Operating Systems
UNIT – V

SHAIK VAHIDA

2/24/2022

UNIT -V

System Protection: Goals of protection, Principles and domain of protection, Access matrix, Access control, Revocation of access rights.

System Security: Introduction, Program threats, System and network threats, Cryptography for security, User authentication, Implementing security defenses, Firewalling to protect systems and networks, Computer security classification.

Case Studies: Linux, Microsoft Windows.

System Protection

Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system.

Need of Protection:

- To prevent the access of unauthorized users
- To ensure that each active programs or processes in the system.
- To improve reliability by detecting errors.

Goals of Protection

- prevent malicious misuse of the system by users or programs.
- To ensure that each shared resource is used only in accordance with system *policies*.
- To ensure that errant programs cause the minimal amount of damage possible.
- protection systems only provide the *mechanisms* for enforcing policies and ensuring reliable systems.

Principles of Protection

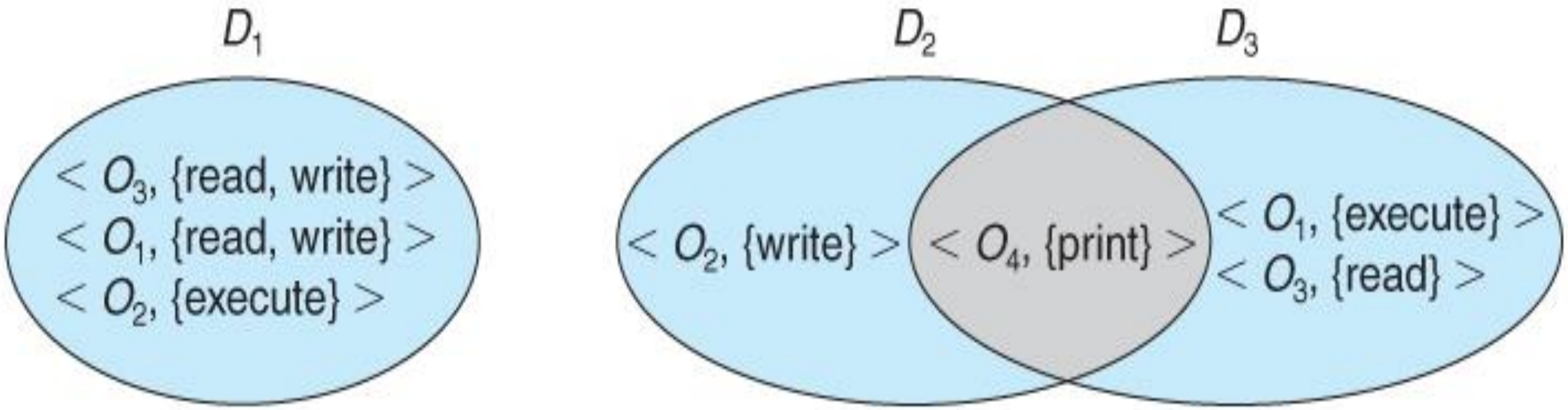
- The ***principle of least privilege*** dictates that programs, users, and systems be given just enough privileges to perform their tasks.
- This ensures that failures do the least amount of harm and allow the least of harm to be done.
- For example, if **a program needs special privileges to perform a task, it is better to make it a SGID program with group ownership of "network" or "backup”.**
- Typically each user is given their own account, and has only enough privilege to modify their own files.
- The root account should not be used for normal day to day activities .

Domain of Protection

- A computer can be viewed as a collection of *processes* and *objects* (both HW & SW).

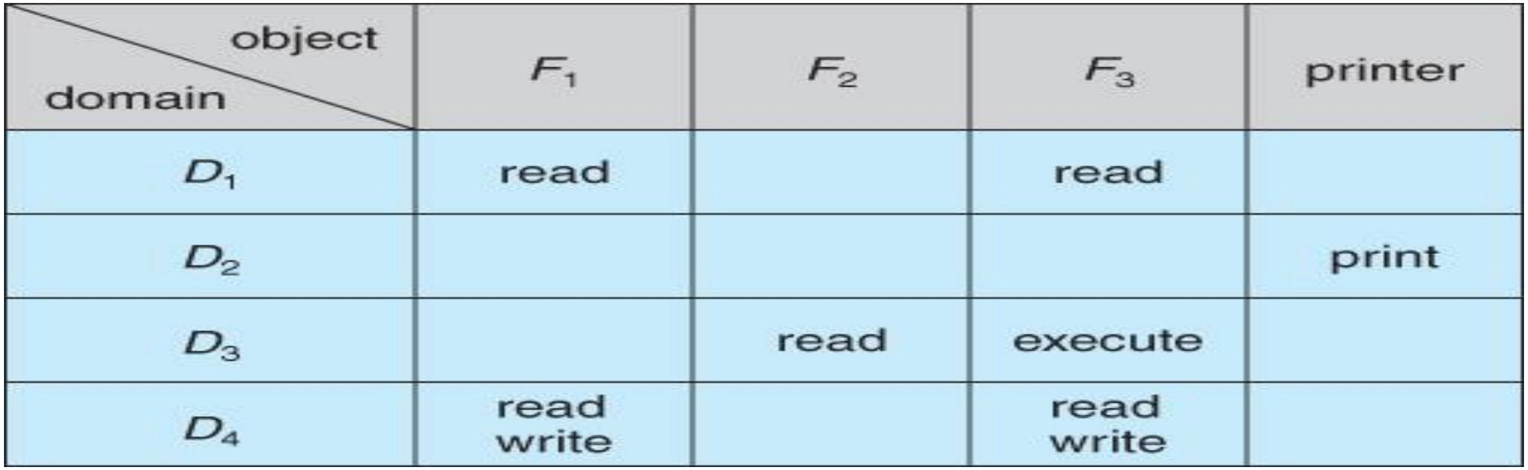
Domain Structure

A domain is defined as a set of < object, { access right set } > pairs, as shown below. Note that some domains may be disjoint while others overlap.



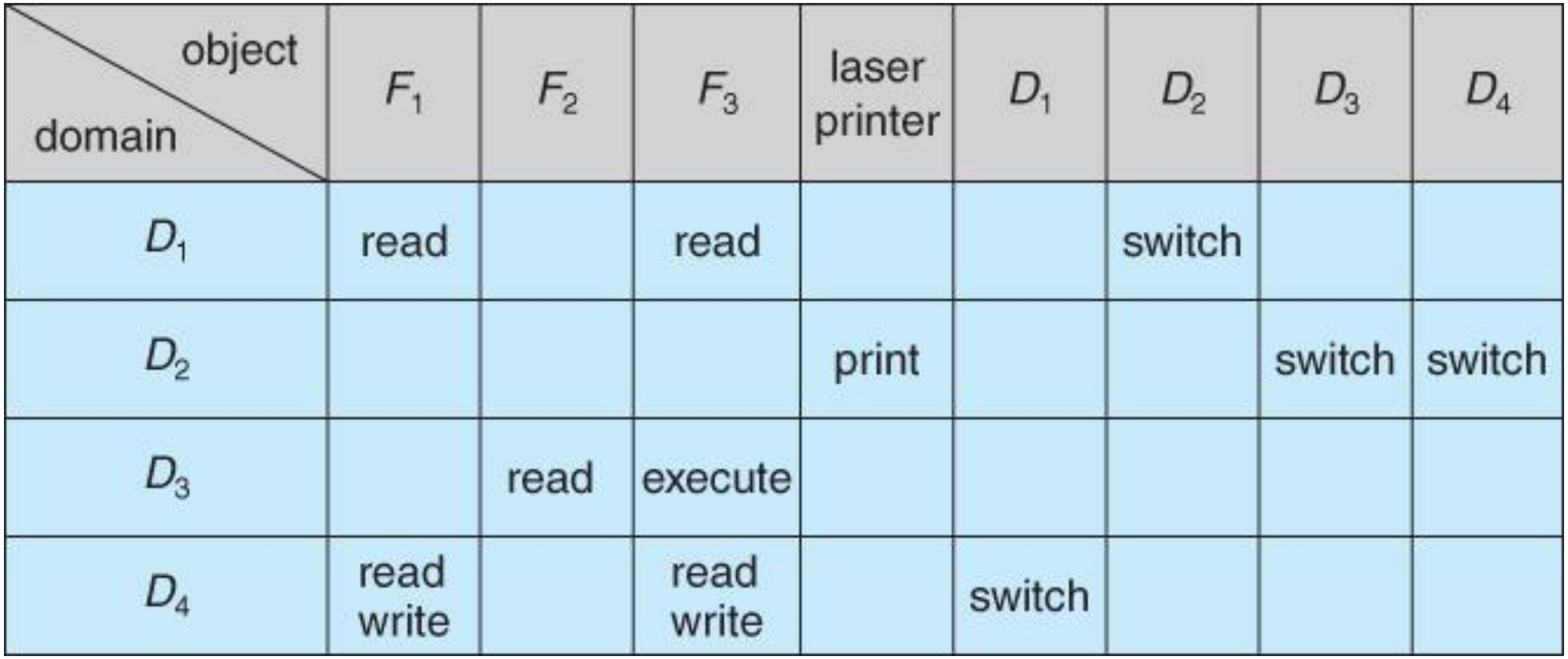
Access Matrix

- The model of protection that can be viewed as an ***access matrix***, in which columns represent different system resources and rows represent different protection domains.
- Entries within the matrix indicate **what access that domain has to that resource.**



object domain	F_1	F_2	F_3	printer
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read write		read write	

- Domain switching can be easily supported under this model, simply by providing "switch" access to other domains



object domain	F_1	F_2	F_3	laser printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	execute					
D_4	read write		read write		switch			

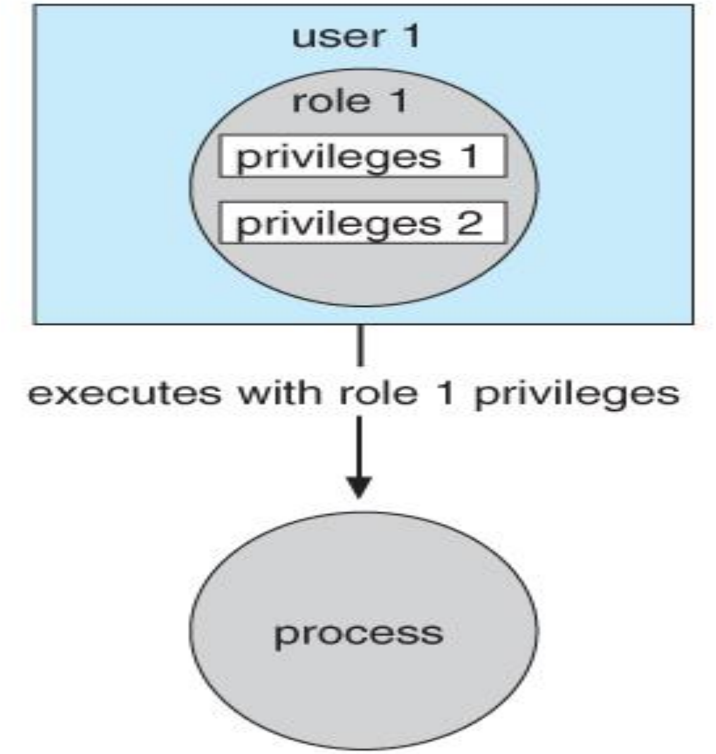
Implementation of Access Matrix

- Global Table
- Access Lists for Objects
- Capability Lists for Domains
- A Lock-Key Mechanism
- Comparison

Access Control

- *Role-Based Access Control*, ***RBAC***, assigns privileges to users, programs. where "privileges" refer to the right to call certain system calls, or to use certain parameters with those calls.

Role-based access control in Solaris 10



Revocation of Access Rights

The need to revoke access rights dynamically raises several questions:

- Immediate versus delayed
- Selective versus general
- Partial versus total
- Temporary versus permanent

System Security

Security refers to providing a protection system to computer system resources such as **CPU, memory, disk, software programs and most importantly data/information stored in the computer system.**

- Authentication
- One Time passwords

Program Threats

If a user program made these process do malicious tasks, then it is known as **Program Threats**.

example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker.

- **Trojan Horse** program traps ***user login credentials and stores them to send to malicious user.***
- **Trap Door** ***perform illegal action without knowledge of user.***
- **Logic Bomb** when a ***program misbehaves only when certain conditions*** met otherwise it works as a genuine program.
- **Virus** replicate themselves on computer system. They ***are highly dangerous and can modify/delete user files, crash systems.***

System AND Network Threats

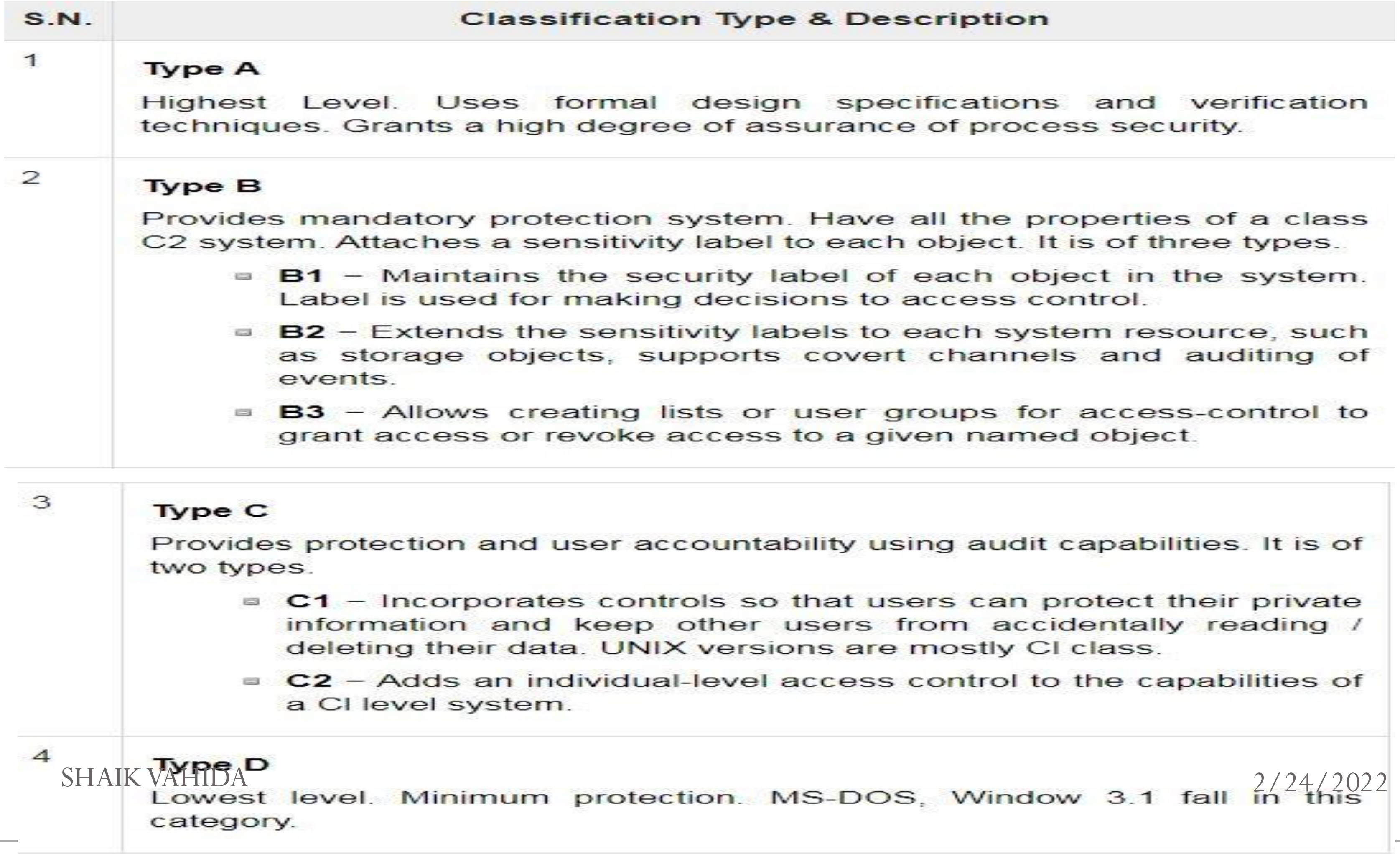
System and network threats refers to misuse of system services and network connections to put user in trouble.

System threats can be used to launch program threats on a complete network called as program attack.

- **Worm** – A Worm process ***generates its multiple copies where each copy uses system resources***, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
- **Port Scanning** – Port scanning is a mechanism or means by which a *hacker can detects system vulnerabilities to make an attack on the system.*
- **Denial of Service** – Denial of service attacks normally prevents user to make legitimate use of the system. For example, a *user may not be able to use internet if denial of service attacks browser's content settings.*

Computer Security Classifications

- As per the U.S. Department of Defence Trusted Computer System's Evaluation Criteria there are ***four security classifications in computer systems: A, B, C, and D.***

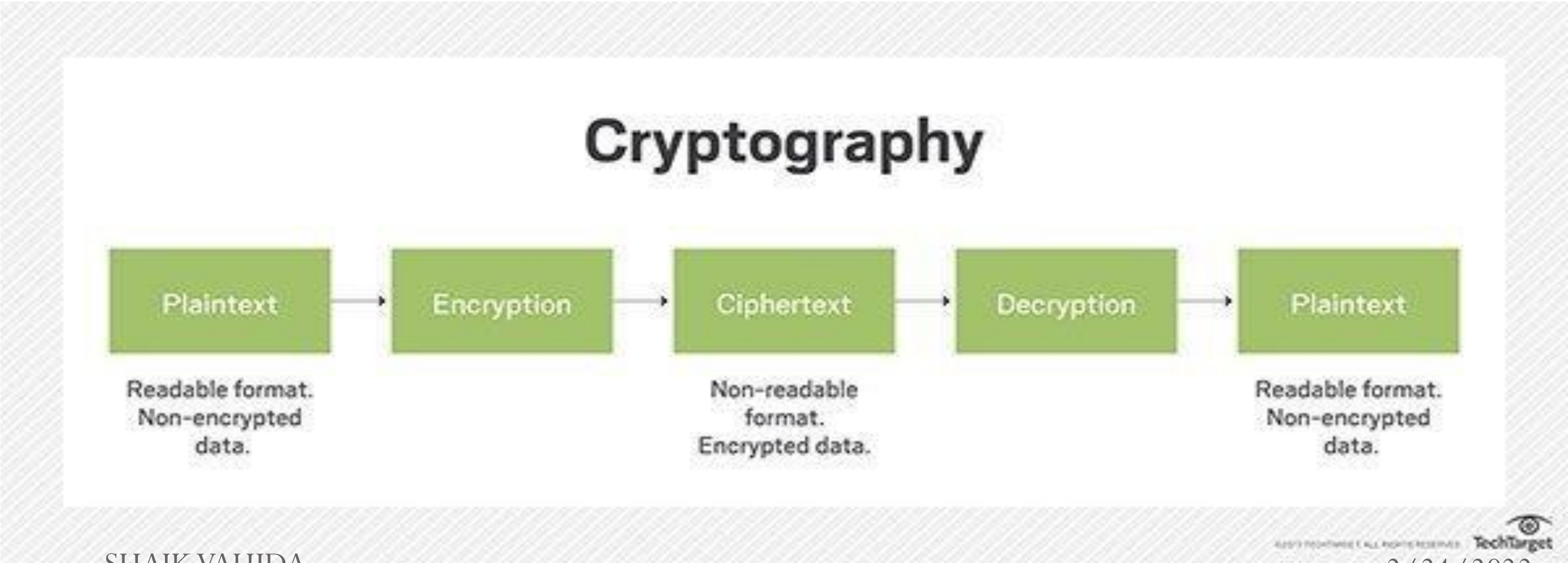


S.N.	Classification Type & Description
1	**Type A** Highest Level. Uses formal design specifications and verification techniques. Grants a high degree of assurance of process security.
2	**Type B** Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object. It is of three types. ▫ **B1** – Maintains the security label of each object in the system. Label is used for making decisions to access control. ▫ **B2** – Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events. ▫ **B3** – Allows creating lists or user groups for access-control to grant access or revoke access to a given named object.
3	**Type C** Provides protection and user accountability using audit capabilities. It is of two types. ▫ **C1** – Incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly CI class. ▫ **C2** – Adds an individual-level access control to the capabilities of a CI level system.
4	**Type D** Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category.

Cryptography for security

Cryptography is technique of securing information and communications through use of codes, so that only those person for whom the information is intended can understand it and process it.

Thus preventing unauthorized access to information.


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
TechTarget

Features Of Cryptography are as follows:

- **Confidentiality:**
  Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:**
  Information cannot be modified in storage or transition between sender and intended receiver.
- **Non-repudiation:**
  The sender of information *cannot deny his intention to send information at later stage*.
- **Authentication:**
  The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types Of cryptography:

1. **Symmetric Key Cryptography**
2. **Hash Functions**
3. **Asymmetric Key Cryptography**

- **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.

Symmetric Key Systems are faster and simpler.

- **Hash Functions:** There is no usage of any key in this algorithm.

A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.

Many operating systems use hash functions to encrypt passwords.

- **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information.

A public key is used for encryption and a private key is used for decryption.

Public key and Private Key are different.

User authentication

- User authentication process is used to identify who the owner is or who the identified person is.
- In personal computer, generally, user authentication can be perform using **password**.

User can be authenticated through one of the following way:

- User authentication **using password**
- User authentication **using physical object**
- User authentication **using biometric**
- User authentication **using countermeasures**

User authentication **using password**

- Password should be minimum of eight characters
- Password should contain both uppercase and lowercase letters
- Password should contain at least one digit and one special characters
- Don't use dictionary words and known name such as stick, mouth, sun, albert etc.

User authentication **using physical object**

Here, physical object may refer to Bank's Automated Teller Machine (ATM) card or any other plastic card that is used to authenticate.

User authentication **using biometric**

- This method measures the physical characteristics of the user that are very hard to forge. These are called as biometrics.
- User authentication using biometric's example is a fingerprint, voiceprint, or retina scan reader in the terminal could verify the identity of the user.

User authentication **using countermeasures**

- For example, a company could have their policy that the employee working in the Computer Science (CS) department are only allowed to log in from 10 A.M. to 4 P.M., Monday to Saturday, and then only from a machine in the CS department connected to company's Local Area Network (LAN).
- Now, any attempt to log in by a CS department employee at any wrong time or from any wrong place would be treated or handled as an attempted break in and log in failure.