UNIT – 7

Security

Outline….

- Introduction
- Discretionary Access control
- Mandatory Access control
- Date Encryption

Introduction

- Managing computer and network security program has become an increasingly difficult and challenging job.
- The information security manager must establish and maintain a security program that ensures three requirements:
- **Confidentiality**
- **Integrity**
- **Availability**

Confidentiality

- **Confidentiality** is the protection of information in the system so that unauthorized persons cannot access it.

Threats of Confidentiality

- **Hacker**
- **Masqueraders**
- **Unauthorized user activity**
- **Unprotected download files**
- **Local Area Network**
- **Trojan Horses**

Integrity

- **Integrity** involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle .

Availability

- **Availability** means that information is accessible by authorized users at any period of time.

Overview of Database Security

- Database security is primary concerned with the secrecy of data. Secrecy means protection a database from unauthorized access by users and software application.
- There are three generally accepted categories of secrecy-related problems in database systems:

1. The improper release of information from reading data that was intentionally or accidentally.
2. The improper modification of data.
3. Denial-of-services threats.

Access Control

- An Access control system is a system which enable an authority to control access to areas and resources in a given computer-based information system.
- Access control system provide the essential services of identification and authentication , authorization and accountability.
- Types of Access Control Techniques:

i. Discretionary Access Control (DAC)

ii. Mandatory Access Control (MAC)

iii. Role Base Access Control (RBAC)

Discretionary Access Control (DAC)

- In computer security, DAC is a kind of access control defined by the Trusted Computer System Evolution Criteria (TCSEC).
- Under DAC, every object has an owner that controls the permission to access the object, probably because many systems to implement DAC using the concept of an owner.
- Two important concepts in DAC are:
- **File and Data owner ship:** In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
- **Access rights and permissions:** These are the controls that an owner can assign to other subjects for specific resources.

Discretionary Access Control (DAC)

- A DAC access control model often exhibits one or more of the following attributes.
- **Data owner can transfer ownership of information to other users.**
- **Data owner can determine the type of access given to other users (read, write, copy, etc.)**
- **Repetitive authorization failures to access the same resources or object generates an alarm and/or restricts the user's access.**
- **Special add-on or plug-in software required to apply an HHTP client to prevent indiscriminant copying by users.**
- **Users who do not have access to information should not be able to determine its characteristics.**
- **Access to information is determined base on authorizations to access control lists based on users identifier and group membership.**

DAC Mechanism

USERS	Objects	KIMSELF	DONS FILE	PAYROL1	PAYROL2	DOS FILE
Kim		RW	R	RW	R	
Joe			R			
Don			RW	R		
Jones				R		
Doe						RW
Mgr Jim		CP	CP	CP	C	C
Jan				RW	RW	

DAC Access Model

- **The various read, write, execute and delete access modes are given below.**
- READ
- WRITE-APPEND or WRITE-EXPAND
- WRITE-CHANGE
- WRITE-UPDATE
- WRITE
- EXECUTE
- NULL
- Control
- Control with Passing ability

Mandatory Access Control (MAC)

- **Mandatory Access Control (MAC) is an access policy determined by the system, not by owner.**
- In general MAC access control mechanisms are more secure than DAC.
- MAC mechanisms assign a security level to all information, assign a security clearance to each user and ensure that all users only have access to that data for which they have a clearance.
- The important terms related to MAC are:
- **Sensitivity labels**
- **Data import and Export**

Mandatory Access Control (MAC)

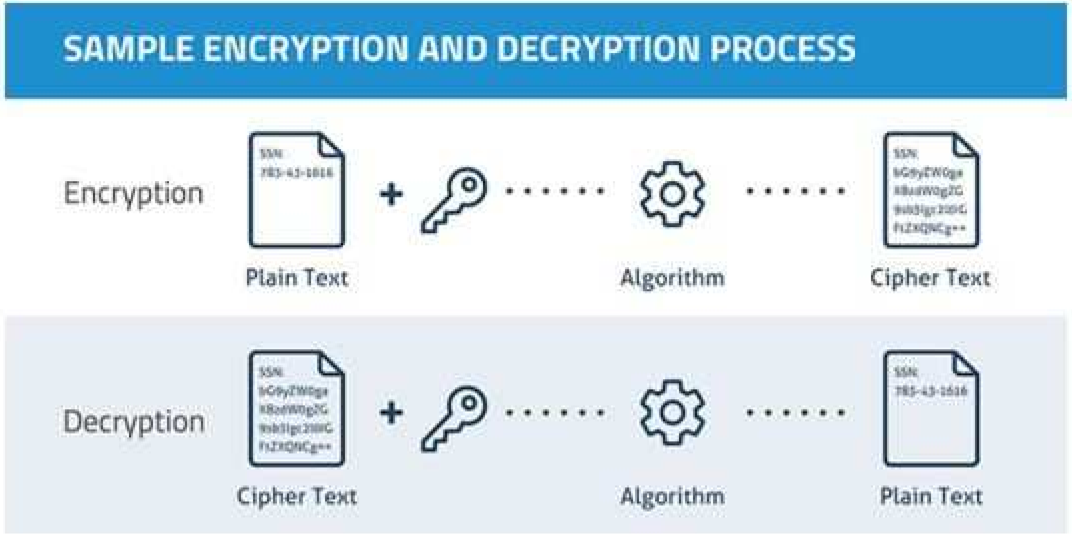
- A MAC access control model often exhibits one or more of the following attributes.
- **Only administrators, not data owners, make changes to a resources' security label.**
- **All data is assigned security level that reflects its relative sensitivity, confidentiality and protection value.**
- **All users can read from a lower classification than the one they are granted.**
- **All users can write to a higher classification.**
- **All users are given read/write access to objects only of the same classification.**
- **Access is authorized or restricted to objects based on the time of day depending on the labeling on the resource and the user's credentials.**
- **Access is authorized or restricted to objects based on the security characteristics of the HHTP client.**

Mandatory Access Control (MAC) Methods

- **Rule-based access control:** This type of control further defines specific conditions for access to requested object. All MAC –based systems implement a simple form of rule-based access control to determine whether access should be granted or denied by matching:
  - **An object's sensitivity label**
  - **A subject's sensitivity label**
- **Lattice-based access controls:** These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of element, such as a subject and an object.

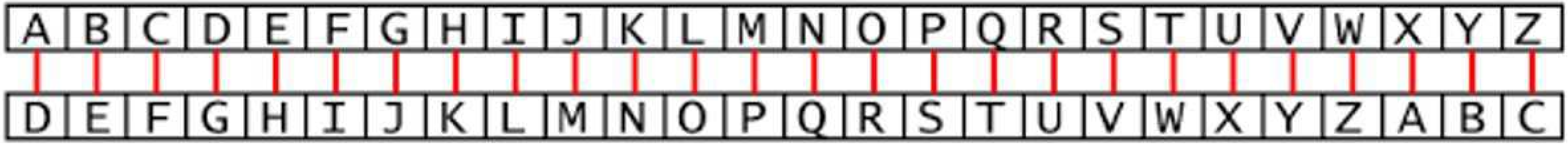
Encryption

- **Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users.**
- This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.
- This encoded data may only be decrypted or made readable with a key. **Symmetric-key** and **Asymmetric-key** are the two primary types of encryption.



Encryption Example

- **The Caesar cipher and the Encryption of the word “secret”**



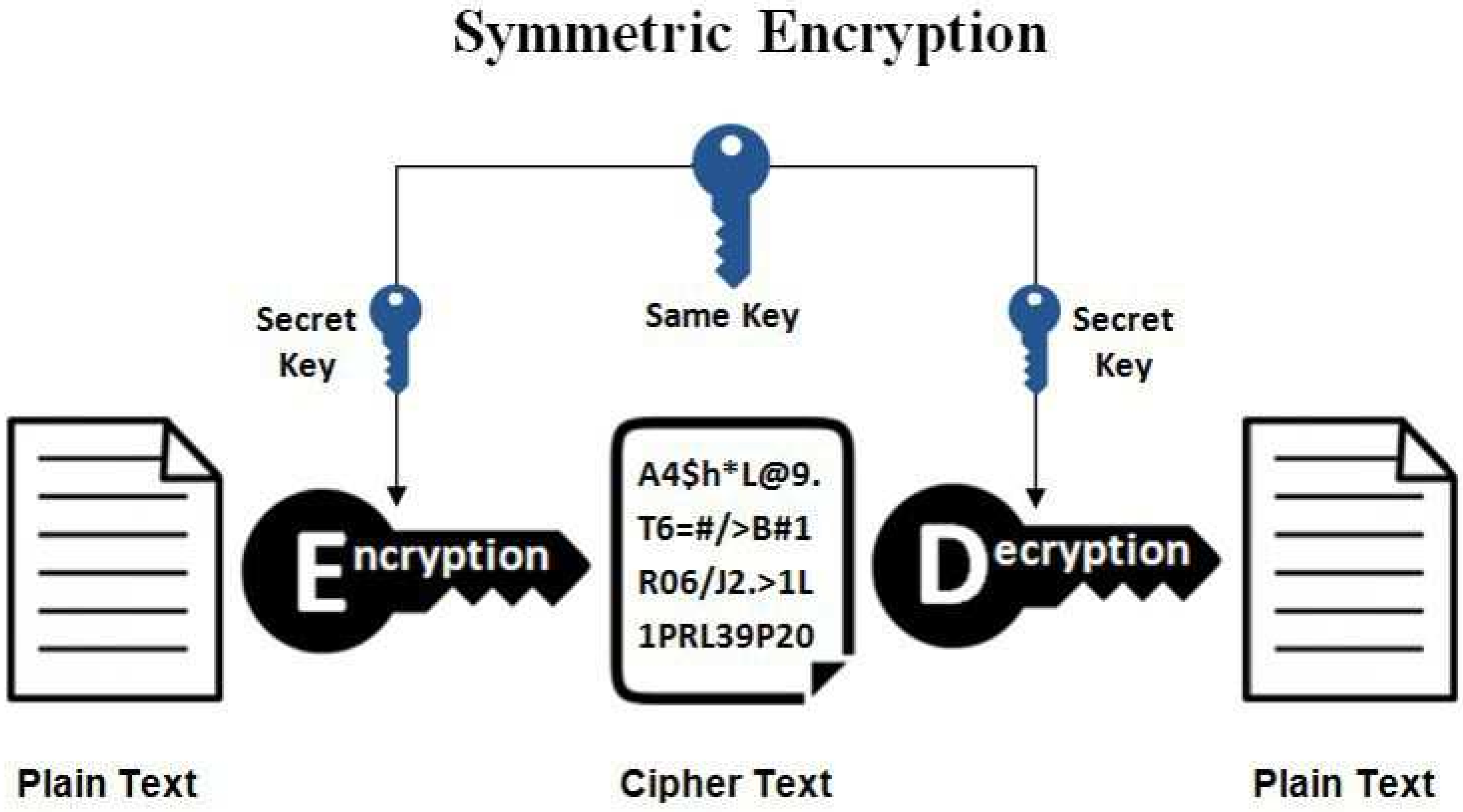
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Alphabet shifted by 3 spaces.

- **Ans: “vhfuhw”**

Keys used in Encryption

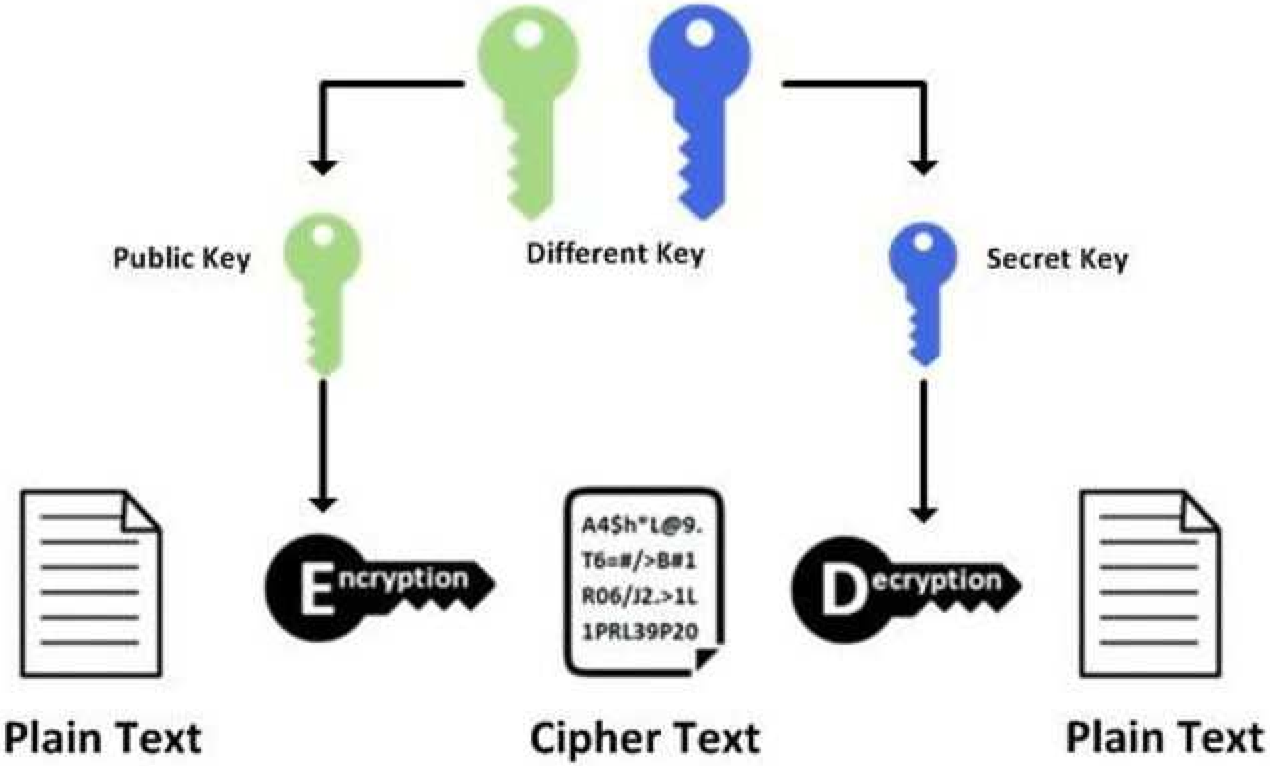
- **Symmetric algorithms**: (also called "secret key") use the same key for both encryption and decryption;



Keys used in Encryption

- **Asymmetric algorithms**: (also called "public key") use different keys for encryption and decryption.

Asymmetric Encryption



Common use of Encryption

- **Authentication**
- **Validation: Fingerprint and Digital Signature**
- **Data Protection**
- **Virtual Private Network**
- **Encryption and Viruses**