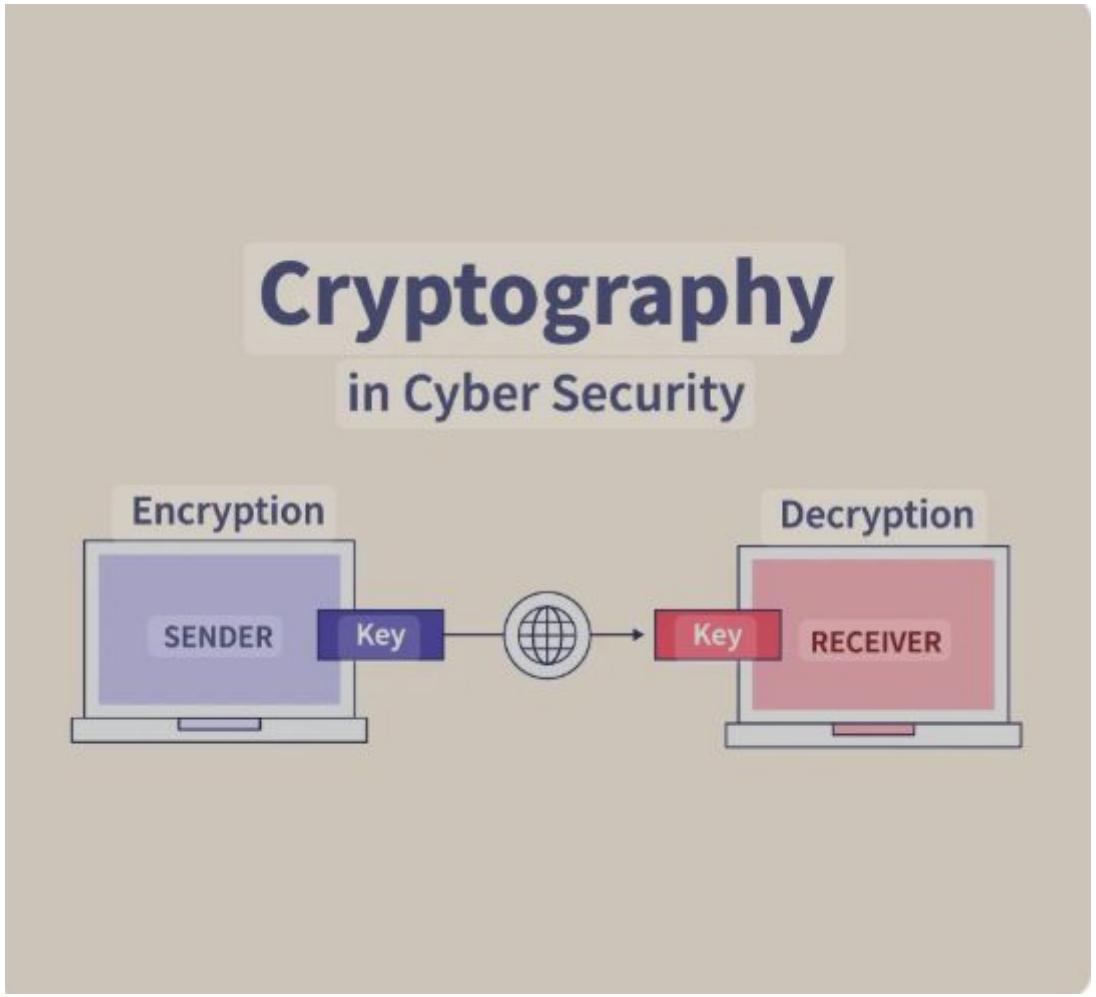
Cryptography and Network Security—CY53
William Stallings 6th Edition

Shubha Malige
Asst.Professor
CSE(Cyber Security)

What is Cryptography?



Course Objectives:

- To discuss various paradigms and principles of modern cryptography.
- Focus will be on the formal security definitions and constructions of various cryptographic primitives.

  - Encryption and Decryption, Message authentication codes, Hash Functions, Digital Signatures etc.

Course Contents

Unit I

Overview: Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security. **Classical Encryption Techniques**: Symmetric Cipher Model: Cryptography, Cryptanalysis and BruteForce Attack, Substitution Techniques: Caesar Cipher, Mono-alphabetic Cipher, Playfair Cipher, Poly alphabetic Cipher..

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit II

Block Ciphers and the data encryption standard: Stream Ciphers and Block Ciphers, the Feistel Cipher, DES encryption, DES decryption. A DES example: Results, The Avalanche effect, The Strength of DES: The Use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block Cipher Design Principles: Number of rounds, Design of function F, Key schedule Algorithm. **Advanced Encryption Standard**: AES structure, AES Transformation Functions, AES Key Expansion.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Unit III

Public-Key Cryptography and RSA: Principles of public-key cryptosystems: Public-key cryptosystems. Applications for public-key cryptosystems, Requirements for public-key cryptosystems. Public-key cryptanalysis. **The RSA algorithm**: Description of the algorithm, computational aspects, the security of RSA. **Other Public Key Cryptosystems**: Diffie Hellman Exchange: The Algorithm, Key Exchange Protocols, Man in the middle attack.

- Pedagogy: Chalk and Talk, PowerPoint Presentations, Active Learning

Unit IV

Key Management and Distribution: Distribution of Public Keys: Public Announcements of Public Keys, Public Available Directory, Public Key Authority, Public Key Certificates, X-509 certificates. Certificates, X-509 version 3, Kerberos, Kerberos version 4. **Web Security Considerations**: Web Security Threats, Web Traffic Security Approaches.

- Pedagogy: Chalk and Talk, PowerPoint Presentations.

Unit V

Secure Sockets Layer: SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and shake Protocol, Cryptographic Computations. **Transport Layer Security**: Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify and Finished Messages, Cryptographic Computations, and Padding. HTTPS Connection Initiation, Connection Closure. Secure Shell(SSH) Transport Layer Protocol, User Authentication Protocol, Connection Protocol. **Electronic Mail Security:** Pretty Good privacy, S/MIME.

- Pedagogy: Chalk and Talk, PowerPoint Presentations

Applications of Cryptography

Computer Security Concepts

A Definition of Computer Security

The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as follows:

> **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Computer Security Concepts

Key Objectives

- **Confidentiality:** This covers two related concepts
  - **Data Confidentiality:-** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - **Privacy:-** Assures that individual's control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- **Integrity**: This term covers two related concepts.
  - **Data integrity**: Assures that information and programs are changed only in a specified and authorized manner.
  - **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- **Availability**: Assures that systems work promptly and service is not denied to authorized users.

CIA Triad

Computer Security Concepts

Key Objectives: According to FIPS(Federal Information and Processing Standards) FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

• **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

• **Integrity**: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

• **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Computer Security Concepts

Additional Security Objectives

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Examples with respect to Security Key Objectives and also impact on organizations or individuals in case of security breach.

Three levels of impact on organizations or individuals:

Low Level: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might

(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

(ii) result in minor damage to organizational assets;
(iii) result in minor financial loss; or
(iv) result in minor harm to individuals.

Examples with respect to Security Key Objectives and also impact on organizations or individuals in case of security breach.

Three levels of impact on organizations or individuals:

Medium Level: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

A serious adverse effect means that, for example, the loss might

(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

(ii) result in significant damage to organizational assets;

(iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

Examples with respect to Security Key Objectives and also impact on organizations or individuals in case of security breach.

Three levels of impact on organizations or individuals:

High Level: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss might

(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
(ii) result in major damage to organizational assets;
(iii) result in major financial loss;
(iv) result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

Examples with respect to Security Key Objectives and also impact on organizations or individuals in case of security breach.

Confidentiality:

Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA). Grade information should only be available to students, their parents, and employees that require the information to do their job.

Student enrollment information may have a moderate confidentiality rating. While still covered by FERPA, this information is seen by more people on a daily basis, is less likely to be targeted than grade information, and results in less damage if disclosed. Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a school's Web site.

Examples with respect to Security Key Objectives and also impact on organizations or individuals in case of security breach.

Integrity:
Several aspects of integrity are illustrated by the example of a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital. The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible.

High Level: Patient allergy information is an example of an asset with a high requirement for integrity. Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.

Moderate Level: Web site that offers a forum to registered users to discuss some specific topic. Either a registered user or a hacker could falsify some entries or deface the Web site.

Low Level: anonymous online poll, Many Web sites, such as news organizations, offer these polls to their users with very few safeguards.

Examples with respect to Security Key Objectives and also impact on organizations or individuals in case of security breach.

Availability: Critical Component or Service.
Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks. The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss.

Moderate Level: public Web site for a university; the Web site provides information for current and prospective students and donors. Such a site is not a critical component of the university's information system, but its unavailability will cause some embarrassment.

Low Level: An online telephone directory lookup application would be classified as a low availability requirement. Although the temporary loss of the application may be an annoyance, there are other ways to access the information, such as a hardcopy directory or the operator.

The Challenges of Computer Security:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Because of point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP [Transmission Control Protocol/Internet Protocol] should mechanisms be placed).

The Challenges of Computer Security:

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.
6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.
9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

• **Security attack**: Any action that compromises the security of information owned by an organization.

• **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

The OSI security architecture focuses on Threats and attacks.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

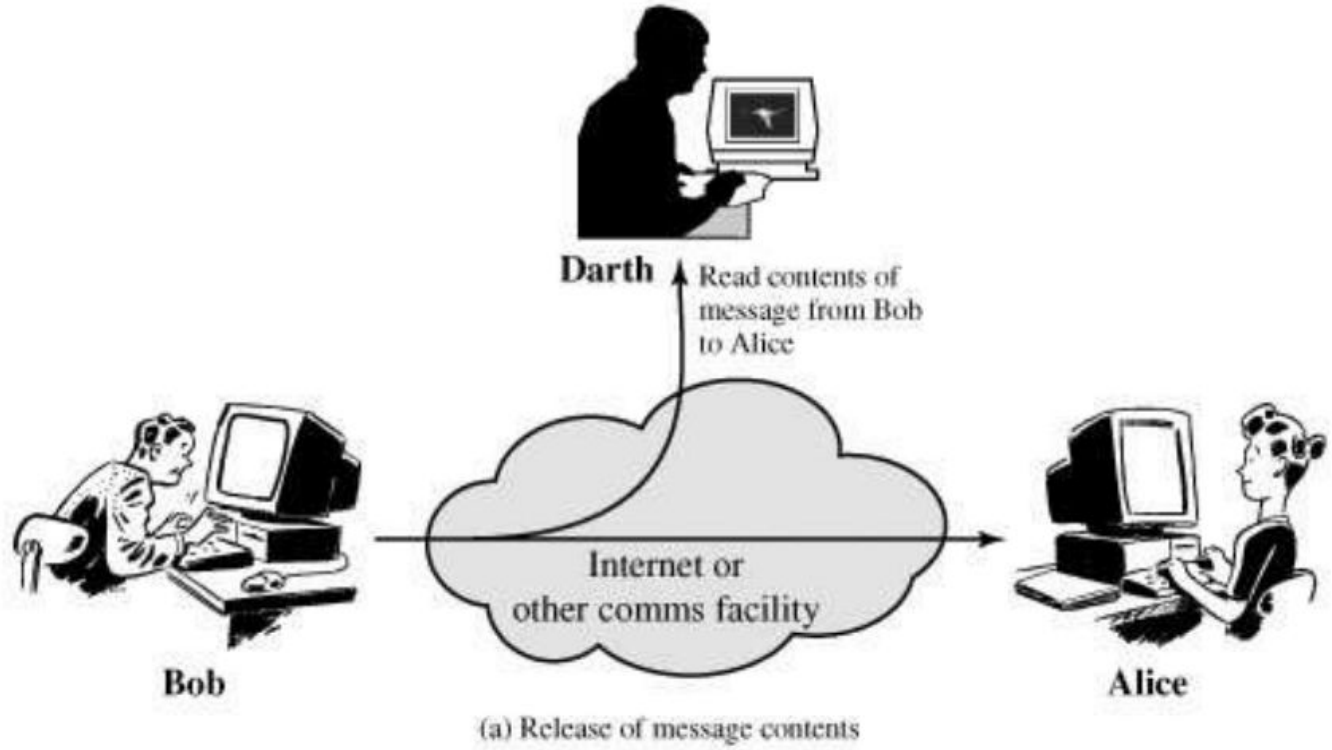
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security Attacks

Passive Attacks:- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

a. Release of message contents



(a) Release of message contents

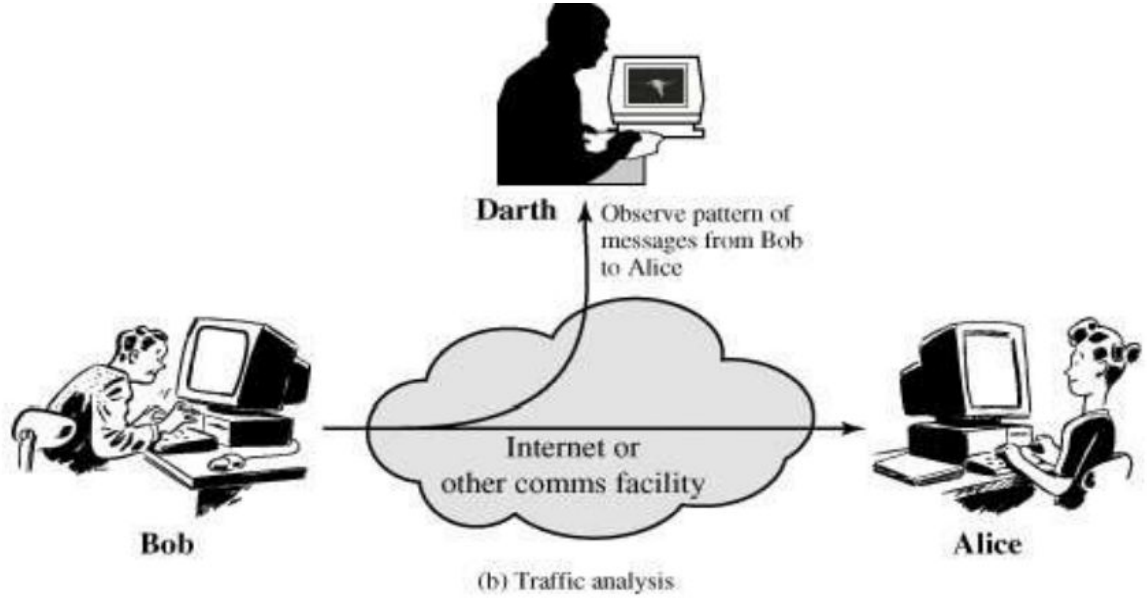
Example: Intercepting an email

Security Attacks

Traffic Analysis:-

If we had a way of masking the contents of messages or other traffic information so that opponents cannot get it, even if they have captured the message, could not extract the information from message.

The common method for masking the contents is Encryption



(b) Traffic analysis

Example: Monitoring that two companies exchange a lot of encrypted traffic during secret deal negotiations.

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

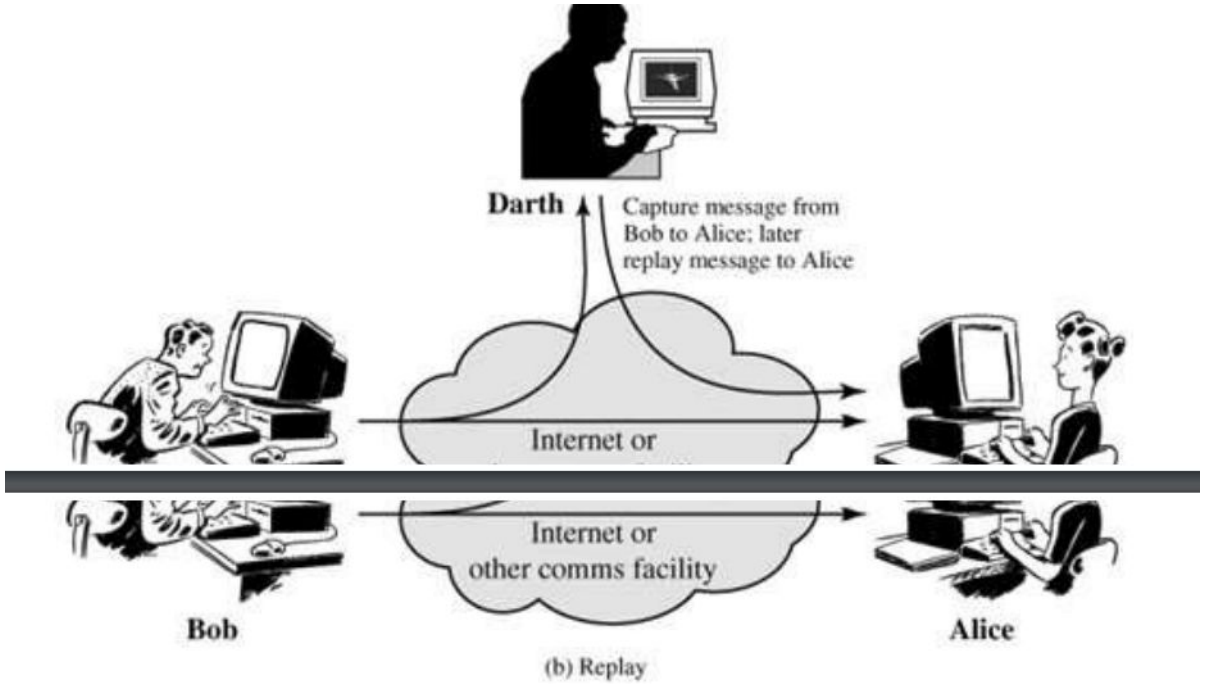
A masquerade(Impersonation) takes place when one entity pretends to be a different entity . A masquerade attack usually includes one of the other forms of active attack.

For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Example: Logging in using stolen credentials.

Active Attacks

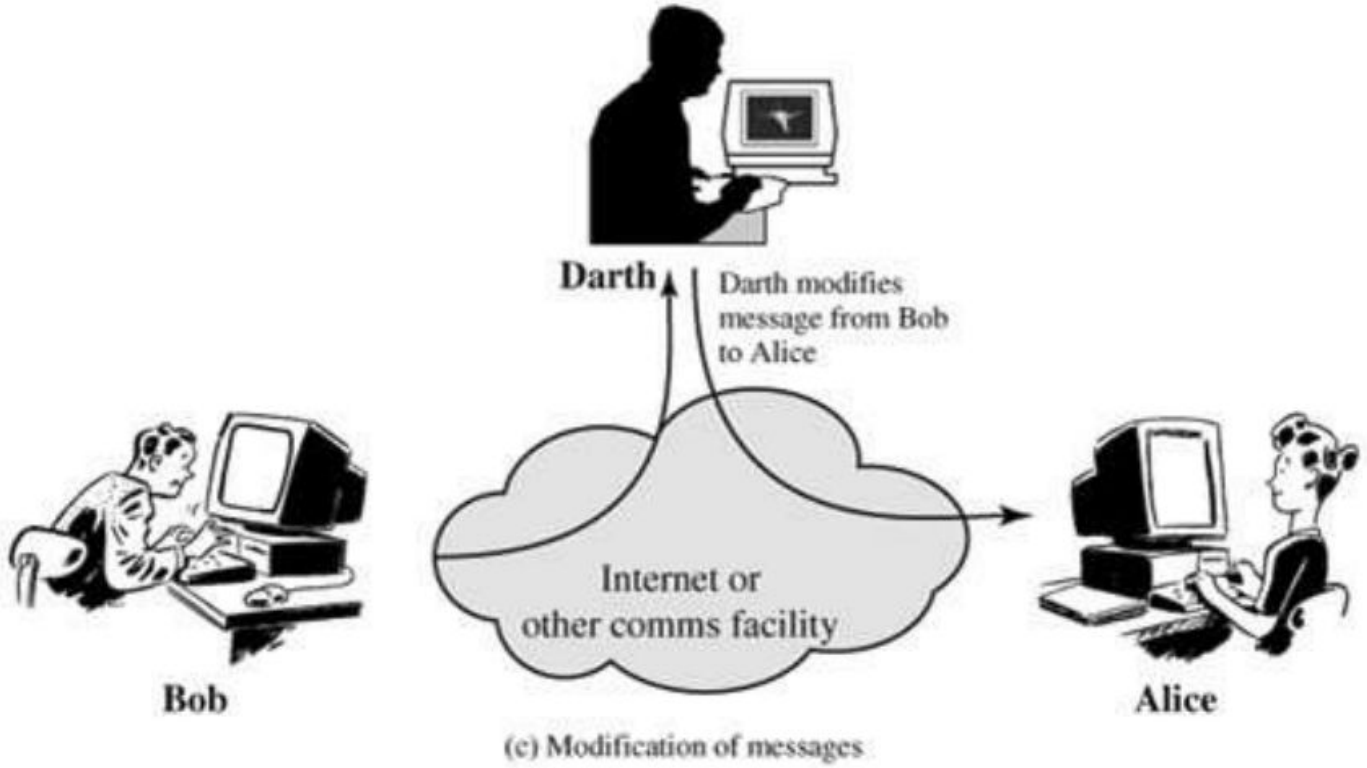
Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



Example: Reusing a payment request message to withdraw money again.

Active Attacks

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect .
For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

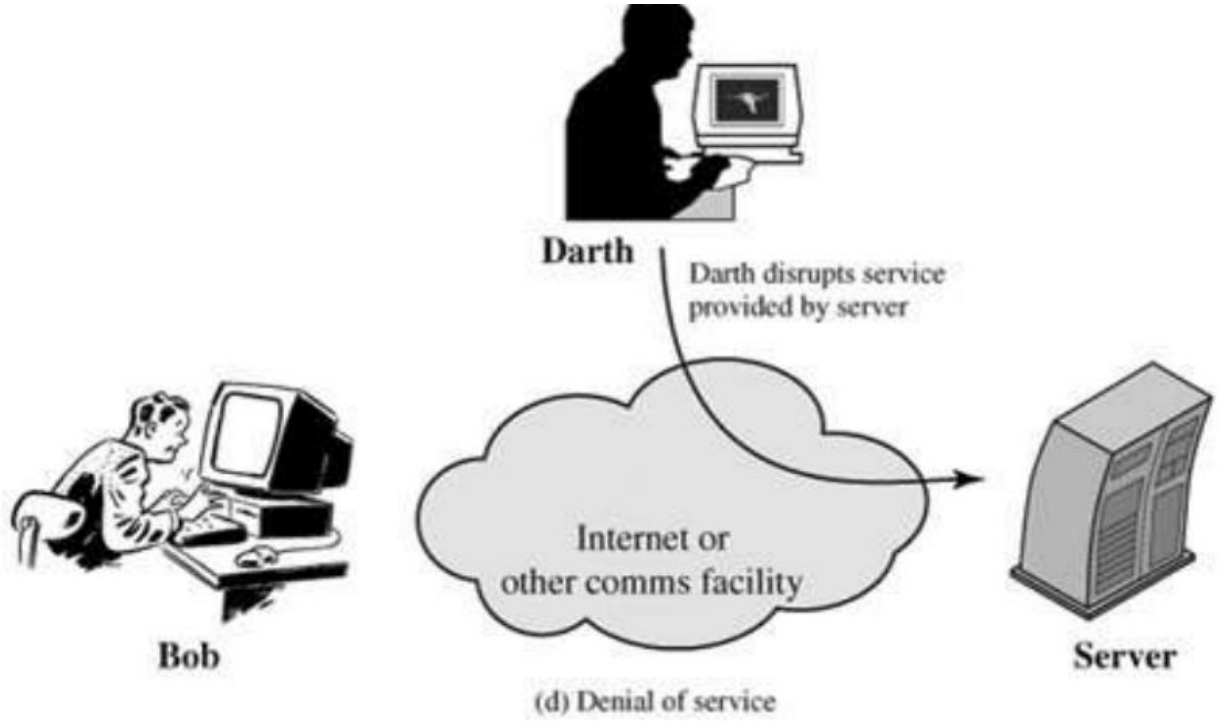


(c) Modification of messages

Example: Altering “transfer ₹1000” to “transfer ₹10,000” in a banking transaction.

Active Attacks

The **denial of service** prevents or inhibits the normal use or management of communications facilities .This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



(d) Denial of service

Example: Flooding a server with requests so real users can’t log in.

Security Services

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Services

Authentication:
The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved.
First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be.
Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Security Services

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

Security Services

Authentication:
Two specific authentication services are defined in X.800:

• **Peer entity authentication**: Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems; for example, two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection.

• **Data origin authentication**: Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.

Security Services

Access Control:

- In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links.

- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data Confidentiality

- Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified.
- The broadest service protects all user data transmitted between two users over a period of time. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection.
- The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

Security Services

Data Integrity

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection.

A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service.

On the other hand, a **connectionless integrity service**, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only. We can make a distinction between service with and without recovery. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention.

If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation.

Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

Availability Service

X.800 treats availability as a property to be associated with various security services. However, it makes sense to call out specifically an availability service. An availability service is one that protects a system to ensure its availability. This service addresses the security concerns raised by denial-of-service attacks. It depends on proper management and control of system resources and thus depends on access control service and other security services.

Security Services

Table 1.2 Security Services (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Security Mechanisms

Security mechanism X.800 defines a security service as a service.

Specific Security Mechanism

- **Encipherment**:- The use of mathematical algorithm to transfer data into a form that is not readily intelligible. The transformation and recovery of the data depend on an algorithm and zero or more encryption keys. **Example: Encrypting a credit card number before sending it online.**

- **Digital Signature:- Data appended to, or cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of data unit and protect against forgeries.**

Example: Signing an email with a digital certificate so the receiver knows it's genuine and unchanged.

- **Access Control:- A variety of mechanisms to enforce access rights to resources. Example: A user login system that allows only employees to access company files.**

- **Data Integrity:- A variety of mechanisms used to assure the integrity of data unit. Ex: Using hashing to detect file tampering**

- **Authentication Exchange:- A mechanism intended to ensure the identity of an entity by means of information exchange. Ex: In online banking.. Username and password logging**

- **Traffic Padding:- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts. Example: A VPN inserting dummy packets so attackers can't guess when or how much real data is sent.**

Security Mechanisms

Specific Security Mechanism

- **Routing Control**: Enables selection of particular physically secure routes for certain data and allows routing changes, when a breach of security suspected.
- **A banking system reroutes sensitive transactions through a VPN tunnel instead of the public internet when unusual activity is detected.**

- **Notarization: The use of a trusted party to assure certain properties of a data exchange.**
- **A digital notary service confirming that a contract was signed by both parties at a specific time, preventing later disputes.**

Security Mechanisms

Pervasive Security Mechanism:- Mechanism that are not specific to any particular protocol layer.

- **Trusted Functionality**

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy). Ex: An operating system's login process.

- **Security Label**

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. Ex: A file marking as a confidential

- **Event Detection**

Detection of security-relevant events. Ex: An IDS that alerts when unusual login attempts occur.

- **Security Audit Trail**

Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. Ex: Web server logs recording login attempts and web downloads

- **Security Recovery**

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions. Ex: Automatically locking attempts after multiple attempts

Security Mechanisms

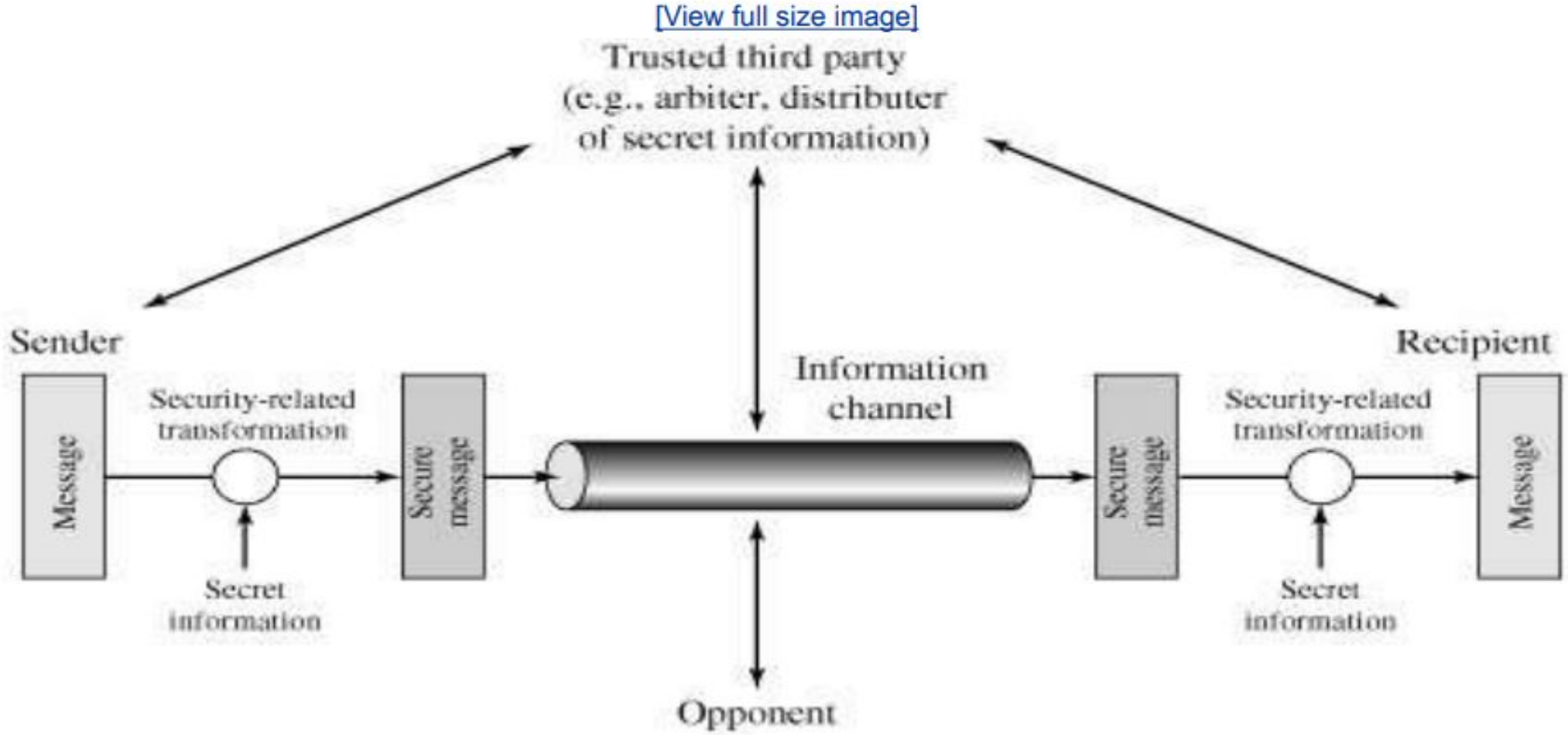
Table 1.4 Relationship Between Security Services and Mechanisms

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Model for Network Security

Figure 1.5. Model for Network Security

[View full size image]



Model for Network Security

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Model for Network Security

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender

- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Model for Network Security

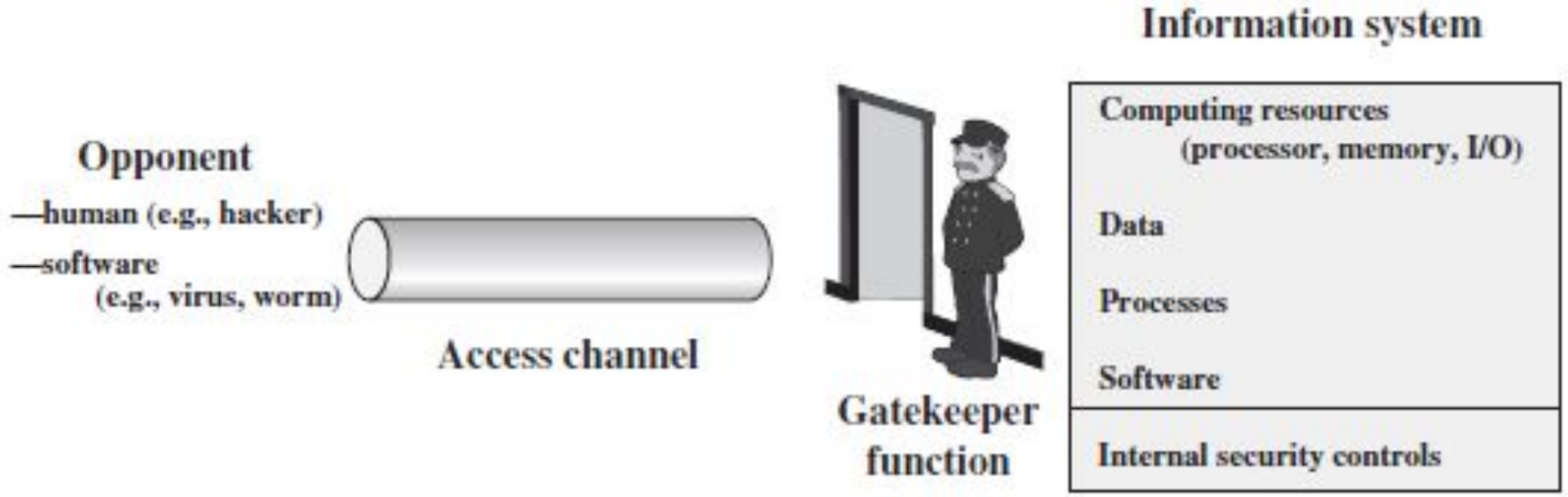


Figure 1.3 Network Access Security Model

Symm

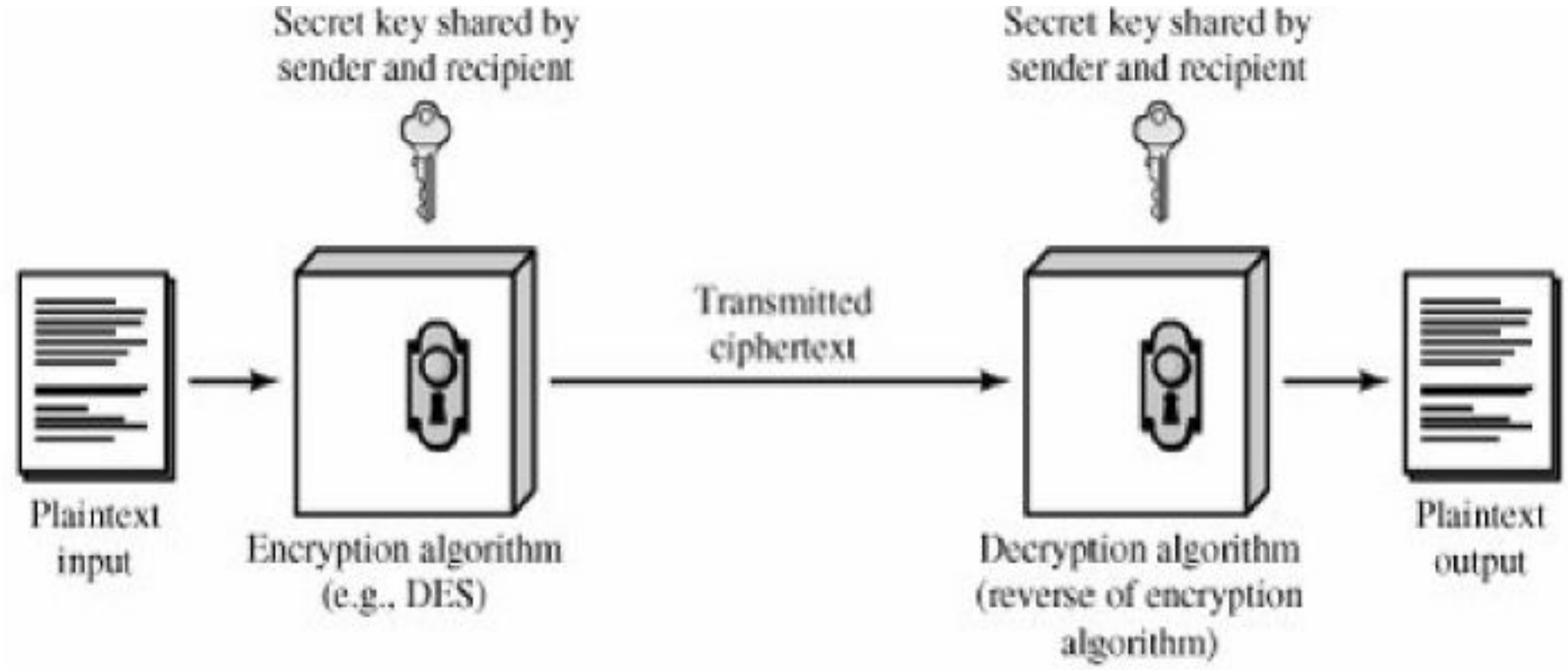


Fig: A simplified model of conventional Encryption

Classical Encryption Techniques

Symmetric Cipher Model

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and as it stands, is unintelligible.

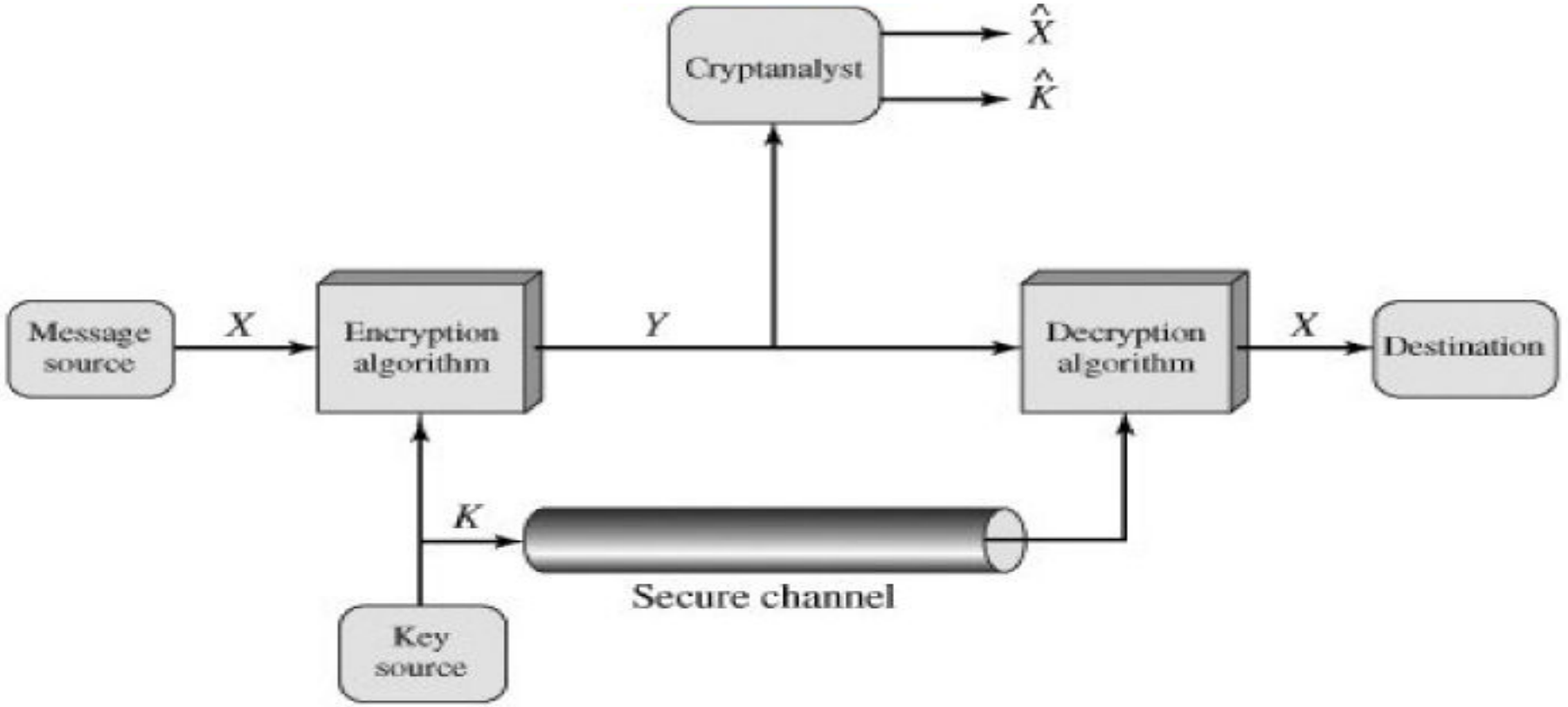
Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher Model

Two requirements for the Secure use of Conventional Encryption:

1. We need strong encryption algorithm. The opponent should be unable to decrypt ciphertext or discover the key even if he or she in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. The Sender and Receiver must obtain the same copies of the secret key in a secure fashion and keep the key secure.



A Model of Conventional Crypto System

Cryptography

Cryptographic Systems are characterized along 3 independent dimensions:

- The type of operations used for transforming plaintext to ciphertext
- The number of keys used
- The way in which plaintext is processed

Cryptanalysis

Two general approaches for attacking conventional encryption scheme

- Cryptanalysis
- Brute Force Attack

Table 2.1. Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext
Known plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Chosen text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Imp things to remember:

- An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available

The users of Encryption Algorithm strive for an algorithm must meet at least one or both of following criteria, if they are met algorithm is computationally secure.

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Substitution Techniques

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Ciphers

The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

For example,

plain: meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB

Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Ciphers

The algorithm

$$C = E(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

$$C = E(k, p) = (p + k) \bmod 26$$

$$P=D(k,C)=(C-k) \bmod 26$$

Caesar Ciphers

The algorithm

Step 1: Encrypting using the formula

Plaintext: HELLO
Shift (n): 3

For each letter in the plaintext, we apply the encryption formula:

H:

Position of H: x=7
x=7 (since A = 0, B = 1, ..., H = 7)

$E(x)$=(7+3)mod26=10
E(x)=(7+3)mod26=10 → Corresponding letter is K

E:

Position of E:x=4
x=4

$E(x)$=(4+3)mod 26 = 7
E(x)=(4+3)mod26=7 → Corresponding letter is H

Caesar Ciphers

The algorithm

Step 2: Decrypting using the formula

To decrypt, we use the decryption formula:

K:

Position of K: x=10
x=10

$D(x)$=(10−3)mod26=7
D(x)=(10−3)mod26=7 → Corresponding letter is H

H:Position of H:x=7
x=7

$D(x)$=(7−3)mod26 =4
D(x)=(7−3)mod26=4 → Corresponding letter is E

Monoalphabetic Ciphers

With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.

Frequency Analysis

- Suppose we have a long ciphertext, the challenge is to decipher it.
- Let we know the text is in English and has been encrypted using a monoalphabetic substitution cipher.

Searching all possible keys is impractical as the key space is of size 26!

Monoalphabetic Ciphers

Ciphertext:-

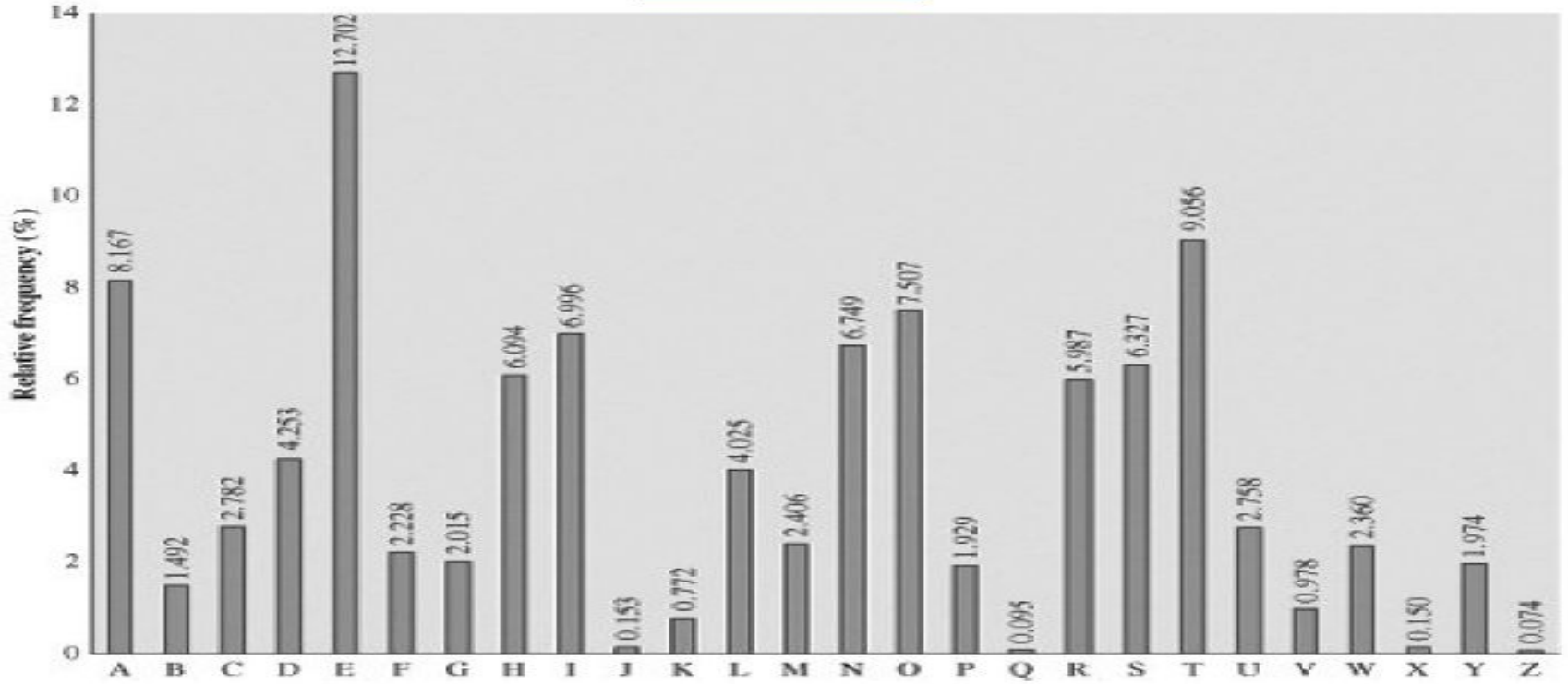
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

As a first step, the relative frequency of the letters can be determined and compared to a standard frequency distribution for English, such as is shown in below figure

Figure 2.5. Relative Frequency of Letters in English Text

[View full size image]



- cipher letters P and Z are the equivalents of plain letters e and t, but it is not certain which is which.
- The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}.
- The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.
- A powerful tool is to look at the frequency of two-letter combinations, known as digrams.
- The most common such digram is th. In our ciphertext, the most common digram is ZW, which appears three times. So we make the correspondence of Z with t and W with h. Then, by our earlier hypothesis, we can equate P with e.
- Now ZWP replaced with “the” trigram(three letter combination)

Monoalphabetic ciphers

Decrypted Text:

“it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in Moscow”

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- A countermeasure is to provide multiple substitutes, known as homophones, for a single letter.

Polyalphabetic ciphers

1. **Monoalphabetic Cipher**:

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key. Examples of monoalphabetic ciphers would include the Caesar-shift cipher, where each letter is shifted based on a numeric key, where each letter is mapped to the letter symmetric to it about the center of the alphabet.

2. Polyalphabetic Cipher :

A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The Playfair and Vigenère cipher is probably the best-known example of a polyalphabetic cipher, though it is a simplified special case.

Playfair Cipher—Multi alphabet substitution Cipher

- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.
- The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

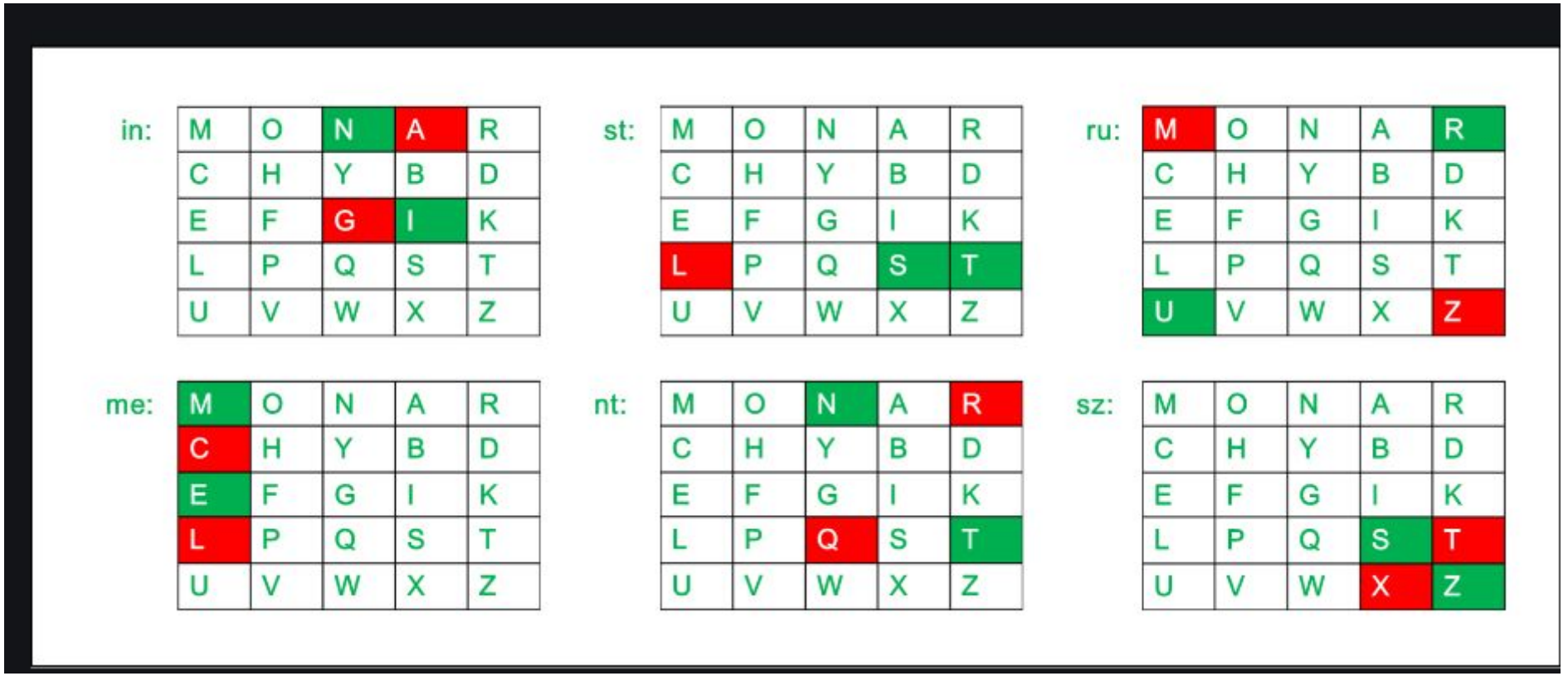
Rules for playfair cipher

- Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
- Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
- Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the enciphered wishes).

Keyword—Monarchy
Message(Plaintext)—Instruments

```
PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
```

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



Ciphertext is : GATLMZCLRQTX

Vigenere Cipher

- Vigenere Cipher is a method of encrypting alphabetic text.
- It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
- The encryption of the original text is done using the Vigenère square or Vigenère table.

Input text:- hellostudents
Keyword:- cyber

The keyword is repeated in the circular manner until it matches the length of the plaintext.

Vigenere Cipher

View full size image

Key \ Plaintext	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
a	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
b	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	A
c	C	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
d	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
e	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	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Vigenere Cipher

Encryption:

The first letter of the plaintext, h is paired with c, the first letter of the key. So use row h and column c of the Vigenère square, namely J. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row e, and column y is c. The rest of the plaintext is enciphered in a similar fashion.

JCMPFURVHVPRT

Decryption:

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row c(from cyber), the ciphertext J appears in column h.

Vigenere Cipher

Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i) \bmod 26$