chapter 8 Security.

2075 Bhadra.

Q. Explain private and public key used in assymetric cryptography. what is the use of ACL?

Ans:- Assymetric encryption use a mathematically related key pair for encryption and decryption; one is the public key and other is the private key.

If the public key is used for encryption; the related ~~privated~~ private key is used for decryption and vice versa. Only the user or computer that generates the key pair has the private key. The public key can be distributed to anyone who wants to send encrypted data to the holder of the private key. The two participants in the assymetric encryption workflow are the sender and the receiver. First, the sender obtains the receiver's public key. Then the plaintext is encrypted with the assymetric encryption algorithm using the recipient's public key, creating the ~~ciphe~~ ciphertext. The ciphertext is then sent to the receiver, who decrypts the ciphertext with this private key so that we can assess the sender's plaintext.

Use of ACL

1. ACL are filters that enable us to control which routing updates or packets are permitted or denied in or out of the network
2. They are specially used by network administrators

to filter traffic and to provide extra security for the network.

3. ACLS provide a powerful way to control traffic into and out of our network.

2074 Bhadra

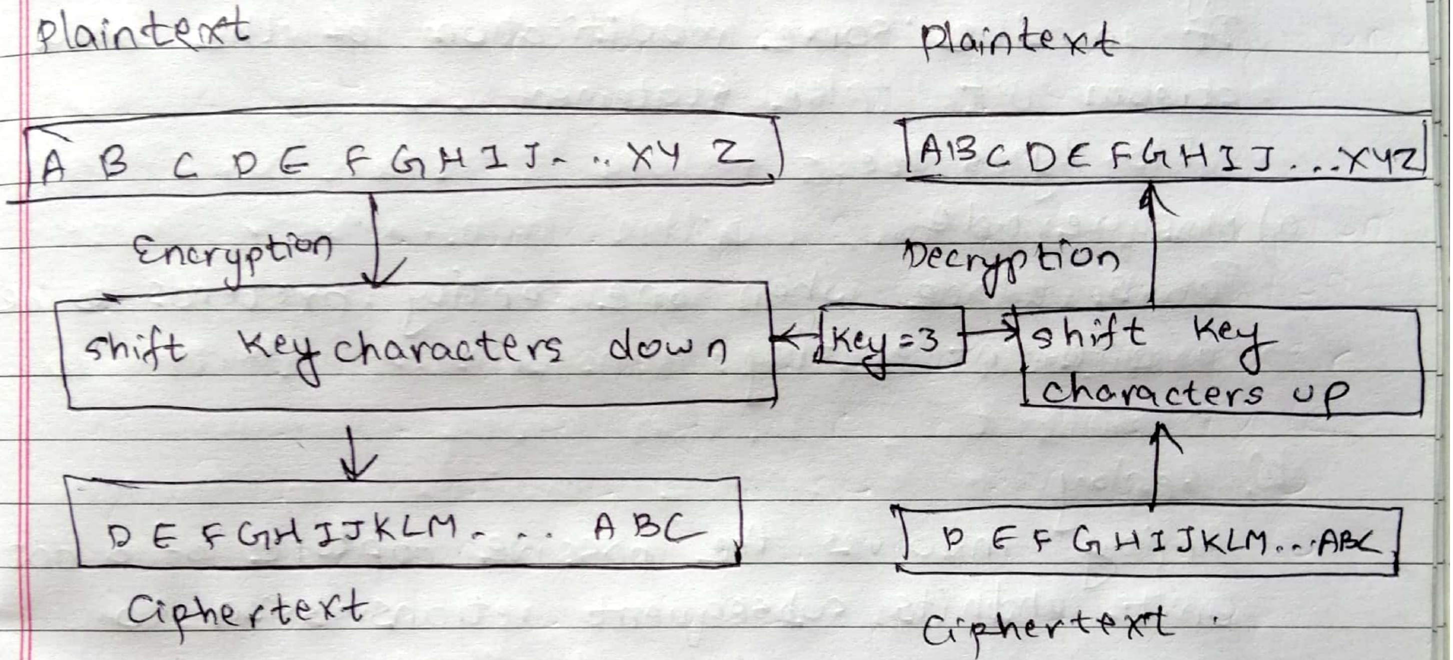
8. How authentication is an essential mechanism for maintaining security. Explain.

Ans:- Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides ~~technology~~ access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. The most widely used form of authentication is to require the user to type a login name and password. Password is easy to understand and implement. The second method for authenticating users is to check for some physical object they have rather than something they know. The third authentication method measures physical characteristics of the user that are hard to forge. These are called biometrics.

Authentication is important because it enables organizations to keep their networks secure by permitting only autheticated users to access its protected areas.

9a) Caesar Cipher

The caesar cipher is one of the earliest known and simplest cipherest. It is a type of substitution cipher in which each letter in 'plaintext' is shifted a certain number of places down the alphabet


Plaintext
A B C D E F G H I J ... X Y Z
Encryption
shift key characters down
D E F G H I J K L M ... A B C
Ciphertext
Plaintext
A B C D E F G H I J ... X Y Z
Decryption
Key = 3
shift key characters up
D E F G H I J K L M ... A B C
Ciphertext

Encryption

$C = (p+K) \bmod 26$

p = plaintext

C = ciphertext

K = shift

Decryption

$p = (C-K) \bmod 26$

2073 Bhadra

8ii) Types of security attack

1) Active attack

An active attacks attempts to alter system resources or effect their operations. It involve some modification of the data stream of false statement

Its types are:-

a) Masquerade

Takes place when one entity pretends to be a different enitity.

b). Replay

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

3. Modification of meassage

means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

4. Man in the middle attack

an attacker sits in the data flow of a communication, masquerading as the sender to the receiver, and vice versa.

5. Denial of service (DOS)

This violation involves preventing legitimate use of the system. Disable network or overload it with messages.

2. Passive attack.
a) obtaining message content
b) Traffic analysis

2073 Magh

8 i) Protection Domain

→ A computer system contains many "objects" that need to be protected.

→ These objects can be hardware (eg. CPUs, memory segments, disk drives or printers) or they can be software (eg, processes, files, databases or semaphores)

→ Each object has a unique name by which it is referenced and a finite set of operations that processes are allowed to carry out on it.

→ a way is needed to prohibit processes from accessing objects that they are not authorized to access.

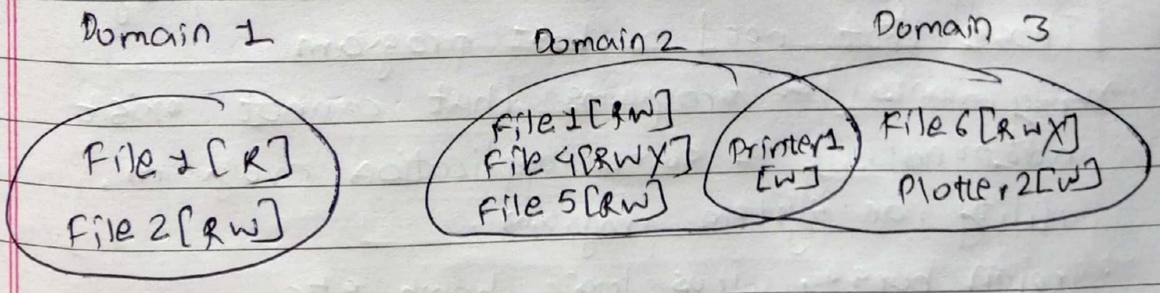


Fig: Three protection domains.

ii) Cryptography

→ It is the science and art of transforming message to make them secure and immune to attack

→ The purpose of cryptography is to take a message or file, called the plaintext, and encrypt it into ciphertext in such a way that only authorized people know how to convert it back to plaintext.

→ Original message before transformation => Plaintext

→ An encryption algorithm transforms => Plaintext to ciphertext

→ Decryption algorithm transforms => Ciphertext to Plaintext.

2072 Magh.

8. The use of internet is possible cause of a security breach. Describe the major threats by which a system connected to the internet is always prone to attack. Explain.

Ans.- The major threats # ~~connected~~ are:-

Category 1: Based on need of Host program.

Those that need a host program

→ Fragments of programs that cannot exist independently of some application program, utility, or system program

→ Trojan horse, virus, logic bomb, etc

Independent

→ Self contained programs that can be scheduled

and run by the operating system
→ Zombie, worms, etc.

Category 2: Based on replicative behavior
Replicative
→ Virus, worm, Zombies

Non-replicative
→ Trap droors, Trojan horse

2071 Magh

8c) Security Policy.

Security policy is a definition of what it means to be secure for a system, organization or other antity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

If it is important to be secure, then it is important to be sure all of the policy is enforced by mechanisms that are strong enough.

2070 Bhadra.

8. Explain the ACL. How its mechanisms are implemented for security?

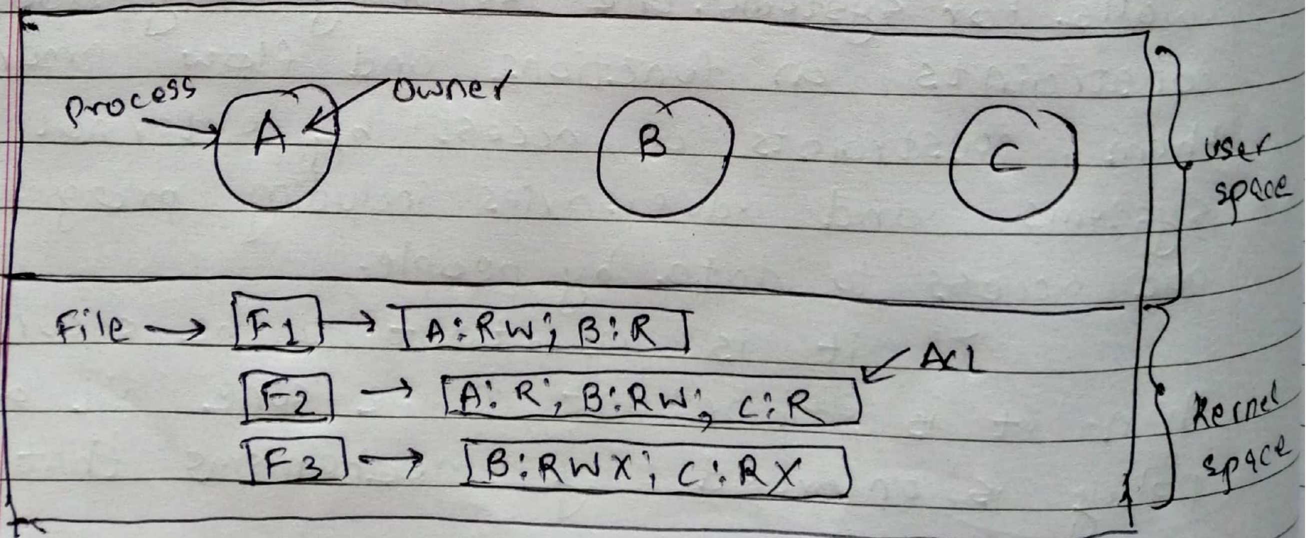
Ans:→ In practice, actually storing the matrix of slide 34 is rarely done because it is large and sparse

→ Most domain have no access at all to most objects, so storing a very large, mostly empty, matrix is a waste. of disk space.

→ More practical approach would be to store the matrix by row or column and then storing only the non empty elements.

→ The first technique consists of associating with each object an (ordered) list containing all the domains that may access the object, and how.

→ The list is called ACL.



2070 Magh

9a) Information security Model.

In formation security modes are models used to ~~aunt~~ authenticate security policies as they are intended to provide a precise set of rules that a computer can follow to implement the fundamental security concepts, processess and procedures contained in a security policy. These models can be abstract or intuitive.

Some of the information security Models are,

1) State Machine Model
2) Bell-La Padula Model
3) Biba Model
4) Clark-Wilson Model
5) Non interference Model, etc