**Description for: CS 492 Homework 4**

Cryptographic hashes

**You may work in groups of 2**

Complete the problems below and submit this word document with the solution to the questions here.

Name: Matthew Krieger

**Problem 1** (book 5.1):

A cryptographic hash function must satisfy:

* Compression
* Efficiency
* One-way
* Weak collision resistance
* Strong collision resistance

1. [14 pts] Suppose that a hash function fails to provide compression, but provides all of the other required properties. Give an application where a cryptographic hash function should be used, but where this hash function would fail to be useful

Password hashing. Analytical and brute force attacks are a lot easier if you hash 512 bits to 512 bits.

1. [14 pts] Repeat part a, but assume all properties hold except for efficiency

Just like with the one-time pad, sometimes it’s too strenuous for continuous hashing.Businesses that have servers to hash important numbers need efficiency or else theirservers will burn out or cause lag for their customers. A sort of availability issue forresources too. Source: the book and me.

1. [14 pts] Repeat part a, but assume all properties hold except for one-way

Well, if you want to keep anything secret, you’re going to need one way, passwords,important numbers, etc. without one-way means that it is invertible. Meaning, I get thehash, invert it, get your information, which the company or holder do not want. Source:the book and me

1. [14 pts] Repeat for part a, but assume that all properties hold except the collision resistance properties

Weak and strong collision resistances are tied to integrity and confidentiality. Weakcollision makes sure you know if the message is modified and strong collision makes itso that it should not be possible to break the message easily through a collision. Source:the book and me.

**Problem 2** (book 5.8):

Consider a CRC that uses the divisor 10011.

1. [14 pts] Find the CRC for the message 10101011 (you **must** show your work)

1 0 1 0 1 0 1 1 0 0 0 0

1 0 0 1 1

0 0 1 1 0 0 1 1 0 0 0 0

1 0 0 1 1

0 0 0 1 0 1 0 1 0 0 0 0

1 0 0 1 1

0 0 0 0 0 1 1 0 0 0 0 0

1 0 0 1 1

0 0 0 0 0 0 1 0 1 1 0 0

1 0 0 1 1 0

0 0 0 0 0 0 0 0 1 0 1 0

CRC Checksum: **1010**

1. [14 pts] Find two collisions with 10101011. That is find two other data values that produce the same CRC checksum as the data 10101011.

Divisor: 1 0 0 1 1

Dividend: 1 0 1 0 1 0 1 1

(xor): 1 0 0 1 1

New Dividend: 1 1 1 0 0 1 1 1

1 1 1 0 0 1 1 1 0 0 0 0

1 1 1 1 0 1 1

10011) 111001110000

10011

\_\_\_\_\_\_\_

11111

10011

\_\_\_\_\_\_\_\_\_

11001

10011

\_\_\_\_\_\_\_

10101

10011

\_\_\_\_\_\_\_

11000

10011

\_\_\_\_\_\_\_

**1010**

CRC Checksum: **1010**

The two checksum’s are the same hence this **IS** a collision.

**Problem 3** (book 5.10)

[6pts] Enter the number of bits on each line the outer diagram of the Tiger hash function (Figure 5.2 in the book) (ex. The lines between a,b,c to F5 are each x bits, the lines from W to key schedule are y bits, …)

The lines between a,b,c to F5 are each 64 bits

the lines from W to key schedule are 512 bits

**Problem 4** (based on book 5.34)

1. [5pts] Suppose we have a “2 out of 2” secret sharing scheme, where Alice and Bob share a secret S. If Trudy obtains Alice’s secret key what information can Trudy discover about S and why?

Trudy would NOT be able to discover any information about S without the cooperation of Bob. A “2 out of 2” scheme hypothetically creates a line, which would make it possible to calculate the y-intercept or S. Just knowing 1 point is useless when it comes to the construction of a line.

1. [5pts] Suppose we want an “m out of n” secret sharing scheme. Mathematically what would you need to do to create the secret scheme and how would you generate the n keys?

I don’t really understand this question but I have researched the “m out of n” sharing scheme and maybe this will help.

From what I understand, one of the greatest motives behind secret sharing schemes is secure key management. For example, a secret key may be used to provide access to many important files. If the key were lost (ie. Person who knew the key dies or computer with key on it is compromised/destroyed), then the files would become inaccessible. To discourage a scenario like this, secret sharing could be used because in secret sharing you would divide the secret key into pieces and give the pieces to different people in a way where specific subsets of people could cooperate to recover the key. A facilitator(for lack of a better term)would divide the secret into n parts and each participant would get 1 part so that any m parts could be be put together to recover the secret. However, m-1 parts would be unsuccessful. The secret sharing scheme would be successful if a group of M-1 participants would have no advantage of guessing the secret over anyone else.