**CSCI 531 Quiz 3**

**Write your name here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**The number of points for each question or sub-question is indicated by the integer in brackets [n] before the question or sub-question. The total number of points is 100.**

1. [10 points] To encrypt a series of plaintext blocks p1, p2, …, pn using a block cipher E operating in electronic code book (ECB) mode, each ciphertext block c1, c2, …, cn is computed as ci = Ek(pi). Which of the following is **NOT** a property of this block cipher mode? Briefly explain your choice.
2. Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.
3. Decryption can be fully parallelized.
4. If a ciphertext block is modified or corrupted, then after decryption the corresponding plaintext block and all the following plaintext blocks will be affected.
5. None of the above; that is, (a), (b), and (c) are all properties of the ECB block cipher mode.

Correct answer \_\_

Explanation:

The correct answer is 3. In ECB, altering a ciphertext block only affects a single plaintext block.

2. [10 points] What is a one-way function? Explain in general terms (plain English)

A one-way function is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible.

3. [10 points] What is the difference between MAC and Hash function?

In Message Authentication Code, the secret key shared by sender and receiver. The MAC is appended to the message at the source at a time which the message is assumed or known to be correct.

Hash Function: The hash value is appended to the message at the source at time when the message is assumed or known to be correct. The hash function itself not considered to be secret.

4. [20 points] It is possible to use a hash function to construct a block cipher with a structure similar to DES. Recall that a hash function is one way and a block cipher must be reversible (to decrypt). If your answer is positive, briefly explain how this can be done.

5 points if “yes”, 15 points for explanation

It is possible to build a block cipher out of a great many things. If you want to use a hash function, the classic trick is to follow a Feistel structure, which is, the same kind of structure that used in DES.

One would use the hash function for the "F" part, which combines one (sub)key and one half of the current block, to produce a value which is to be XORed with the other half of the current block. The beauty of the scheme is that the "F" function is always invoked in the same direction, both for encryption and for decryption. Therefore, it can be a one-way function, like a hash function.

5. [15 points] Suppose a MAC system (S,V) is used to protect files in a file system by appending a MAC tag to each file. The MAC signing algorithm S is applied to the file contents and nothing else. What tampering attacks are not prevented by this system?

1. Changing the last modification time of a file.
2. Replacing the contents of a file with the concatenation of two files on the file system.
3. Changing the first byte of the file contents.
4. Replacing the tag and contents of one file with the tag and contents of a file from another computer protected by the same MAC system, but a different key.

Option numbers: 1

Brief explanation:

The MAC signing algorithm is only applied to the file contents and does not protect the file meta data.

6. [10 points] What is a birthday attack?

A birthday attack is a name used to refer to class of brute-force attacks. It gets its name from the surprising result that the probability that two or more people in a group of 23 share the same birthday as greater than ½ ; such a result is called a birthday paradox.

7. [10 points] Why padding messages with 0s results in insecure MAC?

Given tag on message m attacker obtains tag on m ll 0

pad(m) = pad(m ll 0)

8. [15 points] Let H:M→T be a collision resistant hash function. Which of the following is collision resistant: (as usual, we use ∥ to denote string concatenation)

1. H′(m)=H(m)[0,…,31] (i.e. output the first 32 bits of the hash)
2. H′(m)=H(m)⊕H(m)
3. H′(m)=H(H(m))
4. H′(m)=H(m)∥H(m)
5. H′(m)=H(H(H(m)))
6. H′(m)=H(0)

Options(s): 3, 4, 5

A collision finder for H′ gives a collision finder for H

1. is not collision resistant because an attacker can find a collision in time 216 using the birthday paradox.

2. H(m)⊕H(m) is not collision resistant because H(0) = H(1)