Joshua Rose

CMPE 166 HW5

03/04/2025

4.

a. 2^N/2
b. To find 10 different collisions you need to hash 10 times the amount of values (probably). (10 * 2^N)^½
c. For M collisions you need to hash M times the amount of values. (M * 2^N)^½

9.

a. The most obvious problem is that cutting the amount of bits the hash produces (or at least you use) in half significantly reduces the security of the hash against brute force attacks to find collisions. By using only 128 bits Trudy now only needs to calculate 2^128/2 or 2^64 hashes. This is 18 quintillion hashes so it's probably still safe against brute forcing but it is less secure than using the full 256 bits. There might also be a problem with taking only the first half of the hash based on the algorithm like if the hash is computed in blocks. I don't know if it's 'safe' for Alice to use less bits but it is absolutely less safe for her to do so.
b. The same argument from part a. applies to this problem.

14.

A MAC can be used to provide data integrity using a keyed system just like a HMAC does. However to use a MAC from chained block cipher mode the sender must also send an initialization vector IV so that the MAC can be computed. The security of both systems still just relies on the key and the encryption or hashing function to be safe but the need for the IV is extra information that must be sent.

17.

a. Digital signatures are required to make sure the information in the ledger is agreed upon. For Alice to owe Bob $10 she must sign the message saying so.
b. Transaction numbers are needed to keep every transaction unique. If Alice signs that she owes Bob $10, Bob can keep sending that transaction and it looks like Alice owes him every time. If each transaction has a unique number then this can't happen.

c. Miners are called miners because by doing the work to find hashes that validate blocks they are generating ‘new money’ similar to how gold miners generate new money when they find gold.

d. Yi is included in block i so that each block of the chain does not need to be revalidated at each step so the hash of the previous block is included in the hash of the current block. If the current block is validated then you know all previous blocks are also validated.

   h(Yi, Bi, Ri) < 2^M is required so that you can verify that 2^N-m units of work have been done (on average) to find the block.

e. Each transaction using cryptocurrency requires a digital certificate so we can make sure it's valid. However, a digital certificate does not require a users real identity so cryptocurrency is pseudo anonymous as people can see your digital identity but not your real one.

18.

a. In Trudy’s double spending attack she creates a valid transaction saying she owes Alice money, but instead of broadcasting the transaction to everyone as she should, Trudy keeps the transaction private. If Alice accepts the transaction Trudy can continue to spend her money because nobody else knows it has been spent. This attack does not work using non-digital currencies because Alice only accepts the transaction as complete once she has the money physically in hand (or its gone through a bank and has been verified). For Alice to physically have the money Trudy must have given it to her so Trudy cannot have the money to offer to anyone else.

b. Alice will only accept the transaction if it appears in at least one valid blockchain. If Trudy owns 10% of the computing power she will be the one to mine a valid block before anyone else 10% of the time and then Alice will accept the money and the attack will be successful.

c. Probability that Trudy mine N blocks in a row is the probability that trudy mines a block (p) to the power of N. So probability of success is p^N

21.

In option (i) no information is stored and generating the key is simpler, requiring only the hashing method. While the information stored in option (ii) is ciphertext it could still cause problems if Trudy gets her hands on it.

In option (ii) the only difference is storing the encrypted key which is decrypted by using the hashed password as a decryption key. In option (i) to get the key Trudy only needs to guess the hash (which should not be easy) to get the key and then compare it with ciphertext to verify it. In option (ii) Trudy must guess the hash, somehow get the valid ciphertext from Alice’s computer and decrypt the ciphertext using the guessed key from the hash. Only then can Trudy try verifying she has the correct key. This makes guessing harder since Trudy has no way of knowing if her guessed hash is what's wrong or if the ciphertext stored on Alice’s computer was wrong.

22.

An advantage of key diversification is that only one key needs to be stored compared to a key for each user on the server. A disadvantage is that the security of every key is reliant on the security of Sally’s key. If Trudy somehow gets Sally’s key then she has a way to generate everyone else’s key. Of course in the case of key storage instead of key diversification, if Trudy got access to Sally’s server then she might be able to access the keys.

24.

Differences highlighted in yellow:

Message 1:

```
d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
2f ca b5 87 12 46 7e ab 40 04 58 3e b8 fb 7f 89
55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 71 41 5a
08 51 25 e8 f7 cd c9 9f d9 1d bd f2 80 37 3c 5b
96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
35 73 9a c7 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 cc 15 5c
ed 74 cb dd 5f c5 d3 6d b1 9b 0a d8 35 cc a7 e3
```

Message 2:

```
d1 31 dd 02 c5 e6 ee c4 69 3d 9a 06 98 af f9 5c
2f ca b5 07 12 46 7e ab 40 04 58 3e b8 fb 7f 89
55 ad 34 06 09 f4 b3 02 83 e4 88 83 25 f1 41 5a
08 51 25 e8 f7 cd c9 9f d9 1d bd 72 80 37 3c 5b
96 0b 1d d1 dc 41 7b 9c e4 d8 97 f4 5a 65 55 d5
35 73 9a 47 f0 eb fd 0c 30 29 f1 66 d1 09 b1 8f
75 27 7f 79 30 d5 5c eb 22 e8 ad ba 79 4c 15 5c
ed 74 cb dd 5f c5 d3 6d b1 9b 0a 58 35 cc a7 e3
```

Using code from https://www.geeksforgeeks.org/md5-hash-python/

Message 1: a4c0d35c95a63a805915367dcfe6b751

Message 2: a4c0d35c95a63a805915367dcfe6b751

25(abd).

a.

i. rec2.ps

To Bank of America:

Tom Austin and Ying Zhang are authorized access to all of my account information and may make withdrawals or deposits.

Sincerely,
Mark Stamp

ii. auth2.pls

To Whom it May Concern:

Tom Austin and Ying Zhang have demonstrated decent programming ability. They should do OK in any programming position, provided that the work is not too complex and that the position does not require any independent thought or initiative.

However, I think they like to steal office supplies, so I would keep a close eye on them. Also, their basic hygiene is somewhat lacking so I would recommend that you have them telecommute.

Sincerely,
Mark Stamp

b. rec2.ps MD5 hash: c321325acff48137d62844e481ab01c5
auth2.ps MD5 hash: c321325acff48137d62844e481ab01c5
Since these hashes are a collision and since we normally sign messages after they have been hashed Trudy can have auth2 signed and then attach that signature to a malicious message rec2 and make it appear to be valid.

d. If you use some way to read the entire contents of the file (like notepad) ignoring the conditional statement of the from then you can see that both files have the same 2 messages in them (so they get hashed to the same value) but the conditionals that choose which of the 2 message to display in postscript are likely different so the messages ‘display’ differently to the receiver.

26.

a. Using Alice’s public key you decrypt the signature to find the hashed message. Then you calculate h(M) and you compare them, if they match the signature is valid.
b. If the signature doesn't match then the message was either tampered with or it was not signed by Alice in the first place. If you don't verify you can't guarantee integrity of the message.
c. This assumption is valid because it is the way the system is supposed to work. If you trust the CA then you correctly assume that either the CA or Alice will inform people that Alice’s private key has been compromised. Without this assumption the system does not work.
d. You know nothing about the sender of the certificate.

38.

a. Using the following commands

```
gcc -o stegoRead stegoRead.c
```

```
./stegoRead aliceStego.bmp aliceStego.pdf
```

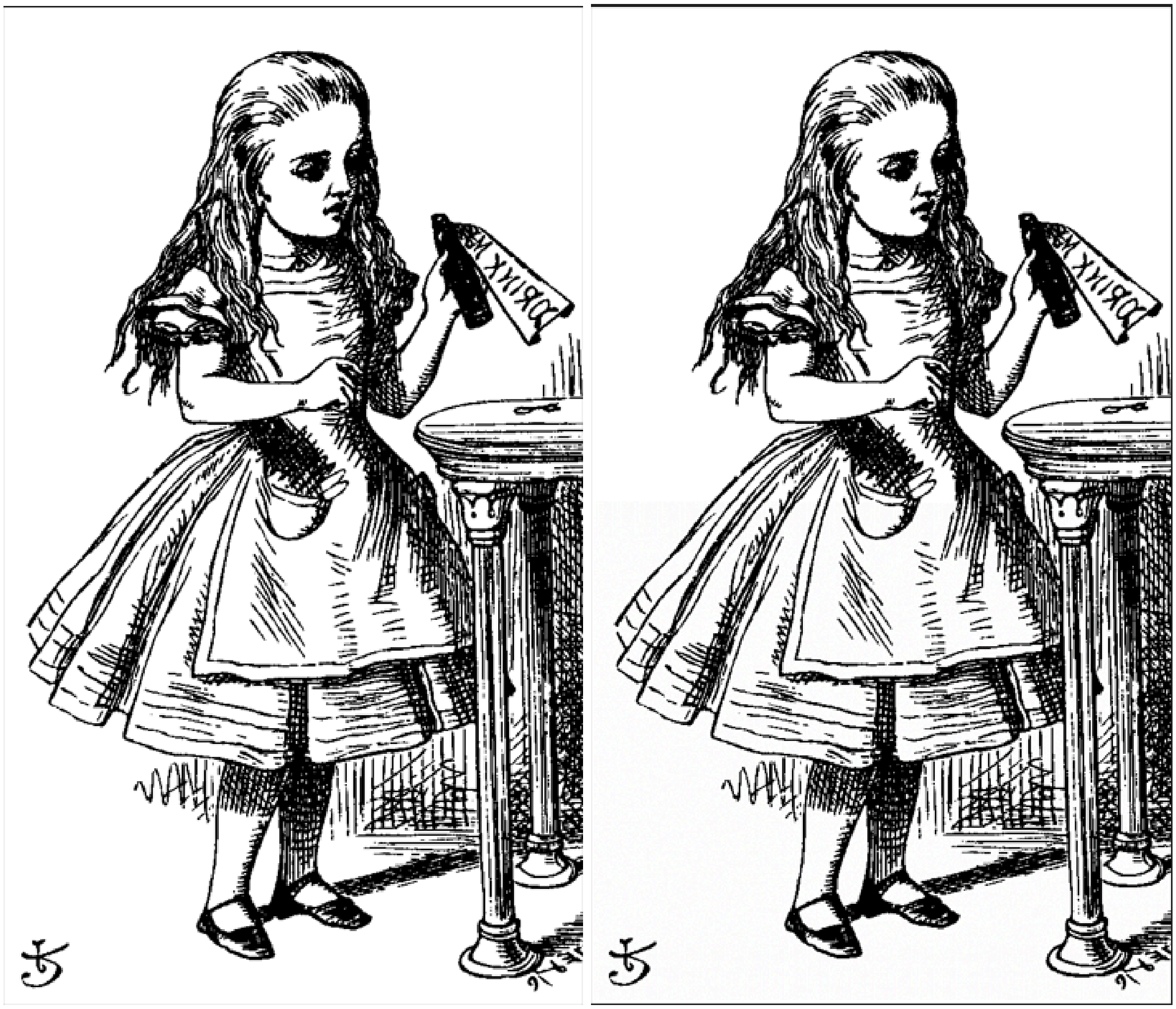
We can see that the entirety of Alice in Wonderland is hidden in pdf format.

b. Using the following commands

```
gcc -o stego stego.c
./stego alice.bmp insertstego.bmp aliceStego.pdf
```

we can insert aliceStego.pdf into insertstego.bmp

c. Left without hidden info, right with hidden info (cropping is a little messed up)



d. Converting the image to JPG keeps the image clean but it becomes unreadable (at least by stegoRead).