


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Information Security	Course Code:	CS3002
	Degree Program:	BS (CS)	Semester:	Fall 2021
	Exam Duration:	2 hours 30 mins	Total Marks:	60
	Paper Date:	22/01/22	Weight:	40
	Exam Type:	Final exam	Page(s):	7

Student Name: SOLUTION (MADE BY STUDENT) Roll No. _____ Section: _____

Instruction: If you think some information is missing then make assumption and write it clearly.

Question 1 a: MCQs and True/False

[10 Marks]

1.1 A trusted third party who provides a way for one party to learn the public key of another party.

- a) Certification authority
- b) Registration authority
- c) Learning authority
- d) Information authority

1.2 A way of checking whether the private key matching the public key in a certificate has been compromised and so the certificate should no longer be accepted.

- a) expired list
- b) rejection list
- c) revocation list
- d) all of the above

1.3 Critical action(s) required on termination of employment includes:

- a) remove name from authorized access list
- b) disclose personal access codes of that person
- c) reuse his lock combinations/access card
- d) inform guards that general access not allowed

1.4 _____ is a set of conventions & rules set for communicating two or more devices residing in the same network?

- a) Security policy
- b) Protocol
- c) Wireless network
- d) Network algorithm

1.5 _____ is used for encrypting data at network level.

- a) IPSec
- b) HTTPS
- c) SMTP
- d) None of the above

1.6 Which of the following is not a strong security protocol?

- a) HTTPS
- b) SSL
- c) SMTP
- d) SFTP

1.7 _____ refers to the extent a device is capable for capturing and detecting any unwanted events.

- a) Acquisition
- b) redaction
- c) Forensic Readiness
- d) None of the above

1.8 Authenticity is not part of the CIA triad

- a) True
- b) False

1.9 Data backup is used to ensure confidentiality.

- a) True
- b) False

1.10 If Alice has a message to send to Bob and she wants to encrypt the message using asymmetric cryptography so that no one other than Bob can read it, she does so by using Bob's public key.

- a) True
- b) False

Question 1 b: [4+4]

Alice and Bob both work in the same organization. Alice works at the executive level while Bob works in the IT department which is at a lower level in the organization compared to Alice. Describe the read, write, etc privileges available to Alice and Bob by filling out following blanks for (a) Bell-Lapadula Model (b) Biba Model.

(a) Bell-Lapadula Model

Alice → read data of Bob → (Allowed/NotAllowed): Allowed

Bob → read data of Alice → (Allowed/NotAllowed): Not Allowed

Bob → write data at Alice's level → (Allowed/Not Allowed): Allowed

Alice → write data at Bob's level → (Allowed/Not Allowed): Not Allowed

(b) Biba Model

Alice → read data of Bob → (Allowed/NotAllowed): Not Allowed

Bob → read data of Alice → (Allowed/NotAllowed): Allowed

Bob → write data at Alice's level → (Allowed/Not Allowed): Not Allowed

Alice → write data at Bob's level → (Allowed/Not Allowed): Allowed

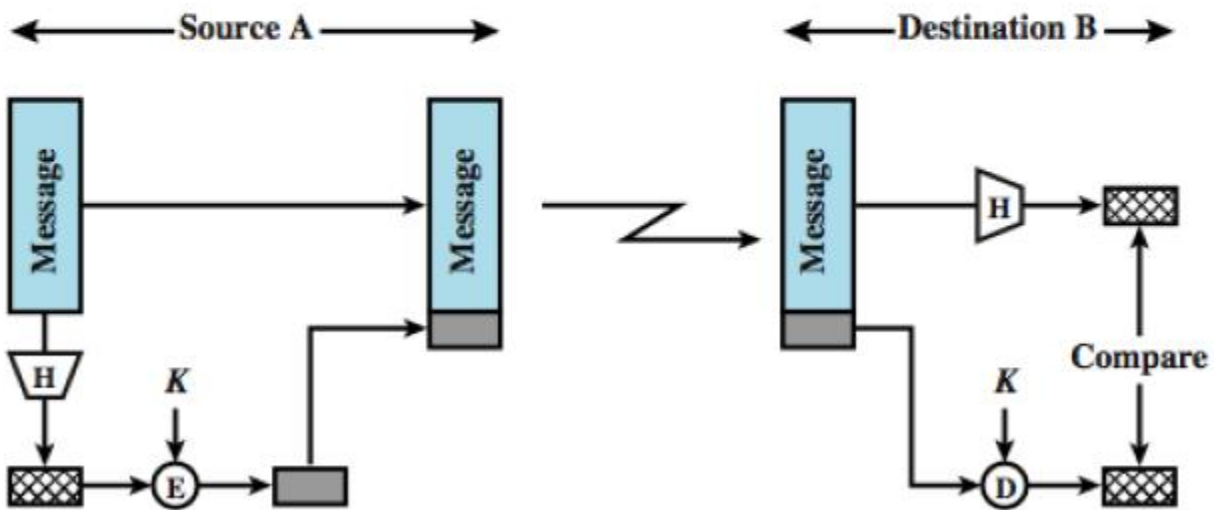
Question 2: [5+5]

User A wants to download an operating system image from the vendor website. On downloading the OS image, the user should be able to assess the integrity of the OS image in an optimal way. Draw a diagram to illustrate the process, which may include the use of hash functions, and comparison as applicable. Briefly describe each step of the process illustrated in your diagram.

Diagram:

Following figure BUT with an important change:

- at the sending side, the key K is the private key of OS vendor
- at receiving side, K is public key of OS vendor



Process Steps:

Vendor will have to create and attach MAC to in order to prove the integrity and authenticity of the downloaded image. Vendor signs the MAC with their private key. User downloads the image and verifies the MAC with vendor's public key.

Question 3: [6+6]

- a) What is inferential attack and how Perturbation can avoid inferential attack? Provide detail of one perturbation technique!

Inferential Attack refers to the type of attack where an attacker accesses authorized information and uses it to infer unauthorized information hence figuring out information that was supposed to be secret.

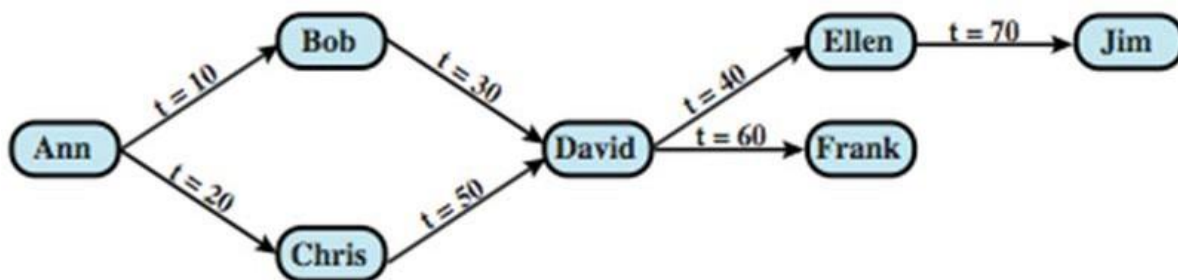
Perturbation adds noise to the statistical data generated.

Attacker does not get exact information and hence is not able to retrieve any fruitful unauthorized information.

Perturbation is of 2 Types:

- 1) Data Perturbation: Swaps attribute data between rows so that individual records are not accurate but overall statistical information does not change
- 2) Output Perturbation
 - a) Random Sample Query: Processes Query on a subset of rows
 - b) Statistical Adjustment: Increases or decreases output value by a given amount in some systematic fashion

- b) Briefly explain the concept of cascading authority in access control. In the following scenario, David has been given authority by both Bob and Chris. What will happen if either Bob or Chris revokes the authority? Provide detail for both cases (Bob revokes, Chris revokes).



Cascading Authority Refers to the concept of removing authority from people who were given access to something by someone who no longer has access i.e. their access has been revoked.

In this scenario,

If bob revokes:

Ellen and Jim's access is also revoked because Ellen was given access by David before Chris gave David access and Jim got access from Ellen.

David access is revoked from Bob side but is still present from chris

If Chris revokes:

David's Access from Chris is revoked but from Bob remains

the rest remains this is because 'When user A revokes an access right, any cascaded access right is also revoked unless that access right would exist even if the original grant from A never occurred.' Here, Frank could have been given access by David even if Chris never gave David the access as Bob already did.

Question 4: [8+12]

- a) **Why the Challenge response authentication is better than password based authentication? How this process works? What is the difference between Symmetric and Asymmetric challenge response authentication? Explain by depicting the whole process including encryption and keys being used!**

Challenge Response Authentication is better than Password Based Authentication because there is no transfer of actual password hence more security.

The process of Challenge Response Authentication works by server sending client a challenge and client responds with the solution and server verifies if the response is correct.

This process can be done in two ways:

1) Using Symmetric Cryptography:

Here, the server sends a Random number R, to client who then encrypts it using the shared key and sends to server. Server also encrypts the Random Number R using the same shared key and then matches them both if they are same client is successfully authenticated.

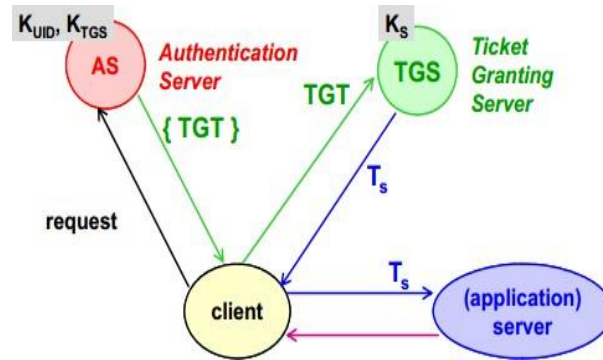
2) Using Asymmetric Cryptography:

Here, the server encrypts the Random number R, using the public key of Client and sends this to Client. Client decrypts this using its private key and sends random number R back to server. Server verifies the Number R is correct and if it is, client is successfully authenticated.

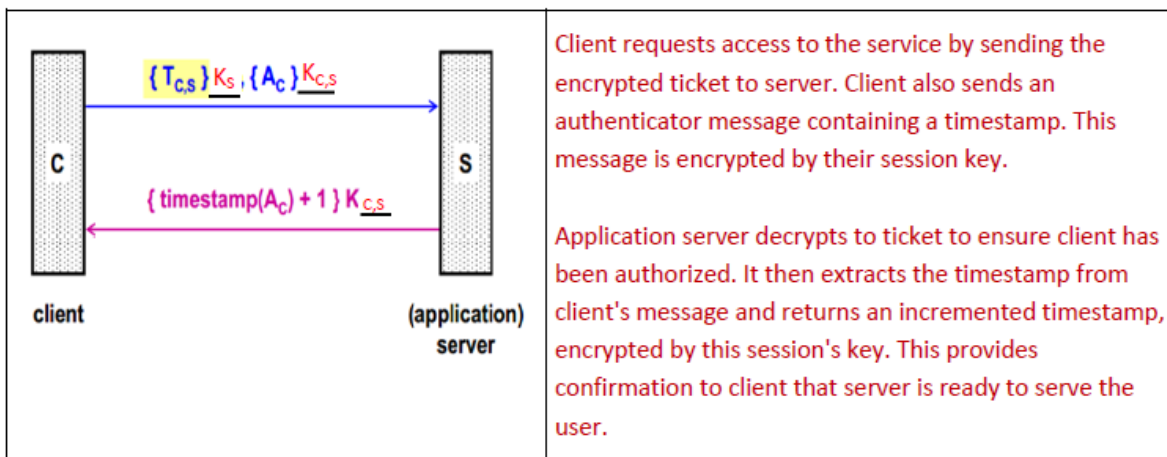
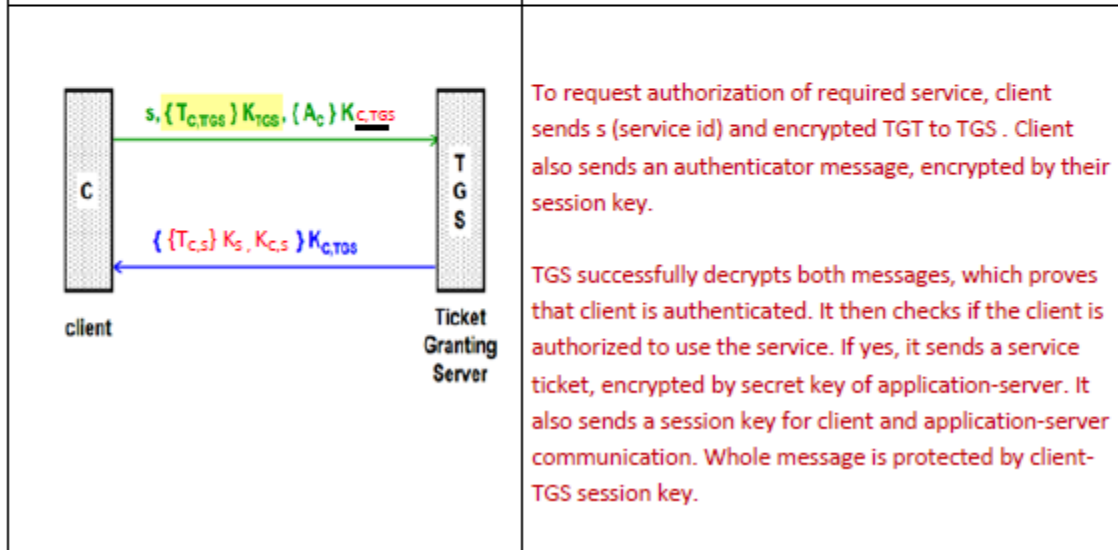
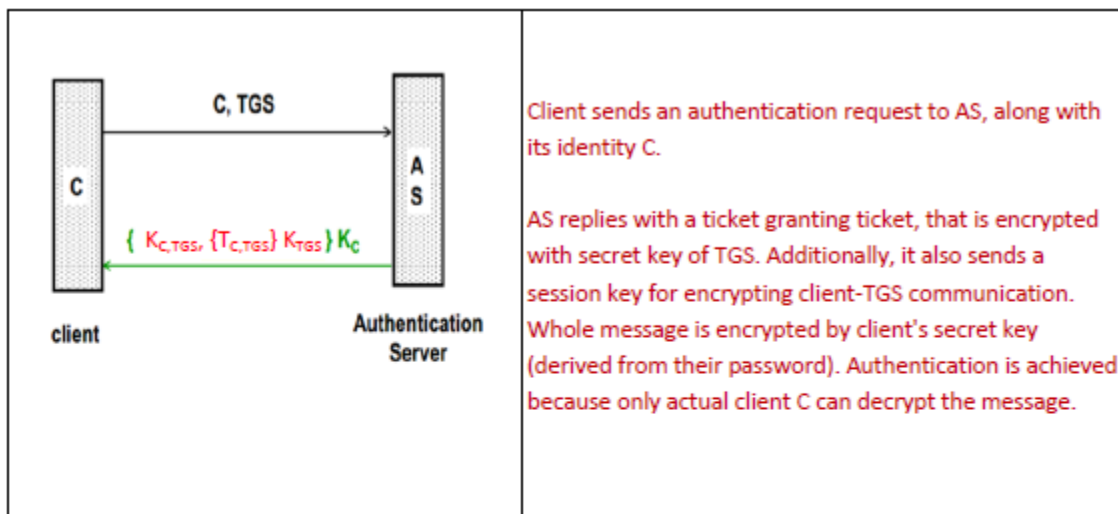
b) What is centralized authentication?

It refers to the concept of using one server for authentication instead of separate authentications required for use of each service.

The following figure depicts the Kerberos Authentication process with keys involved.



- i. If a client wants to access a specific service from application server then how the user will be authenticated? Partial information is provided in the following figures. Complete the missing information and explain each process in the right column.



- ii. **What is the role of TGS server? Why not the service is granted directly after authentication from AS server?**

TGS Server generates and sends the Service Ticket to Client after successfully verifying client's credentials and allowance to use the service.

This ensures the service is only granted if it is available and client is allowed access to it

- iii. **If the ticket generated by servers is given to client for forwarding then why the client cannot modify it.**

The tickets are encrypted using keys of other servers making sure only those servers can decrypt them. Client does not have their keys hence is unable to decrypt the tickets and modify them