**Q (1)[12] Answer the following question about digital Signature.**

**A)What is digital Signature?**

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash

•The document is first run through a one-way hashing algorithm that is very difficult to invert (e.g., MD5 or SHA)

• The hash typically produces a fixed-length result independent of the original document size

• The document owner applies his private key to the hashed document – this encrypted result is called the signature block

• The signature block is appended to the document and both are sent to the receiver

• When the document arrives, the receiver first computes the hash of the document as agreed upon

• Then the receiver applies the sender’s public key to the signature block, getting the hash computed by the sender

• This hash must match the hash of the document computed by the receiver

• A digital signature also makes it possible to sign e-mail messages and other digital documents such that they cannot be repudiated by the sender late

**B)** **Let m be a message. Suppose Alice and Bob share a secret key k. Alice sends Bob m || { m }k (that is, the message and its encipherment under k). Is this a digital signature?**

First, Alice has authenticated the contents of the message, because Bob deciphers { m }k and can check that the message matches the deciphered one. Because only Bob and Alice know k, and Bob knows that he did not send the message, he concludes that it has come from Alice. He has authenticated the message origin and integrity. However, based on the mathematics alone, Bob cannot prove that he did not create the message, because he knows the key used to create it. Hence, this is not a digital signature

**Q[2][11] Answer the following questions about kereboeros Protocol.**

**A)Describe briefly the roles of the 3 different servers used in kerboeros**

Kerberos uses the Needham-Schroeder protocol as modified by Denning and Sacco. Kerberos is used to control access to servers (file server, print server, etc). It emphasizes the difference between authentication (determining who the user is) and authorization (determining what the authenticated user is allowed to do).

The name Kerberos refers to the three headed dog from Greek mythology that guarded the gates of hell. The three heads are

1. The authentication server which authenticates a user and issues him a ticket that allows him to use the authorization server

2. The authorization (ticket-granting) server checks whether the user is authorized to use the requested server and if so issues him a ticket to use the server.

3. The server checks to make sure that the authorization server's ticket is valid and if so grants the user access to the server.

**B) what is potential problem of kerboeros?**

Kerberos relies on clock synchronization and also dictionary attack is possible which can break this protocol.

Kerberos relies on clocks being synchronized to prevent replay attacks. If the clocks are not synchronized, and if old tickets and authenticators are not cached, replay is possible. Also, because the tickets have some fixed fields, a dictionary attack can be used to determine keys shared by services or users and the ticket-granting service or the authentication service, much as the WordPerfect cipher was broken.

**Q.3 [9] Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad.**

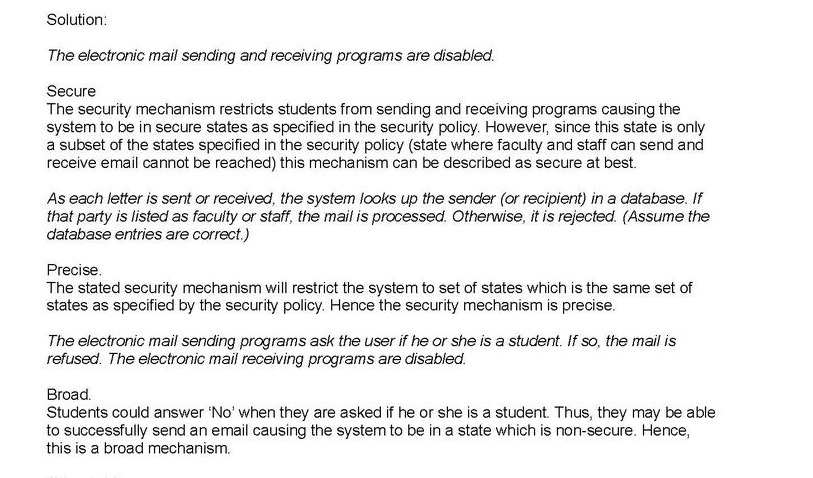
a. The electronic mail sending and receiving programs are disabled.[secure]

b. As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.)

[precise]

c. The electronic mail sending programs ask the user if he or she is a student. If so, the

mail is refused. The electronic mail receiving programs are disabled. [broad]



**Q[4][9]**

**The security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest)The categories are A, B and C.**

**Discretionary access controls allow anyone access unless**

**otherwise specified**

**[3] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}). What types of access does she have?**  
CONFIDENTIAL is greater than UNCLASSIFIED and the empty set (the categories of Robin) is a subset of {B} so the object dominates the subject and hence Robin can write.

**[3] Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}). What type of access does he have?  
neither**

**[3] Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}). What types of access does he have?**

**read**

C S S E 442 – Computer Security      Rose‐Hulman Institute of Technology     
Winter 2008‐2009    Computer Science and Software Engineering  
**Homework 4 solutions**  
**Due: 9th February(Monday), in class**  
1. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED   
(ordered from highest to lowest), and the categories A, B, and  C, specify what type of access   
(read, write, both, or neither)  is allowed in each of the following situations. Assume that the   
discretionary access controls allow anyone access unless otherwise specified.   
a. Paul, cleared for (TOP SECRET, {A,C}}, wants to access a document classified   
(SECRET, {B,C}}.   
b. Anna, cleared for {CONFIDENTIAL,{C}}, wants to access a document classified   
(CONFIDENTIAL, {B}}.   
c. Jesse, cleared for {SECRET, {C}}, wants to access a document classified   
{CONFIDENTIAL, {C}}.   
d. Sammi, cleared for {TOP SECRET,  {A,C}}, wants to access a document classified   
{CONFIDENTIAL, {A}}.   
e. Robin, who has no clearances (and so works at the UNCLASSIFIED  level), wants to   
access the document classified (CONFIDENTIAL, {B}).   
    **Answers:**    
Let *A*’s compartment be (*LA*, *CA*) and *B*’s be (*LB*, *CB*). The simple security condiion says that  
*A* can read *B* if and only if *LA* ≥ *LB* and *CB* ∏ *CA*. The \*-property says that *A* can write *B* if  
and only if *LB* ≥ *LA* and *CA* ∏ *CB*. Remember that TOPSECRET ≥ SECRET ≥  
CONFIDENTIAL ≥ UNCLASSIFIED.  
a. *L*Paul = TOPSECRET ≥ SECRET = *L*doc, so Paul cannot write the document. Paul cannot  
read the document either, because *C*doc = { B, C } ℵ { A, C } = *C*Paul.  
b. *L*Anna = CONFIDENTIAL ≥ CONFIDENTIAL = *L*doc, but *C*doc = { B } ℵ { C } = *C*Anna so  
Anna cannot read the document, and *C*Anna = { C } ℵ { B } = *C*doc, so Anna cannot write  
the document.  
c. *L*Jesse = SECRET ≥ CONFIDENTIAL = *L*doc, and *C*doc = { C } ∏ { C } = *C*Jesse, so Jesse  
can read the document. As *L*Jesse > *L*doc, however, Jesse cannot write the document.  
d. As *L*Sammi = TOPSECRET ≥ CONFIDENTIAL = *L*doc and*C*doc = { A} ∏ { A, C } =  
*C*Sammi, Sammi can read the document. But the first inequality means Sammi cannot  
write the document.  
e. As *C*Robin = ∅ ∏ { B } = *C*doc and *L*doc = CONFIDENTIAL ≥ UNCLASSIFIED = *L*Robin,  
Robin can write the document. However, because *L*doc ≥ *L*Robin, she cannot read the  
document

**Q5[9] Advantages of CAs over KDCs**

The CA doesn't have to be online. It can be in a locked room, create a certificate and put it on a floppy disk. A user has to communicate with a KDC online (as described in lecture 8) to get a session key.

• Since a CA is not online, it can be simpler (economy of mechanism)

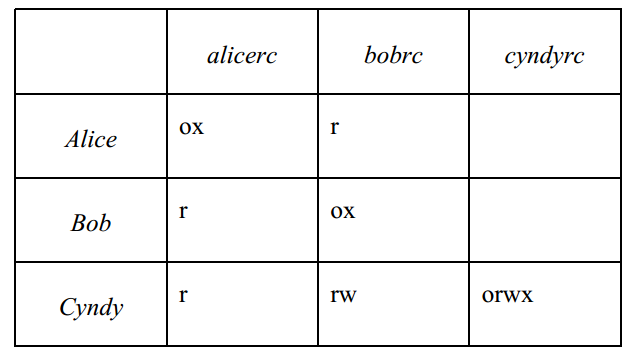
• There is no single point of failure for a CA. But if the KDC (Cathy) goes down, Alice and Bob cannot create a session key.

• Certificates are not security sensitive. All an attacker can do is delete certificates, he can't create bogus certificates because he doesn't have the private key of the CA.

• Since a compromised CA doesn't have a private key, it can't decipher conversations but a compromised KDC can (it has the keys that it shares with the users that trust it). That is, you have to trust a KDC more than a CA. All you give the CA is your public key.

**Q 9 [6] Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file obrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it.**

**a. Create the correspond ing access matrix**



**Q. 10[6] Briefly explain how clark-wilson integrity model support the separation of duty .**

The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user. The TP cannot access that CDI on behalf of a user if she/he is not associated with that TP and CDI.

* + System must maintain, enforce certified relation
  + System must also restrict access based on user ID (*allowed* relation)
  + Now we have human, and we have to enforce separation of duty and authentication

**Q 11[6] Differentiate between a known plaintext attack and chosen plaintext attack.**

* Known plaintext

Adversary has the ciphertext for a known plaintext, wants to find the key

* Chosen plaintext

Adversary can generate ciphertext for any plaintext, wants to find the key

The **known**-**plaintext attack** (KPA) is an **attack** model for cryptanalysis where the attacker has access to both the **plaintext** (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

A **chosen**-**plaintext attack** (CPA) is an **attack** model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary **plaintexts**. The goal of the **attack** is to gain information which reduces the security of the encryption scheme