EECE 412, Fall 2009

Quiz #1

Your Family name: _____
Your Given name: _____
Your student ID: _____

Name of your nearest left neighbor: _____
Name of your nearest right neighbor: _____

Questions:

1. (7 points) Based on the video fragment from ABC World News episode of May 25, 2009, shown at the beginning of the quiz, analyze (1) the value of the assets at risk, (2) threats to these assets, and (3) threat agents, for the Facebook users due to Nigerian 419, application attack, Koobface Virus. If necessary make reasonable assumptions and state them clearly. Classify which of the CIA properties of the valuable assets were reduced as a result of the incident.

Attacks	Assets	Threats	Threat Agents	CIA
Nigerian 419	Money ($500)	-A social engineering attack (deception) where you will unintentionally transfer your money	-Organized criminals	Availability
application attack	Personal profile information	-Disclosure and misuse of your profile info	-Marketing agents -spammers	Confidentiality
Koobface Virus	Data on personal computer	-Disclosure, disrupt, misuse of your data on the computer -Turn your PC into part of Bot-net -Make your PC unworkable	- Bot-net hackers - Organized criminals - Malicious hackers	-Confidentiality -Integrity -Availability

2. (4 points) Consider the risks due to attacks explained in the video for the previous problem. For each of the four ways of managing this risk, give one example of what Facebook users can do. Be specific.

1. Accept: accept the risk by installing any Facebook application.

2. Avoid: do not use any Facebook application or launch any downloaded program.

3. Transfer: have a friend to try a Facebook application or downloaded program first.

4. Reduce: use anti-virus to scan downloaded executables before launching them.

3. (2 points) The basic assumption in cryptography (a.k.a. **Kerckhoff's Principle**) states which of the following? (select one most appropriate)

[ ] Security should be achieved through secrecy.

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

[ ] 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.

4. (8 points) Explain what the Elf needs to do with the dice and the script in order to implement a block cipher.

Input: fixed length string, key
Output: fixed length string

To encrypt:

A user provides a plaintext m and a key k. Elf looks up m and k on his scroll. If the corresponding ciphertext c exists, Elf returns c. If not exists, Elf rolls the dice to generate the ciphertext c, records the tuple (m, k, c) on the scroll, and returns c.

To decrypt:

A user provides a ciphertext c and a key k. Elf looks up c and k on his scroll, and returns the corresponding plaintext m.

5. (6 points) Explain the difference between weak and strong collision resistance properties of hash functions.

weak collision resistance :

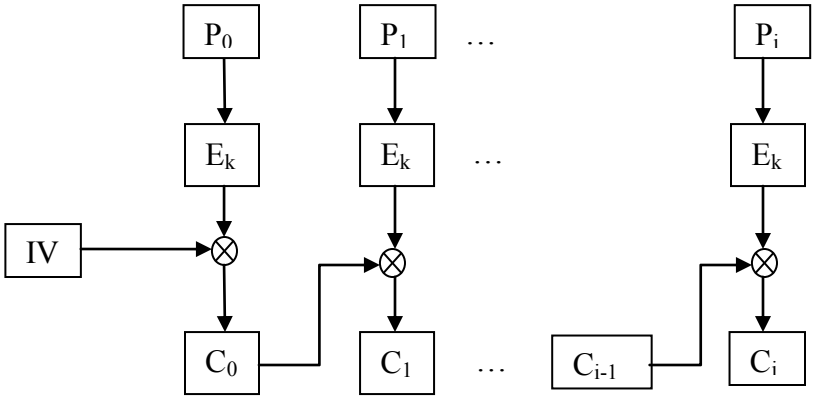
Given a x, it is difficult for an attacker to find a y, s.t. $y \neq x$ and h(y) = h(x).

strong collision resistance :

It is difficult for an attacker to find any x and y, s.t. $y \neq x$ and h(y) = h(x).

6. (8 points) Suppose that we use a mode of operation defined by the following rule: $C_0 = IV \oplus E(P_0, K)$, $C_i = C_{i-1} \oplus E(P_i, K)$

(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?

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

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

This method does not have the property of diffusion as it encrypts on plaintext only. Because an IV is publically known, it is essentially an EBC mode. Thus, it has the same disadvantages as the EBC mode has, such as:

- Same message has same ciphertext
- Redundant/repetitive patterns will show through
- Subject to "cut-and-splice" attacks