SECURITY

- ✓protection of information and property from *theft, corruption, or natural disaster* while allowing the information and property to remain accessible to its intended users
- ✓ is the protection from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or *misdirection of the services* they provide.
- ✓A system is said to be secured if the resources in the system is accessed and used as intended under all circumstances
- ✓A **vulnerability** is a weakness in a system, technology, product or policy
- ✓A **threat** is the potential for a security violation, stich as the discovery of a vulnerability
- ✓an **attack** is the attempt to break security.

SECURITY: CATEGORIES

Information Security

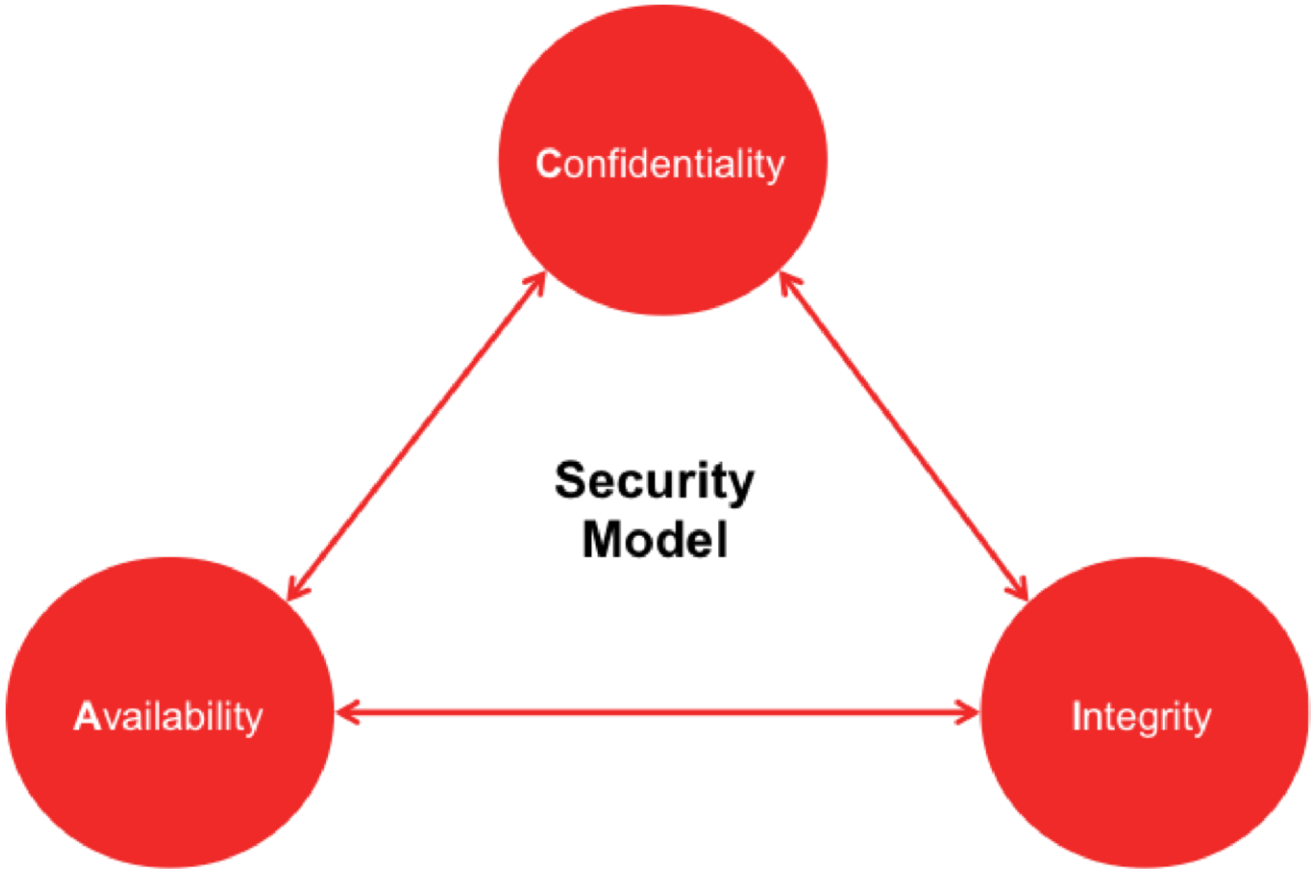
✓It is the practice of defending **information** from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

✓It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)

Network and Internet Security

✓Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

INFORMATION SECURITY GOALS : CIA TRIAD



CIA TRIAD

Confidentiality

- prevent the disclosure of sensitive information from unauthorized people, and processes Integrity

- protect the information from intentional or accidental modification

Availability

-assuring that the system and data are accessible by authorized users

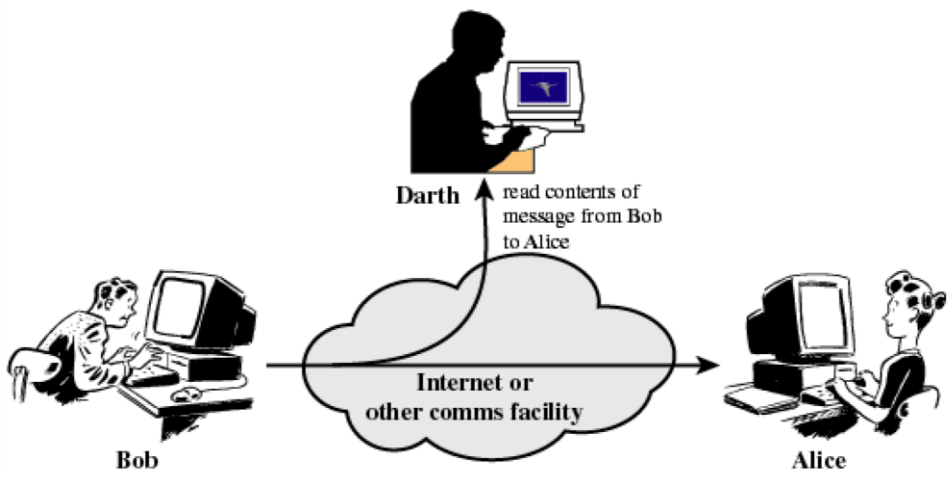
SECURITY GOALS AND THREATS

Goal	Threat
Data confidentiality	Exposure of data
Data integrity	Tampering with data
System availability	Denial of service
Exclusion of outsiders	System takeover by viruses

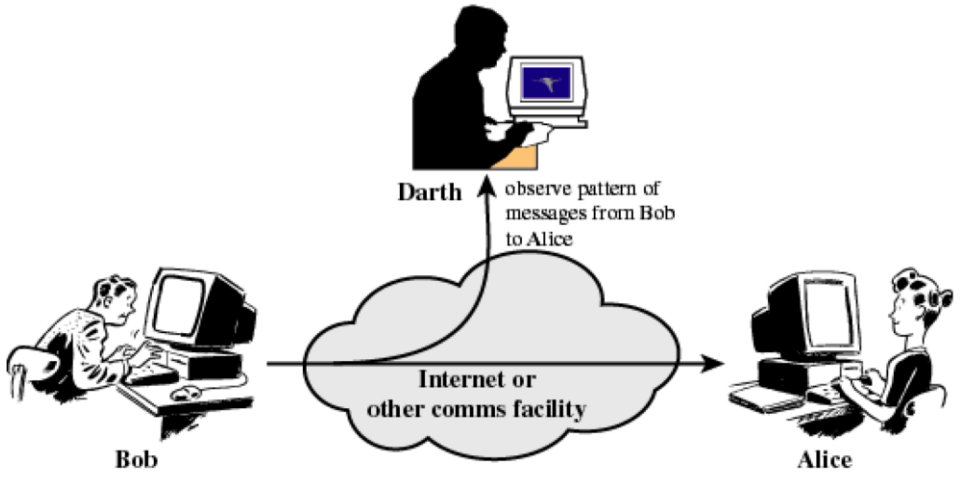
TYPES OF ATTACKS

Passive Attack

1. Obtaining Message Content
2. Traffic Analysis



(a) Release of message contents



(b) Traffic analysis

TYPES OF ATTACKS

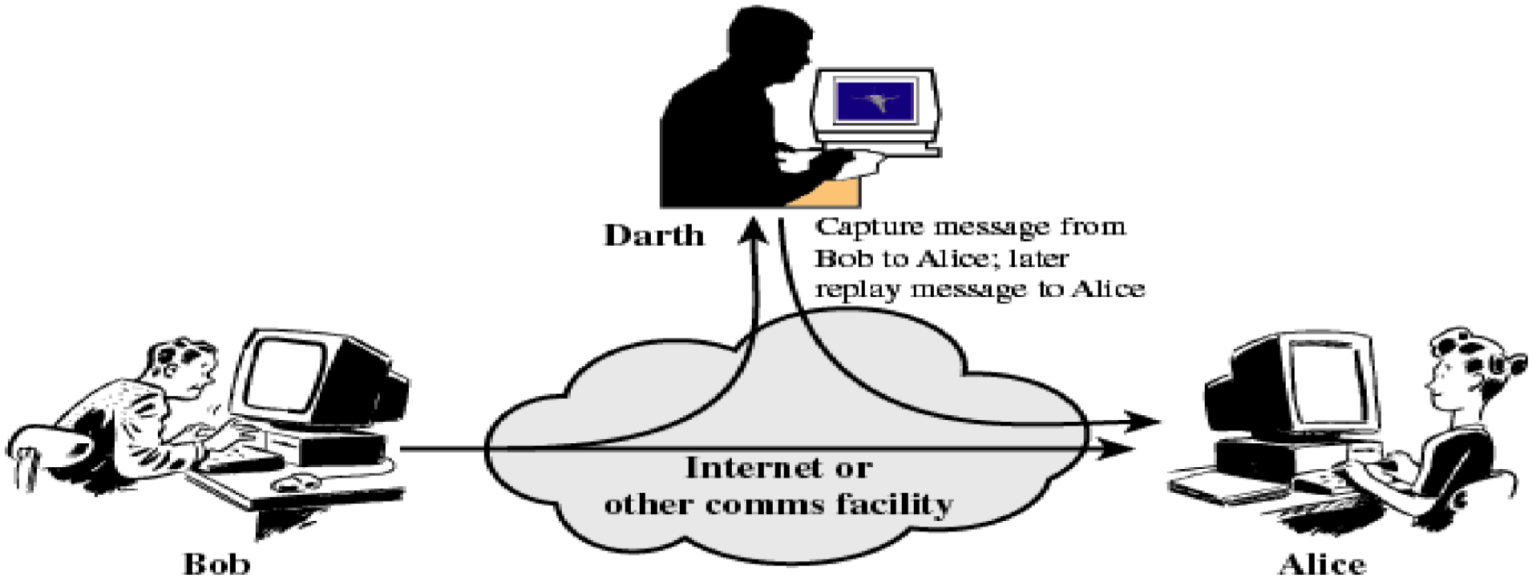
Active Attacks

1. Masquerade : takes place when one entity pretends to be a different entity

(a) Masquerade

TYPES OF ATTACKS

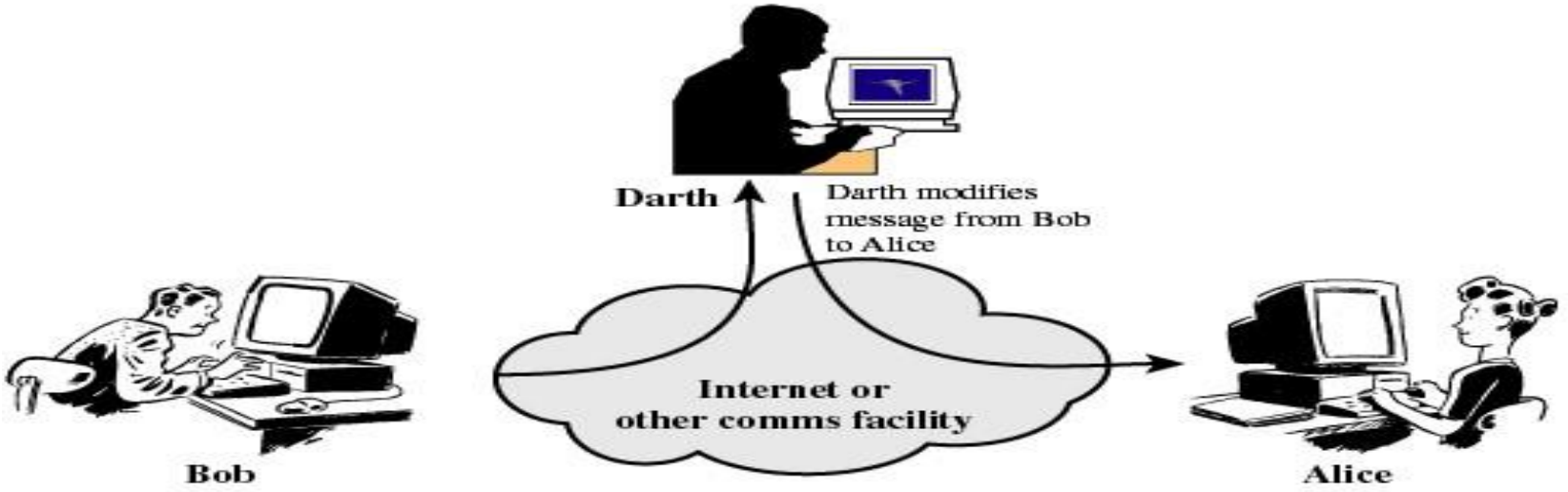
2. **Replay:** Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



(b) Replay

TYPES OF ATTACKS

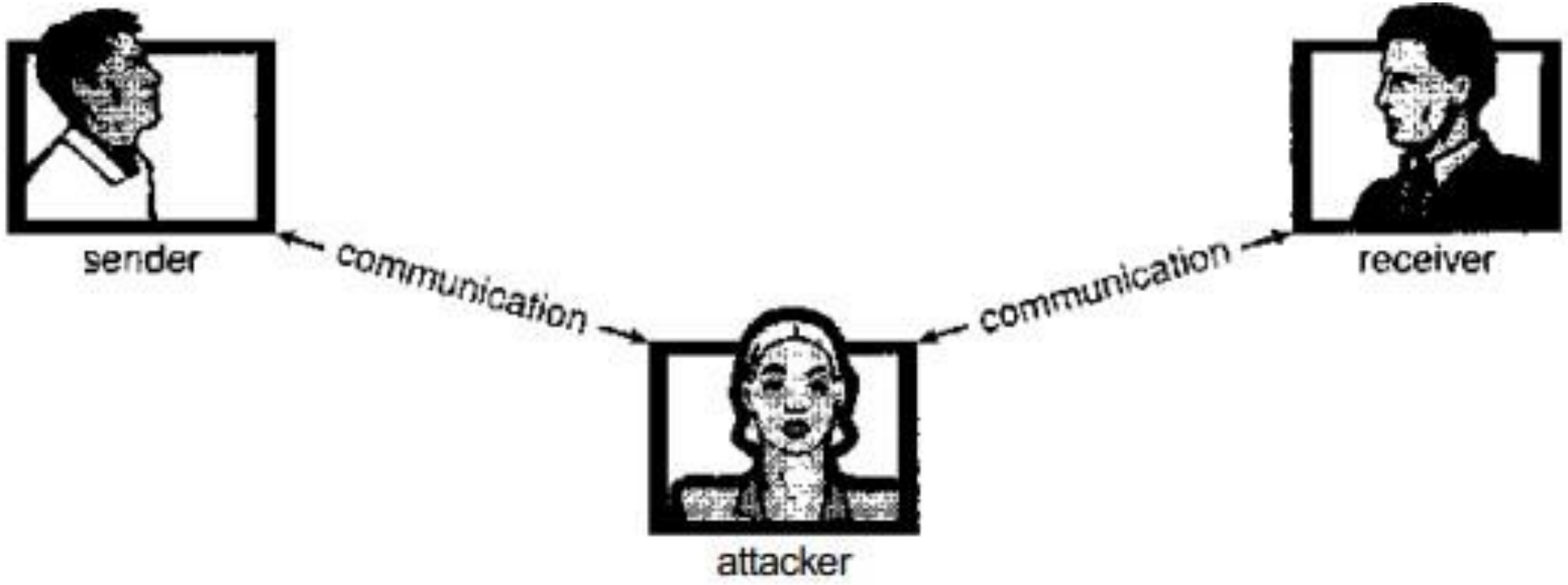
3. **Modification of messages :** means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect



(c) Modification of messages

TYPES OF ATTACKS

2. 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.



TYPES OF ATTACKS

4. Denial of service (DOS) : This violation involves preventing legitimate use of the system. Disable network or overload it with messages

(d) Denial of service

HOW TO ACHIEVE CIA GOALS?

Confidentiality

✓**Authentication**

-User IDs and passwords

-Using a physical object

-biometric verification

✓Two-factor authentication

✓Challenge response authentication

✓Data encryption

HOW TO ACHIEVE CIA GOALS?

Integrity

✓file permissions and user access controls

✓**Version control** maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem

✓ checksums

HOW TO ACHIEVE CIA GOALS?

Availability

- ✓maintaining all hardware
- ✓Do necessary system upgrades periodically
- ✓Providing adequate communication bandwidth and preventing the occurrence of bottlenecks
- ✓Redundancy

THREATS: MALICIOUS PROGRAMS

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.

THREATS: MALICIOUS PROGRAMS

Category 2 : Based on replicative behavior

Replicative

✓Virus, Worm, Zombies

Non-replicative

✓Trap doors, Trojan horse

INSIDER ATTACKS

✓These are executed by programmers or other employees of the company

✓They include:

1. Logic Bombs
2. Trap Doors
3. Login Spoofing

INSIDER ATTACKS

Logic Bombs/time bombs

- ✓is a piece of code written by one of a company's (currently employed) programmers and secretly inserted into the production system.
- ✓As long as the programmer feeds it its daily password, it does nothing. However, if the programmer is suddenly fired and physically removed from the premises without warning, the next day (or next week) the logic bomb does not get fed its daily password, so it goes off.
- ✓Going off might involve clearing the disk, erasing files at random, carefully making hard-to-detect changes to key programs, or encrypting essential files.

INSIDER ATTACKS

Trap Doors

- ✓**c**ode inserted into the system by a system programmer to bypass some normal check.
- ✓For example, a programmer could add code to the login program to allow anyone to log in using the login name "zzzzz" no matter what was in the password file.
- ✓If this trap door code were inserted by a programmer working for a computer manufacturer and then shipped with its computers, the programmer could log into any computer made by his company, no matter who owned it or what was in the password file.

INSIDER ATTACKS

Trap Doors

```
while (TRUE) {
        printfflogin:");
        geLstring(name);
        disable_echoing();
        printf("password: ");
        get_string(password);
        enable_echoing();
        v = check_validity(name, password);
        if (v) break;
}
execute_shell(name);
```

(a)

```
while (TRUE) {
        printf("login: °);
        geCstring(name);
        disable_echoing();
        printffpassword:");
        get_string(password);
        enable_echoing();
        v » check_validity(name, password);
        if (v || strcmpfname, 'zzzzz') == 0) break;
}
execute_shell(name);
```

(b)

Figure 9-22. (a) Normal code, (b) Code with a trap door inserted.

INSIDER ATTACKS

Login Spoofing

✓**Involves creating a fake login screen that looks exactly like the real login screen to collect passwords**

Figure 9-23. (a) Correct login screen, (b) Phony login screen.

EXPLOITING CODE BUGS

1. Buffer Overflow Attacks
2. Format String Attacks
3. Return to libc Attacks
4. Inter Overflow Attacks
5. Code Injection Attacks
6. Privilege Escalation Attacks

MALWARE

- ✓malicious software (intends to do harm)
- ✓They are designed and spread as quickly as possible over the Internet and infect as many machines as it can
- ✓A backdoor is also installed on the machine that allows the criminals who sent out the malware to easily command the machine to do what it is instructed to do
- ✓A machine taken over in this fashion is called a ***zombie***, and a collection of them is called a **botnet**, a contraction of "robot network“
- ✓Another common application of malware has it install a ***keylogger*** on the infected machine.
- ✓Malware are used for commercial or even criminal purposes

SOME COMMON MALWARES

Trojan Horse

- ✓A Computer program that appears to have a useful function, but also has a hidden and potentially malicious function
- ✓These software with Trojans inside are usually free and attractive which causes the software to be downloaded voluntarily
- ✓When the free program is started, it calls a function that writes the malware to disk as an executable program and starts it.
- ✓The malware can then do whatever damage it was designed for, such as deleting, modifying, or encrypting files.
- ✓It can also search for credit card numbers, passwords, and other useful data and send them back to the author of Trojan horse over the Internet.
- ✓More likely, it attaches itself to some IP port and waits there for directions, making the machine a zombie, ready to send spam or do whatever its remote master wishes.

SOME COMMON MALWARES

Viruses

- ✓a virus is a program that can reproduce itself by attaching its code to another program
- ✓A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels.
- ✓Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program.

SOME COMMON MALWARE

Worms

- ✓A worm is similar to a virus by design and is considered to be a sub-class of a virus.
- ✓Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.
- ✓A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.
- ✓One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book

SOME COMMON MALWARE

Spywares

- ✓spyware is software that is loaded onto a PC without the owner's knowledge and runs in the background doing things behind the owner's back.
- ✓First, it hides, so the victim cannot find it easily.
- ✓Second, it collects data about the user (Websites visited, passwords, even credit card numbers).
- ✓Third, it communicates the collected information back to its distant master.
- ✓ And fourth, it tries to survive determined attempts to remove it

SOME COMMON MALWARE

Spywares

✓Barwinsky et al. divided the spyware into three broad categories.

✓The first is ***marketing:*** the spyware simply collects information and sends it back to the master, usually to better target advertising to specific machines.

✓The second category is ***surveillance,*** where companies intentionally put spyware on employee machines to keep track of what they are doing and which Websites they are visiting.

✓The third gets close to classical malware, where the infected machine becomes part of ***a zombie army*** waiting for its master to give it marching orders.

PROTECTION MECHANISM

1 . Protection Domains

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

✓These objects can be hardware (e.g., CPUs, memory segments, disk drives, or printers), or they can be software (e.g., 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.

PROTECTION MECHANISM : PROTECTION DOMAIN

- ✓A domain is a set of (object, rights) pairs.
- ✓Each pair specifies an object and some subset of the operations that can be performed on it.
- ✓A right in this context means permission to perform one of the operations.
- ✓ Often a domain corresponds to a single user, telling what the user can do and not do or it could mean a group of user
- ✓At every instant of time, each process runs in some protection domain.
- ✓In other words, there is some collection of objects it can access, and for each object it has some set of rights.

PROTECTION MECHANISM : PROTECTION DOMAIN

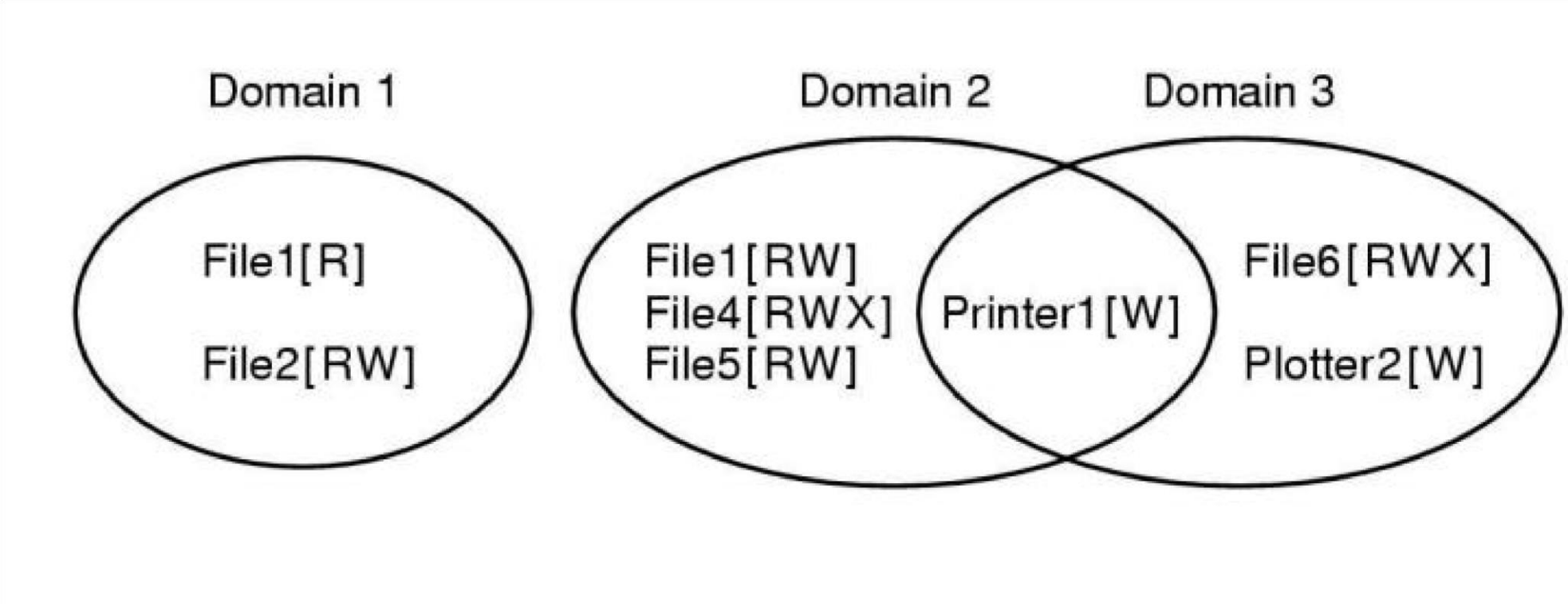


Fig: Three protection domains

PROTECTION MECHANISMS : MATRIX

✓OS keeps tracks of which object belongs to which domain using a protection matrix

	Object							
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
Domain 1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

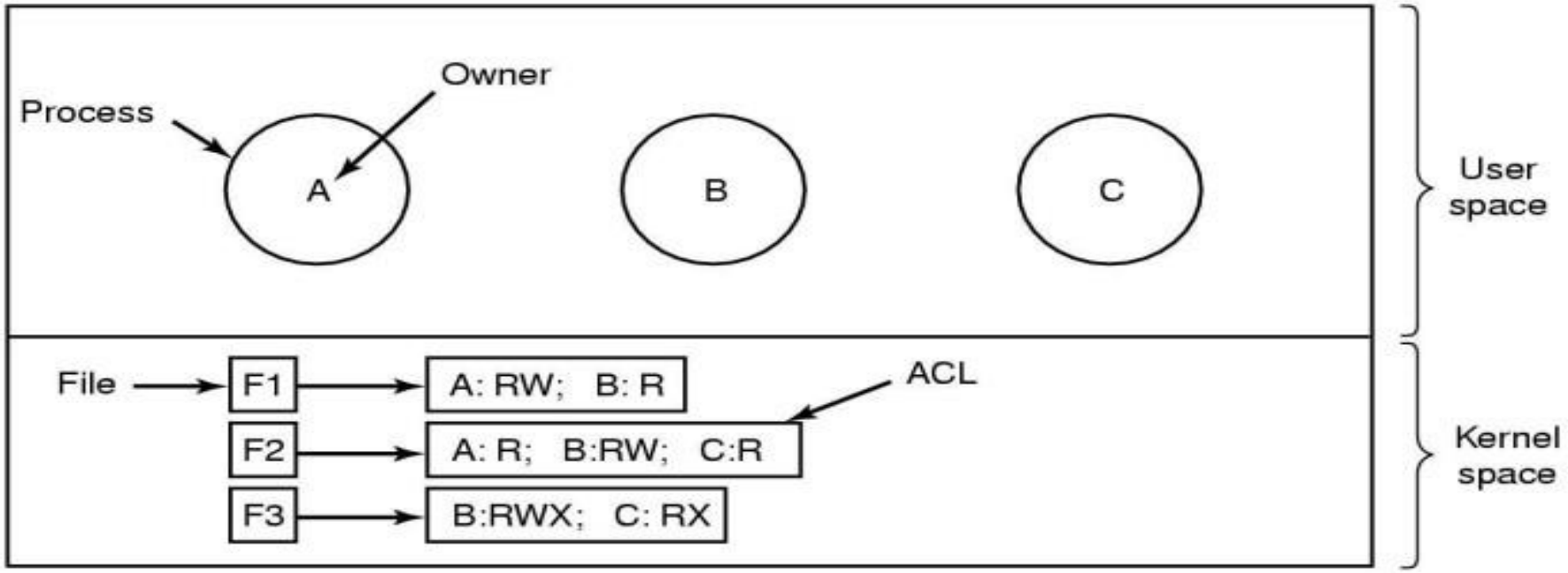
PROTECTION MECHANISM

2 . Access Control List (ACL)

- ✓In practice, actually storing the matrix of slide 34 is rarely done because it is large and sparse.
- ✓Most domains 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.
- ✓This list is called the Access Control List (ACL)

PROTECTION MECHANISM : ACL

✓An access list for a specific object is a list that contains all non-empty cells of a column of access matrix associated with a given object.

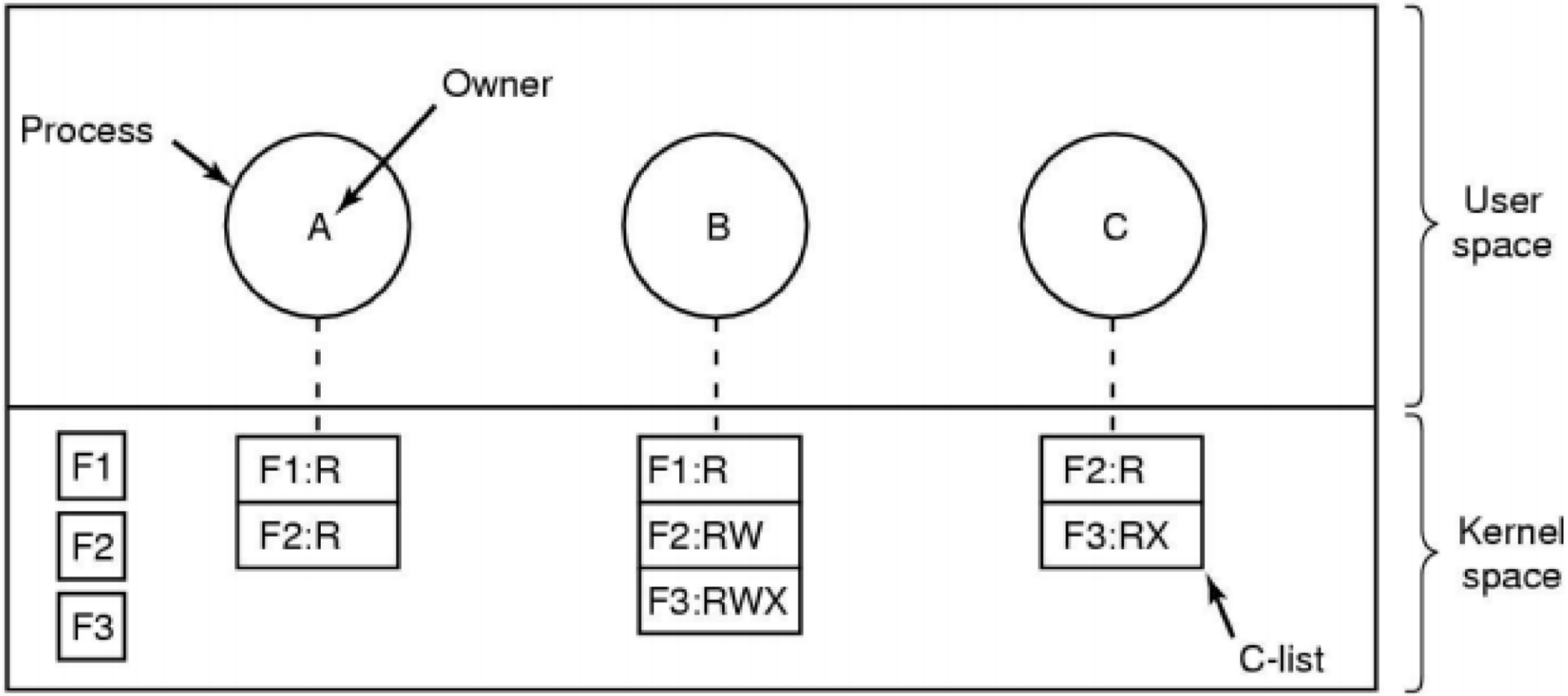


PROTECTION MECHANISM

3. Capabilities List (C-List)

- ✓Instead of storing and maintaining access lists per object, the system can also maintain access rights list per subject/principals/users.
- ✓With this method, associated with each process is a list of objects that may be accessed, along with an indication of which operations are permitted on each

PROTECTION MECHANISM : C LIST



PROTECTION MECHANISM : C-LIST

- ✓In addition to the specific object-dependent rights, such as read and execute, capabilities usually have ***generic rights*** which are applicable to all objects

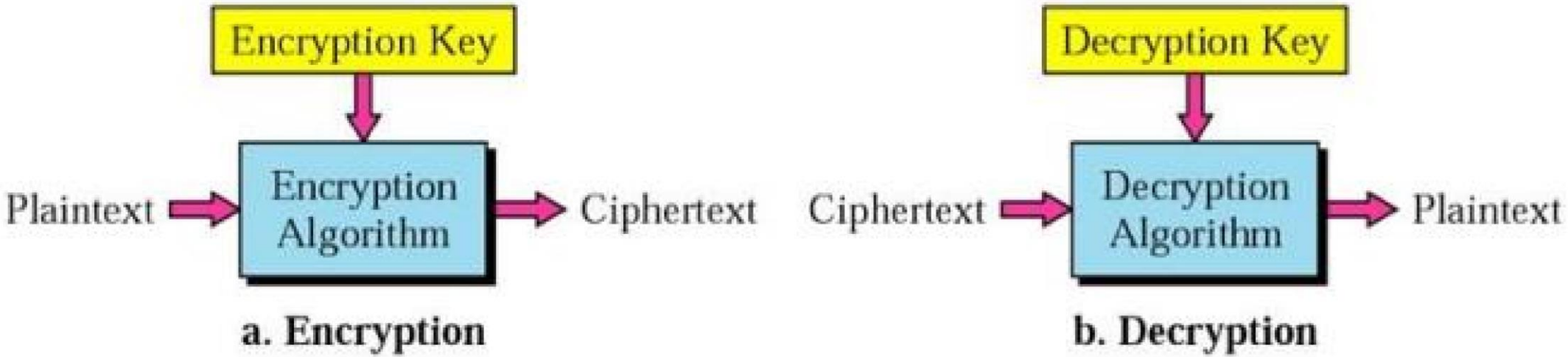
- ✓**Copy capability:** create a new capability for the same object.
- ✓**Copy object:** create a duplicate object with a new capability.
- ✓**Remove capability:** delete an entry from the C-list; object unaffected.
- ✓**Destroy object:** permanently remove an object and a capability

CRYPTOGRAPHY

- ✓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

CRYPTOGRAPHY

CRYPTOGRAPHY : ENCRYPTION AND DECRYPTION SECRET KEY



ENCRYPTION

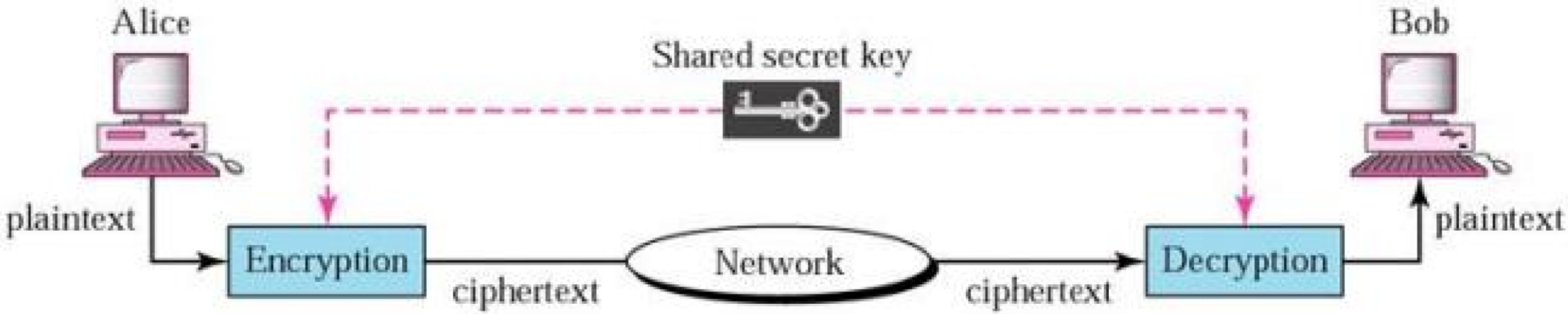
- ✓Secret key encryption uses a single key to both encrypt and decrypt messages
- ✓It is also called symmetric key encryption
- ✓The same key must be shared between all the parties in the communication.
- ✓The key must be kept secret by all parties involved in the communication. If the key fell into the hands of an attacker, they would then be able to intercept and decrypt messages

Mathematically

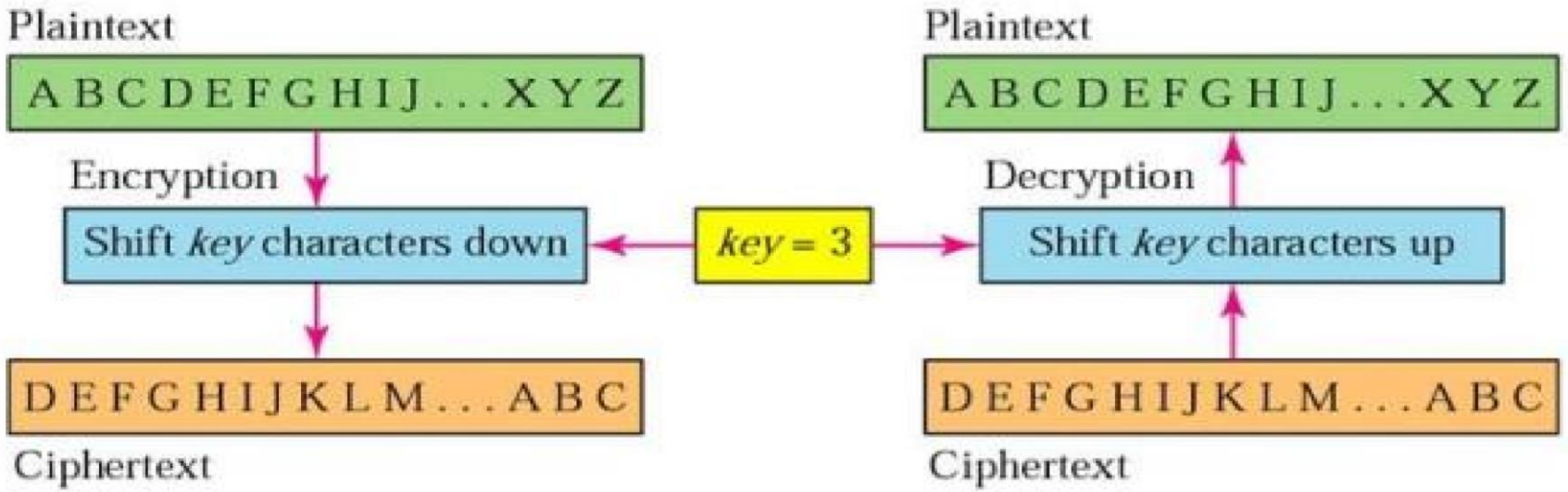
$Y=E_K(X)$ [EncryptionModel]

$X=D_K(Y)$[DecryptionModel]

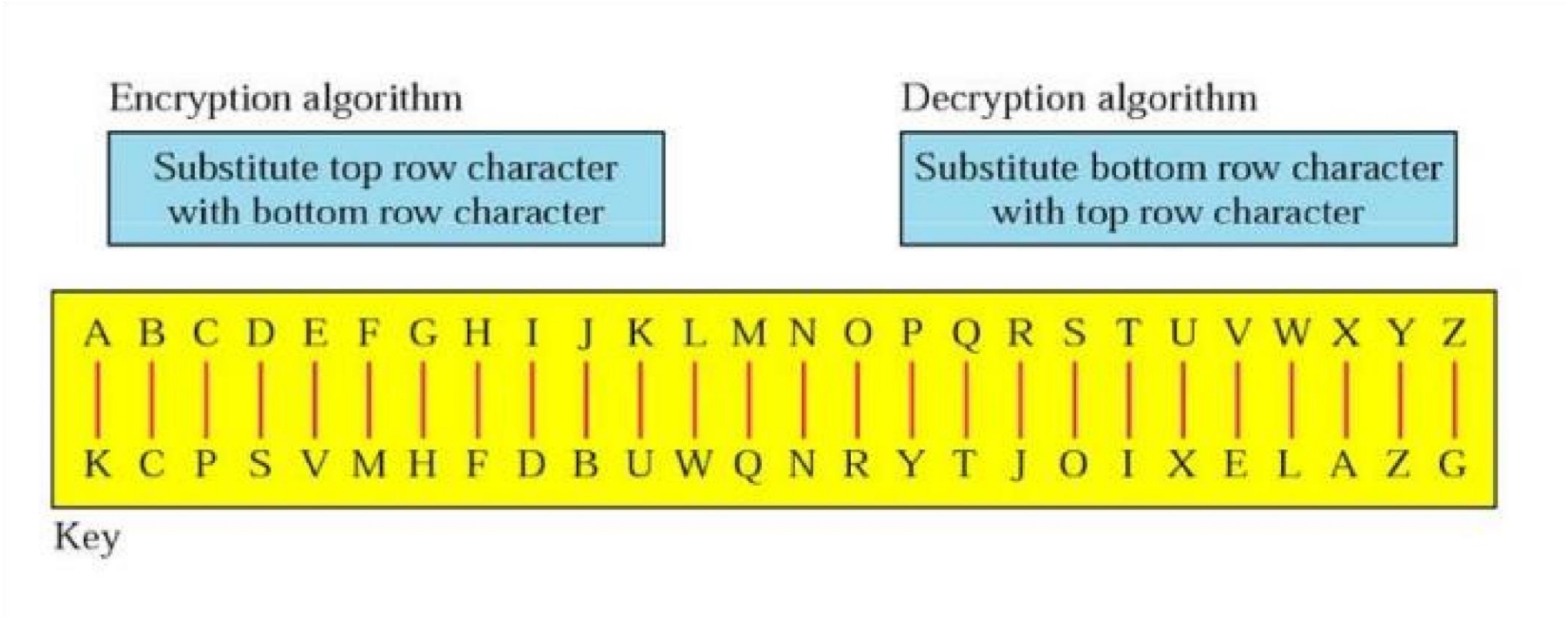
SECRET-KEY ENCRYPTION SECRET



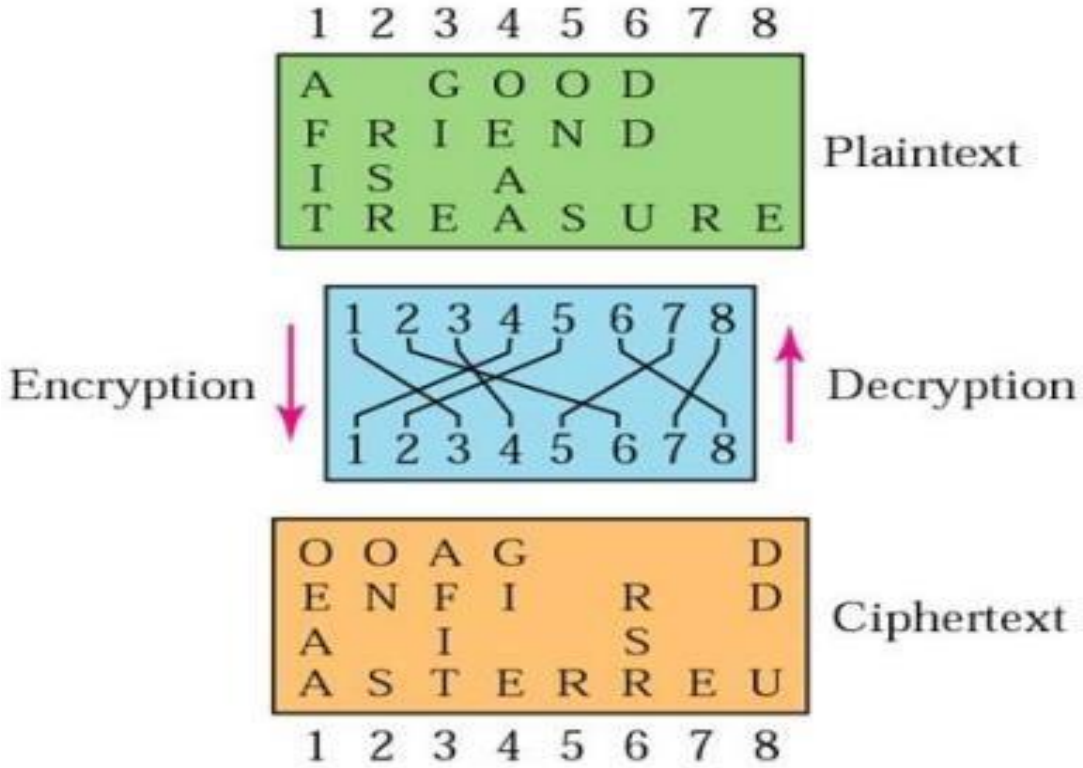
KEY ENCRYPTION : CAESAR CYPHER



SECRET KEY ENCRYPTION : MONOALPHABETIC SUBSTITUTION

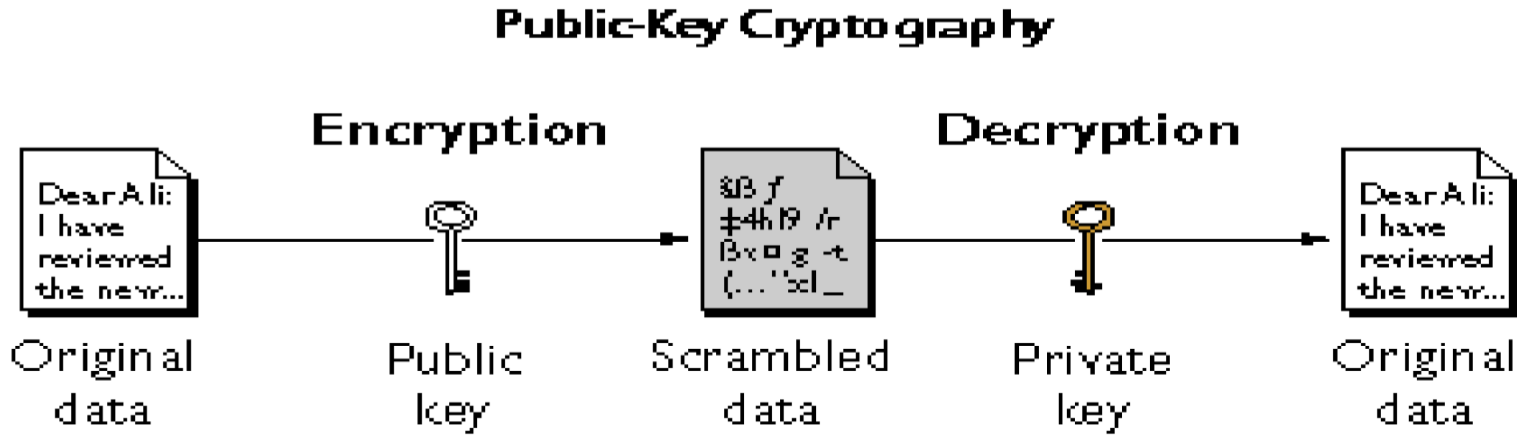


SYMMETRIC KEY ENCRYPTION : TRANSPOSITION CYPHER

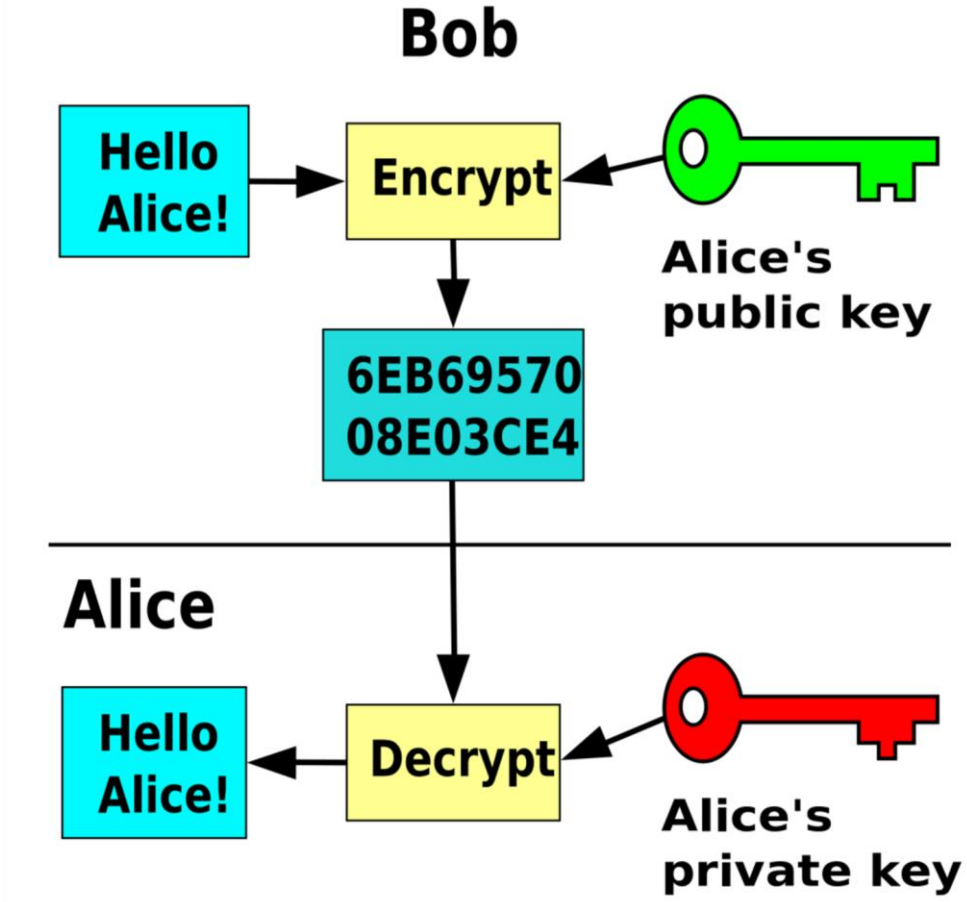


PUBLIC KEY ENCRYPTION

- ✓distinct keys are used for encryption and decryption
- ✓The public key can be shared with everyone, whereas the private key must be kept secret.
- ✓The message is encrypted using a public key to get the cipher text that can only be decrypted by private key or vice versa



PUBLIC KEY CRYPTOGRAPHY



DIGITAL SIGNATURE

- ✓Digital signatures make it possible to sign e-mails and other digital documents in such a way that they cannot be repudiated by the sender later.
- ✓One common way is to first run the document through a one-way cryptographic hashing algorithm that is very hard to invert.
- ✓The most popular hashing functions used are **MD5 (Message Digest 5),** which produces a 16-byte result and **SHA-1 (Secure Hash Algorithm),** which produces a 20-byte result. Newer versions of SHA-1 are **SHA-256** and **SHA-512,** which produce 32-byte and 64-byte results, respectively
- ✓The document owner then applies his private key to the hash
- ✓This value, called the signature block, is appended to the document and sent to the receiver

DIGITAL SIGNATURE

- ✓When the document and hash arrive, the receiver first computes the hash of the document using MD5 or SHA, as agreed upon in advance.
- ✓The receiver then applies the sender's public key to the signature block
- ✓If the computed hash does not match the hash from the signature block, the document, the signature block, or both have been tampered with