CS166 Section-04
Mikhail Sumawan
Homework 2

Problem 1:

a. The security flow of this program starts with the method IsAccessAllowed() which checks the user if they have the privileged to access the data. Next, the first if statement basically checks if the value dwRet is equal to ERROR_ACCESS_DENIED, if it is equal, then the condition evaluates to true, the system check will fail and inform the user that their access has been denied. However, when the condition evaluates to false, the else code will get executed which allows for access to the privileged user. Taking a closer look, we can see that this program is heavily flawed on the IsAccessAllowed() method since the access variable for other conditions must go through there and if IsAccessAllowed() method were to fail by any reason it would evaluate the else code regardless because dwRet does not return anything.

b. To avoid the flaw in the previous code, I think the best way is to rely on a check for successful execution instead of a checking variable. I can rewrite this code as such:

```
DWORD dwRet = IsAccessAllowed(...);
If (dwRet == NO_ERROR){
    //Security Check OK
} else {
    //Security Check failed
    //User access Denied
}
```

In this code, if IsAccessAllowed() were to fail for any reason, it would not give access to the user because I rely on the success of execution to check if access is allowed.

Problem 2:

a. (Message Integrity) Bob will most definitely detect the changes in the message because the auth(x) value will not match with the x from the modified message he received. For both DS and MAC algorithms, the auth(x) would not match x, therefore Bob will certainly detect the changes in the message. The data enclosed with DS is signed with a private key but anyone with the public can check the authenticity of that data, while in MAC, the key is shared with all parties involved thus protecting the data from modifications without the key.
b. (Replay) Bob should not be able to detect this unless somehow the computation affected the value of auth(x) by sequence number or time-stamp.
c. (Sender Authentication with a cheating third party) Yes, Bob will be able to clear the question with both DS and MAC algorithms. With DS, Bob will use Alice's private key and public key to see if they match and is then used to authenticate message x. With

MAC, only Alice shared the secret key with Bob to generate the auth(x), the auth(x) generate by Oscar might work but it would not match the one calculated by Bob and Alice.

d. (Authentication with Bob cheating) Alice will be able to clear this question using DS because unique auth(x) gets generated using Alice's private key and verified with Alice's public key, therefore only Alice can generate the auth(x). However, for MAC, Alice will not be able to clear the question because auth(x) is generated and has to get verified with a secret key that both Alice and Bob hold.

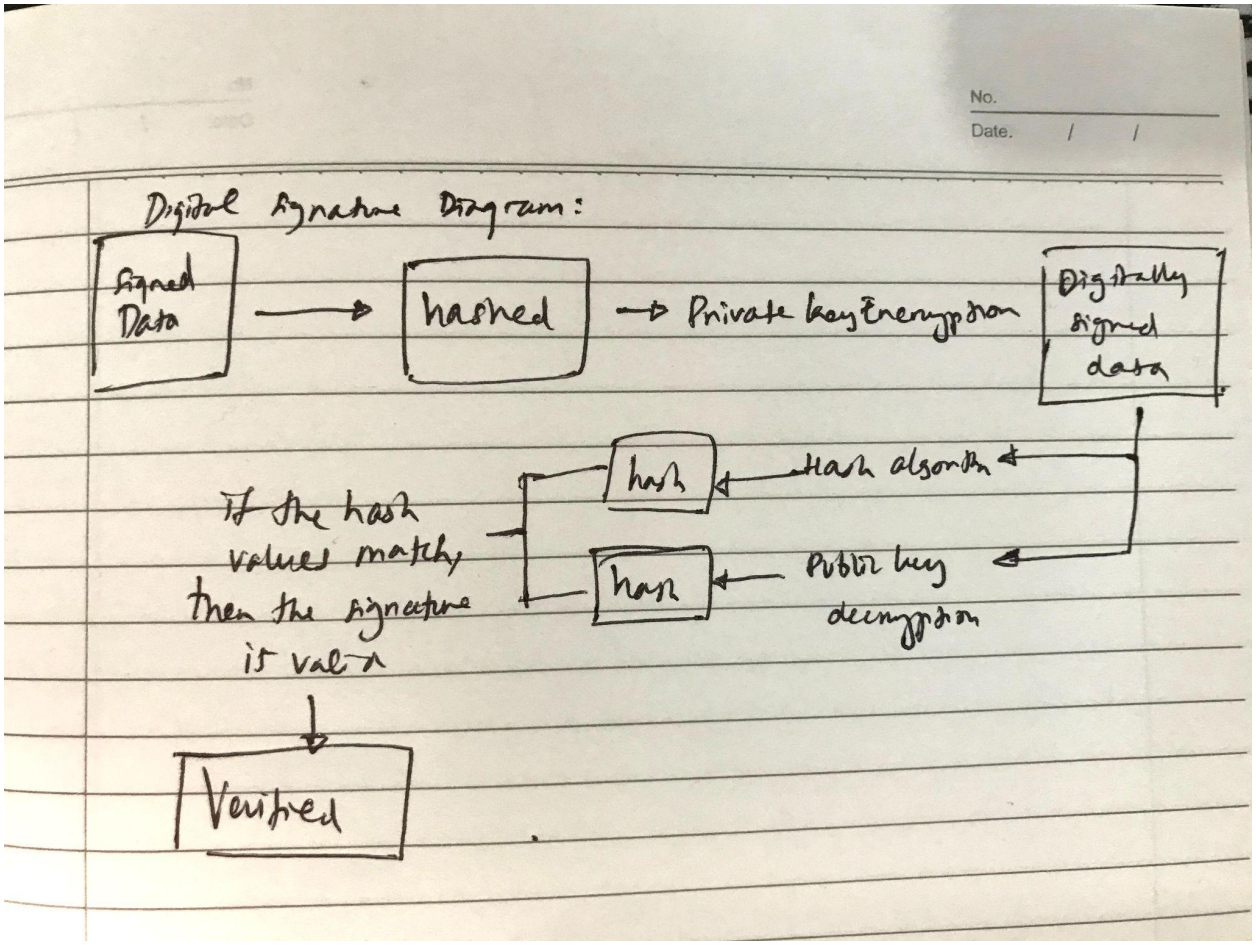
Problem 3:

a. By looking at the frequency of each letter in that ciphertext, I can tell that the first letter t corresponds to A, letter h corresponds to B, letter e corresponds to C, and so on. Looking at this pattern, we can deduct that that each letter corresponds to another letter, while second and subsequent occurrences of letter from the key are to be ignored. The ciphertext: SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA. Translate to the plaintext: basilisk to leviathan blake is contact.
b. This is a monoalphabetic cipher algorithm which is very vulnerable and can be easily broken with cryptoanalysis and frequency testing.
c. The use of the first sentence is much preferable than the use of the last, because when the first sentence is used, the second and subsequent sentences may also be used until it exhausted all 26 letters of the alphabet, however, if the last sentence is used, it may or may not contain all letters of the alphabet.

Problem 4:

a. To achieve their goal only with secret-key cryptography:
   Sender -> Recipient : M || Ek (M).
b. To achieve their goal only with hash function:
   Sender -> Recipient : {M || Ek (H (M))}
c. It is not possible for them to get non-repudiation using only a commonly shared key, this is because the sender can reject the previously authenticated message by claiming that the shared secret is compromised for any reason. There is also a possibility where a recipient who has the same copy of the shared secret key might have forge the signature.
d. I think that A and B can achieve non-repudiation using digital signatures. Digital signature uses an asymmetric key operation to digitally sign the message/data with the private key and uses the public key to verify the signature. Digital signatures provide authenticity and integrity protection as well as non-repudiation to the recipient.

Diagram for 4. d to show the procedure:



Problem 5:

a. A passive attack is a type of attack that does not directly engage with the target. A passive attack works with monitoring, observing, or eavesdropping on the target's transmission. Passive attack also doesn't have any impact on the system resources and does not modify any data, therefore the data stay unchanged. Passive attacks usually aim to achieve vulnerabilities or data from the victim/target's network, passive attacks usually would escalate to active attacks. Now, on the other hand, an active attack is a type of attack that is directly involved in modifying data and altering contents that impact the system's resources. An active attack will cause damage to the victim/target and poses a threat to the integrity and accessibility of data, the goal of an active attack is usually to gain unauthorized access/privileged in computer systems.

b. Few examples of passive and active attacks:

Passive Attack	Active Attack
Eavesdropping attack	Denial-of-Service (DoS)
Sniffing networks and recording the traffic	Trojan Horse attack
	Man-in-the-Middle attack (MitM)