Homework 1

- Question 1) Scenario
  - A) Which/how CIA AA was affected (there are at least 7)
    - Authenticity = Chubs McGee was not the owner of the credit cards that were stolen, and so when he used them and was pretending to be the owner, he was breaking authenticity
    - Accountability = Walter should not have had his password on a sticky note so that when John got into the office, he should not have been able to login without it there.
    - Availability = The ease of access to the to the file without any secondary form of authentication to access such a sensitive document made it overly accessible for Jon once he logged into the computer (though Walter probably had the same password for that, or the Sticky note would have been longer)
    - Confidentiality = The customers trusted LKS to keep their information safe and away from prying eyes (like Johns) and so their data being leaked was a breach of their confidentiality.
    - Accountability = LKS trusted John to do his job they contracted him for and not to break into their offices so that was another breach.
    - Integrity = This was not touched as nothing was changed or deleted, just copied and sold.
  - B) Impact Severity Level

    - LKS: I would rate the impact as moderate or high based on the amount lost though I would lean towards high. This situation will cost the company money, paying back customers, investing into better security and encrypting, and employee training. The company will also lose support from current customers who may not return and reputation keeping newer customers away as well losing more money again.
    - Walter: I would hope the impact on Walter is High, causing severe issue and possibly the loss of his job with him having caused such issues for the companies losing money, customers, and reputation. This is a common issue among people that can be easily avoided with simple (seemingly common sense) practices, rules and training from the company too.
    - Customer's: High, the accumulation of excess debt for some people could be severe and lead to issue in the future in terms of credit score and financially. Could be moderate or low if the credit card company is nice and allows you to cancel the purchases or charges LKS for the issue they caused.
  - C) Security Terminology
    - Adversary: The contractor John.
    - Threat: Learning of sound on keypad and password available to anyone in the HR room and no MFA on client credit card data.
    - System Resource attacked: Physical security on door, and computer (Walter's), and important customer data
    - Vulnerability: Open password written on sticky notes, passcode key tone distinct per key for pattern recognition.

    - Attack Surface: Pin pad, Walter’s computer, accessable data.
- D) Active or Passive
    - I would say the learning of the door pin was a passive and possibly accidental process. From there, the rest of the attack was an active attack with Jon walking in, logging in, and stealing the information and handing it over to his land shark.
- E) Inside or Outside
    - This was and Outside attack being that it came from someone who was not employed by the company directly (though in a way he was) and shouldn’t have had access to any of the doors or computers that were involved. (Just being Inside the building does not make it an inside attack either)
- F) Threat Consequence and Attack Type
    - Unauthorized Disclosure by intrusion with John having the log in and the document being on the desktop.
    - Unauthorized Disclosure by inference with John learning the passcode for the door by passively hearing the chimes while working down the hall.
- G) Security Requirements
    - Personnel Security, with John being contracted in and gaining access, he most likely broke a terms of agreement between LKS and the contracting firm.
    - Audit and Accountability, it seemed Walter was not the only one in HR office and so others should have told him to hide his password and keep it safer. Or an auditor walking through could have noticed it had it changed.

        - Awareness and training, Walter should have known to not keep his password on a sticky note attached to his computer, especially being HR and having access to sensitive data.

- Question 2) Hash Function
    - True H(x) != H(x’), whether weak or strong collision resistance, a hash algorithm should make it infeasible for two different values to have the same hash.
    - Adding salt should make it so that even if x = x’ that they should be different as well.

- Question 3) Textbook 2.1
    - This plan does seem like a good idea. There is a chance of a vulnerability of a man in the middle attack as just xor’s the two passed values that you and your partner sent then they end up with the public key as well.

- Question 4) Textbook 2.5
    - A) Message Integrity: In both MAC and DS their would be the detection of tampering when Bob gets the message. MAC, Oscar doesn’t have the secret key, DS Oscar has the public key to decrypt the message but not the private key to re-encrypt the message and send it on its way.
    - B) Replay: This part I think I get confused with.
        - To me, Oscar can know the un-decrypted message and make a copy to decrypt for himself so yes.
        - Also the way we talked in class made it seem like that is not an option so no? This part I am confused on.

  - C) Sender Auth: For MAC transmissions the secret key is shared between the two so Bob should be able to tell who sent it. For DS similar is true, where the sender encrypts with the private key that only the public key for that person can decrypt.
  - D) Auth (bob cheated): For MAC, it is a shared key so it would be hard to tell if Bob made it up or Alice actually sent it. With DS, the original message would be encrypted with Alice's private key if it came from her so you could tell if she was the one who sent it.

- Question 5) Password Strength
  - To start, the book recommends a minimum of 16 characters based on the NIST standards of the time. Also, the inability of the system to handle symbols in the passwords eliminates much of the time needed to crack a password. Though it may be assumed but doesn't state it, the protection of these passwords after creation needs to be considered as well since a hash function (with salt for flavor) would be needed for further security to protect the password file.