier key. While forward secrecy implies that a compromise of the current key should not compromise any future key.

Example: Backward secrecy
key updating, Ki = H(Ki-1)

Example: Forward secrecy
Autokeying , Ki+1 = H(Ki,Mi1, Mi2, …)

4. (6 points) Suppose that we use a mode of operation defined by the following rule: $C_0 = E_K(P_0, IV \oplus K)$, $C_i = E(P_i, C_{i-1} \oplus K)$, …, where P_i is i-th chunk of the plaintext.

(2 point) Draw this mode's diagram, similar to the ones Kosta used for illustrating modes of operation in class.



(2 points) What is the corresponding decryption rule?

$P_i = E(C_i, C_{i-1} \oplus K)$, $P_0 = E(C_0, IV \oplus K)$,

(4 points) Explain security disadvantages of this mode, compared to CBC mode.

In this mode, the plain text is not diffused with previous cipher text, but instead, the key is diffused with previous cipher text. Compare to CBC mode, this mode reduces the diffusion property as the cipher text may not significantly change with a change in the plain text. The diffusion property of the cipher text only comes from the algorithm of the block cipher.