CS8792

CRYPTOGRAPHY AND NETWORK SECURITY

UNIT 1 NOTES

UNIT I **INTRODUCTION**

Security trends – Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies – Model of network security – Security attacks, services mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.

DEFINITION

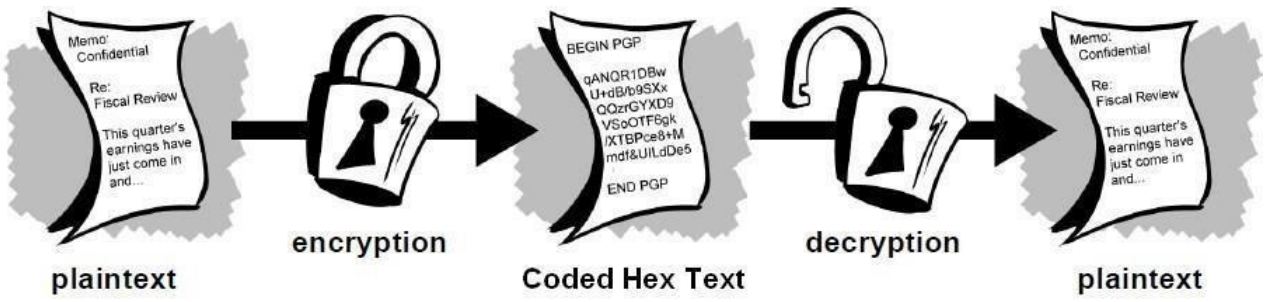
- Cryptography is the science of using mathematics to encrypt and decrypt data.

  Phil Zimmermann
- Cryptography is the art and science of keeping messages secure.

  Bruce Schneier
- The art and science of concealing the messages to introduce secrecy in information Security is recognized as cryptography.
- It is the study and practice of techniques for secure communication in the presence of third parties called adversaries. Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

Terminologies

A message is **plaintext** (sometimes called clear text). The process of disguising a message in such a way as to hide its substance is **encryption**. An encrypted message is **cipher text**. The process ofturning cipher text back into plaintext is **decryption**.



A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**. The various components of a basic cryptosystem are as follows

- Plaintext
- Encryption Algorithm
- Cipher text
- Decryption Algorithm
- Encryption Key
- Decryption Key

While **cryptography** is the science of securing data, **cryptanalysis** is the science of analyzing andbreaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. **Cryptanalysts** are also called attackers. **Cryptology** embraces both cryptography and cryptanalysis.

1.1 SECURITY TRENDS

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)

This definition introduces three key objectives that are at the heart of computer security:

1. **Confidentiality:** This term covers two related concepts:
   (i) **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
   (ii) **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
2. **Integrity:** This term covers two related concepts:
   (i) **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
   (ii) **System integrity:** Assures that a system performs its intended function in an unimpaired manner,free from deliberate or inadvertent unauthorized manipulation of the system.
3. **Availability:** Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the **CIA triad** (Figure 1.1). The three concepts embody the fundamental security objectives for both data and for information and computing services.

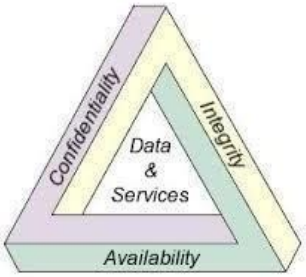
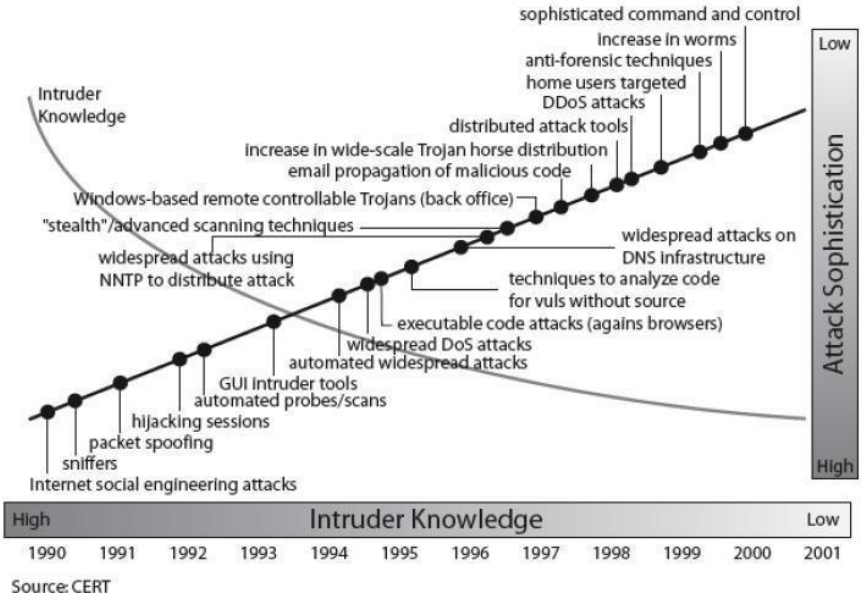


Figure 1.1 The Security Requirements Triad

Two of the most commonly mentioned are as follows:

- **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 non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
- **Computer Security** - Generic name for the collection of tools designed to protect data and to thwart hackers**.**
- **Network Security -** Measures to protect data during their transmission.
- **Internet Security** - Measures to protect data during their transmission over a collection of interconnected networks Our Focus is on Internet Security which consists of measures to deter, prevent, detect and correct security violations that involve the transmission and storage of information.**Figure 1.2 Security Trends**



THE CHALLENGES OF COMPUTER SECURITY

Computer and network security is both fascinating and complex. Some of the reasons follow:

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, non repudiation, or integrity

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.

3. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.

4. Having designed various security mechanisms, it is necessary to decide where to use them.This is trueboth in terms of physical placement and in a logical sense

5. Security mechanisms typically involve more than a particular algorithm or protocol

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 littlebenefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today‟s short-term,overloadedenvironment.

9. Security is still too often an afterthought to be incorporated into a system after the design iscompleterather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment toefficientand user-friendly operation of an information system or use of information.

1.2 LEGAL, ETHICAL AND PROFESSIONAL ASPECTS OF SECURITY

We must understand the scope of an organization's legal and ethical responsibilities. To minimize liabilities/reduce risks, the security practitioner must:

1. Understand current legal environment.
2. Stay current with laws and regulations.
3. Watch for new issues and emerge.

Information is endangered both by external factors, such as hackers, computer viruses, thefts, and internal ones - the loss of data as a result of improper protection, the lack of backup copies orthe loss of a flash drive that contains unprotected data. An improper protection of data may resultin the loss of company's reputation, its customers' trust or in financial losses. This issue is of particular importance as regards the court system due to the volume of personal data that are processed and stored in courts and their unique character (sentences, orders, and statements of reasons, convictions, and personal details of victims or land registers). They all constituteinformation that must be protected against theft, loss or alterations. The loss of data could affect negatively the trial and the judicial independence by possible external pressure in cases where datawas lost.

Cryptography and Law:

Cyber-Crime: - Criminal activities or attacks in which computer and computer networks are tool, target, or place of criminal activity. Cybercrime categorize based on computer roles such as target, storage device and communication tool.

Computers as targets: To get the information from the computer system or control the computer system without the authorization or payment or alter the interfaces or data in the particular system with use of server.

Computers as storage devices: Computers can be used to further unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer canbe usedto store stolen password lists, credit card details and proprietary corporate information.

Computers as communications tools: Many of the crimes falling within this category are simply traditional crimes that are committed online. Examples include the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography. Other than these crimes there are more specific crimes in computer networks. There are:

Illegal access: The access to the whole or any part of a computer system without right. Illegal interception: The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Data interference: The damaging, deletion, deterioration, alteration or suppression of computerdata without right.

System interference: The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressingcomputer data.

Computer-related forgery: The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Crime related to child pornography: Producing child pornography or distribution through a computer system and making available or distributing or transmitting child pornography through a computer system.

The relative lack of success in bringing cyber-criminals to justice has led to an increase in their numbers, boldness, and the global scale of their operations. It is difficult to profile cybercriminalsin the way that is often done with other types of repeat offenders. The success of cybercriminals and the relative lack of success of law enforcement, influence the behaviour of cybercrime victims. As with law enforcement, many organizations that may be the target of attack have not invested sufficiently in technical, physical, and human-factor resources to prevent attacks.

The law is used regulate people for their own good and for the greater good of society. Cryptography also regulated activity.

Some Example laws which are forced on cryptography.

Control use of cryptography: Closely related to restrictions on content are restrictions on the use of cryptography imposed on users in certain countries. For examples, 2 In China, state council order 273 requires foreign organizations or individuals to apply permission to use encryption in China. Pakistan requires that all encryption hardware and software be inspected and approved by the Pakistan telecommunication authority.

Cryptography and Free speech: The Cryptography involve not just products, it involves ideas too, although governments effectively control the flow of products across borders, controlling thefloe ideas either head or on the internet, is also impossible.

Cryptography and Escrow: Although laws enable governments to read encrypted communications. In 1996, US government offered to relax the export restriction for so called escrowed encryption, in which the government would ableto obtain the encryption key for any encrypted communication.

The victory in use of law enforcement depends much more on technical skills of the people. Management needs to understand the criminal investigation process, the inputs thatinvestigators need, and the ways in which the victim can contribute positively to the investigation.

Intellectual Properties

There are three main types of intellectual property for which legal protection is available. **Copy rights:** Copyright law protects the tangible or fixed expression of an idea, not the idea itself. Copy right properties exists when proposed work is original and creator has put original idea in concrete form and the copyright owner has these exclusive rights, protected against infringement such as reproduction right, modification right, distribution right

Patents: A patent for an invention is the grant of a property right to the inventor. There are 3 types in patents:-

- Utility (any new and useful process, machine, article of manufacture, or composition ofmatter).
- Design (new, original, and ornamental design for an article of manufacture)
- Plant (discovers and asexually reproduces any distinct and new variety of plant).

Trade-Marks: A trademark is a word, name, symbol or expression which used to identify the products or services in trade uniquely from others. Trade mark rights used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark.

- Intellectual Property Relevant to Network and Computer Security A number of forms of intellectual property are relevant in the context of network and computer security.
- Software programs: software programs are protected by using copyright, perhaps patent.
- Digital content: audio / video / media / web protected by copy right Algorithms: algorithms may be able to protect by patenting
- Privacy Law and Regulation: An issue with considerable overlap with computer securityis that of privacy. Concerns about the extent to which personal privacy has been and may be compromised have led to a variety of legal and technical approaches to reinforcing privacy rights. A number of international organizations and national governments have introduced laws and regulations intended to protect individual privacy.
- European Union Data Protection Directive was adopted in 1998 to ensure member states protectfundamental privacy rights when processing personal info and prevent member states from restricting the free flow of personal info within EU organized around principles of notice, consent, consistency, access, security, onward transfer and enforcement. US Privacy Law have Privacy Act of 1974 which permits individuals to determine records kept, forbid records being used for other purposes, obtain access to records, ensures agencies properly collect, maintain, and use personalinfo and createsa private rightofactionfor individuals.Cryptography and Ethics.
- There are many potential misuses and abuses of information and electronic communication that create privacy and security problems. Ethics refers to a system of moral principles that relates to the benefits and harms of particular actions. An ethic an objectively defined standard of right and wrong.Ethical standards are often idealistic principles because they focus on one objective. Even though religious group and professional organization promote certain standards of

ethical behaviour, ultimately eachperson is responsible for deciding what do in a specific situation.

Ethical issues related to computer and info systems

Computers have become the primary repository of both personal information and negotiable assets, such as bank records, securities records, and other financial information.

Repositories and processors of information: Unauthorized use of otherwise unused computer services or of information stored in computers raises questions of appropriateness or fairness.

Producers of new forms and types of assets: For example, computer programs are entirely new types of assets, possibly not subject to the same concepts of ownership as other assets.

Symbols of intimidation and deception: The images of computers as thinking machines, absolute truth producers, infallible, subject to blame, and as anthropomorphic replacements of humans who err should be carefully considered.

Ethics and Security

The Ten Commandments of Computer Ethics[6]

From The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

1.2.1 NEED FOR MULTILEVEL SECURITY

Multilevel security or multiple levels of security (MLS) is the application of a computer system to process information with incompatible classifications (i.e., at different security levels), permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.

There are two contexts for the use of multilevel security.

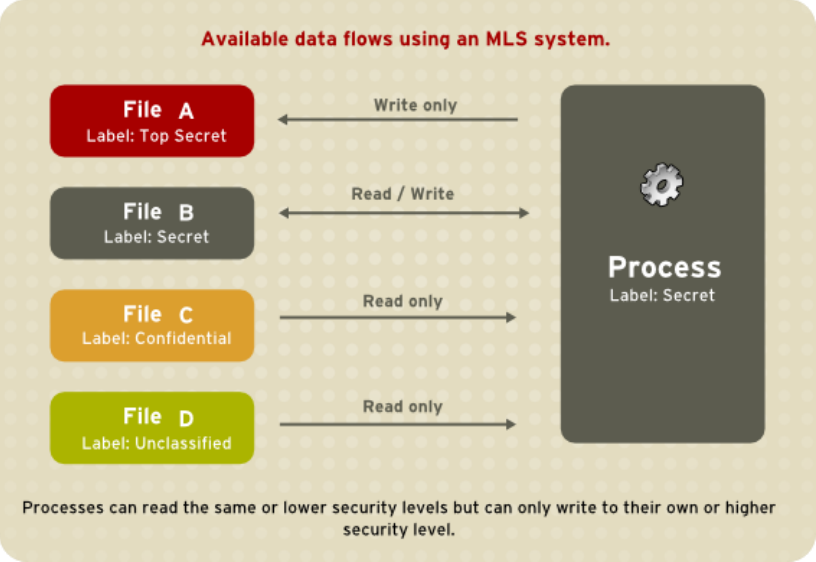
- One is to refer to a system that is adequate to protect itself from subversion and has robust mechanisms to separate information domains, that is, trustworthy.
- Another context is to refer to an application of a computer that will require the computer to be strong enough to protect itself from subversion and possess adequate mechanisms to separate information domains, that is, a system we must trust. This distinction is important because systems that need to be trusted are not necessarily trustworthy.

A threat is an object, person, or other entity that represents a constant danger to an asset.

Having information of different security levels on the same computer systems poses a real threat. It is not a straight-forward matter to isolate different information security levels, even though different users log in using different accounts, with different permissions and different access controls. Some organizations go as far as to purchase dedicated systems for each security level. This is often prohibitively expensive, however. A mechanism is required to enable users at different security levels to access systems simultaneously, without fear of information contamination.

The term multi-level arises from the defense community's security classifications: Confidential,Secret, and Top Secret.

Individuals must be granted appropriate clearances before they can see classified information. Those with Confidential clearance are only authorized to view Confidential documents; they arenot trusted to look at Secret or Top Secret information. The rules that apply to data flow operatefrom lower levels to higher levels, and never the reverse. This is illustrated below.



Information Security Levels **Available data flow using MLS system**

Under such a system, users, computers, and networks use labels to indicate security levels. Data can flow between like levels, for example between "Secret" and "Secret", or from alower level to a higher level. This means that users at level "Secret" can share data with one another, and can also retrieve information from Confidential-level (i.e., lower-level), users.

However, data cannot flow from a higher level to a lower level. This prevents processes at the "Secret" level from viewing information classified as "Top Secret". It also prevents processes at a higher level from accidentally writing information to a lower level. This is referred to as the"no read up, no write down" model.

MLS and System Privilege

MLS access rules are always combined with conventional access permissions (file permissions). For example, if a user with a security level of "Secret" uses Discretionary AccessControl (DAC) to block access to a file by other users, this also blocks access by users with a security level of "Top Secret". A higher security clearance does not automatically give permission to arbitrarily browse a file system.

Users with top-level clearances do not automatically acquire administrative rights on multi-level systems. While they may have access to all information on the computer, this is different from having administrative rights.

Security Levels, Objects and Subjects

As discussed above, subjects and objects are labeled with Security Levels (SLs), whichare composed of two types of entities:

Sensitivity: — A hierarchical attribute such as "Secret" or "Top Secret". Categories: — A set of non-hierarchical attributes such as "US Only" or "UFO".An SL must have one sensitivity, and may have zero or more categories.

Examples of SLs are: { Secret / UFO, Crypto }, { Top Secret / UFO, Crypto, Stargate }and { Unclassified }

Note the hierarchical sensitivity followed by zero or more categories. The reason for having categories as well as sensitivities is so that sensitivities can be further compartmentalizedon a need-to-know basis.

1.2.2 SECURITY POLICES

Following are some points which help in security policy of an organization.

- Who should have access to the system?
- How it should be configured?
- How to communicate with third parties or systems?Policies are divided in two categories −
- User policies
- IT policies.

User policies generally define the limit of the users towards the computer resources in a workplace. For example, what are they allowed to install in their computer, if they can use removable storages.Whereas, IT policies are designed for IT department, to secure the procedures and functions of IT fields.

- **General Policies** − This is the policy which defines the rights of the staff and access levelto the systems. Generally, it is included even in the communication protocol as apreventive measure in case there are any disasters.
- **Server Policies** − This defines who should have access to the specific server and with what rights. Which software's should be installed, level of access to internet, how they should be updated.
- **Firewall Access and Configuration Policies** − It defines who should have access to the firewall and what type of access, like monitoring, rules change. Which ports and services should be allowed and if it should be inbound or outbound.
- **Backup Policies** − It defines who is the responsible person for backup, what should be the backup, where it should be backed up, how long it should be kept and the frequency of the backup.

- **VPN Policies** − These policies generally go with the firewall policy, it defines those users who should have a VPN access and with what rights. For site-to-site connections with partners, it defines the access level of the partner to your network, type of encryption to be set.

Structure of a Security Policy

When you compile a security policy you should have in mind a basic structure in order to make something practical. Some of the main points which have to be taken into consideration are −

Description of the Policy and what is the usage for?

- Where this policy should be applied?
- Functions and responsibilities of the employees that are affected by this policy.
- Procedures that are involved in this policy.
- Consequences if the policy is not compatible with company standards.

Types of Policies

In this section we will see the most important types of policies.

- **Permissive Policy** − It is a medium restriction policy where we as an administrator block just some well-known ports of malware regarding internet access and just some exploits are taken in consideration.
- **Prudent Policy** − This is a high restriction policy where everything is blocked regarding the internet access, just a small list of websites are allowed, and now extra services are allowed in computers to be installed and logs are maintained for every user.
- **Acceptance User Policy** − This policy regulates the behavior of the users towards a system or network or even a webpage, so it is explicitly said what a user can do and cannot in a system. Like are they allowed to share access codes, can they share resources, etc.
- **User Account Policy** − This policy defines what a user should do in order to have or maintain another user in a specific system. For example, accessing an e-commerce webpage. To create this policy, you should answer some questions such as −
    - Should the password be complex or not?
    - What age should the users have?
    - Maximum allowed tries or fails to log in?
    - When the user should be deleted, activated, blocked?
- **Information Protection Policy** − This policy is to regulate access to information, hot to process information, how to store and how it should be transferred.

- **Remote Access Policy** − This policy is mainly for big companies where the user and their branches are outside their headquarters. It tells what should the users access, when they can work and on which software like SSH, VPN, RDP.
- **Firewall Management Policy** − This policy has explicitly to do with its management, which ports should be blocked, what updates should be taken, how to make changes in the firewall, how long should be the logs be kept.
- **Special Access Policy** − This policy is intended to keep people under control and monitorthe special privileges in their systems and the purpose as to why they have it. These employees can be team leaders, managers, senior managers, system administrators, and such high designation based people.
- **Network Policy** − This policy is to restrict the access of anyone towards the network resource and make clear who all will access the network. It will also ensure whether thatperson should be authenticated or not. This policy also includes other aspects like, who will authorize the new devices that will be connected with network? The documentation of network changes. Web filters and the levels of access. Who should have wireless connection and the type of authentication, validity of connection session?
- **Email Usage Policy** − This is one of the most important policies that should be done because many users use the work email for personal purposes as well. As a result information can leak outside. Some of the key points of this policy are the employees should know the importance of this system that they have the privilege to use. They shouldnot open any attachments that look suspicious. Private and confidential data should not besent via any encrypted email.
- **Software Security Policy** − This policy has to do with the software's installed in the user computer and what they should have. Some of the key points of this policy are Software of the company should not be given to third parties. Only the white list of software's should be allowed, no other software's should be installed in the computer. Warez and piratedoftware's should not be allowed

1.3 THE OSI SECURITY ARCHITECTURE

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.

- ITU-T Recommendation X.800, Security Architecture for OSI, defines such a systematic approach
- The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- The OSI security architecture focuses on security attacks, mechanisms, and services.

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 securityattack.

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

1.3.1 SECURITY ATTACKS

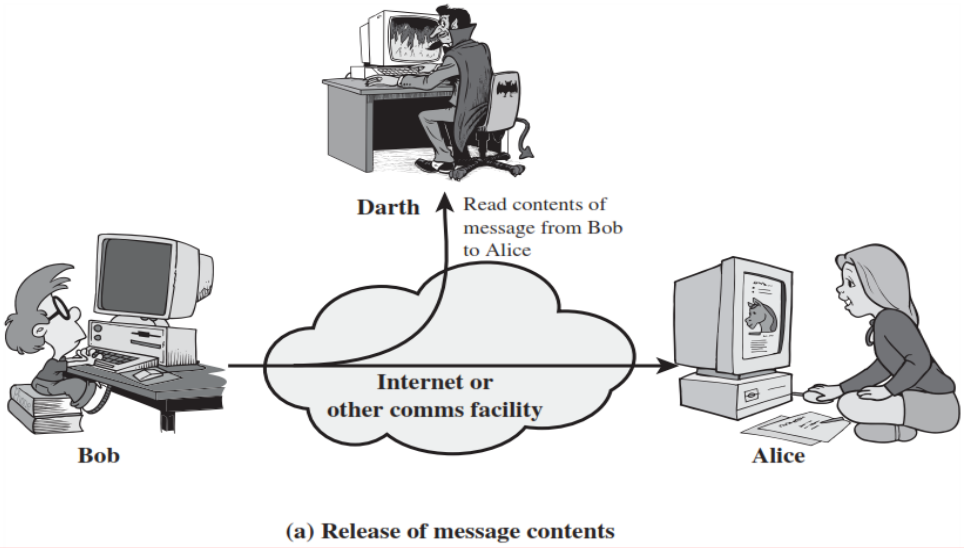
- A useful means of classifying security attacks used both in X.800 and RFC 2828 is in terms of ***passive attacks* and *active attacks.***
- A passive attack attempts to learn or make use of information but does not affect systemresources.
- An active attack attempts to alter system resources or affect their operation.

Passive Attacks

- It is the nature of eavesdropping on, or monitoring of, transmissions.
- The goal is to obtain information that is being transmitted.
- Very difficult to detect, because they do not involve any alteration of the data
- Feasible to prevent the success of these attacks, usually by means of encryption
- Emphasis in dealing with passive attacks is on prevention rather than detection
- Two types of passive attacks
    - Release of message content
    - Traffic analysis.

(i) Release of Message Contents

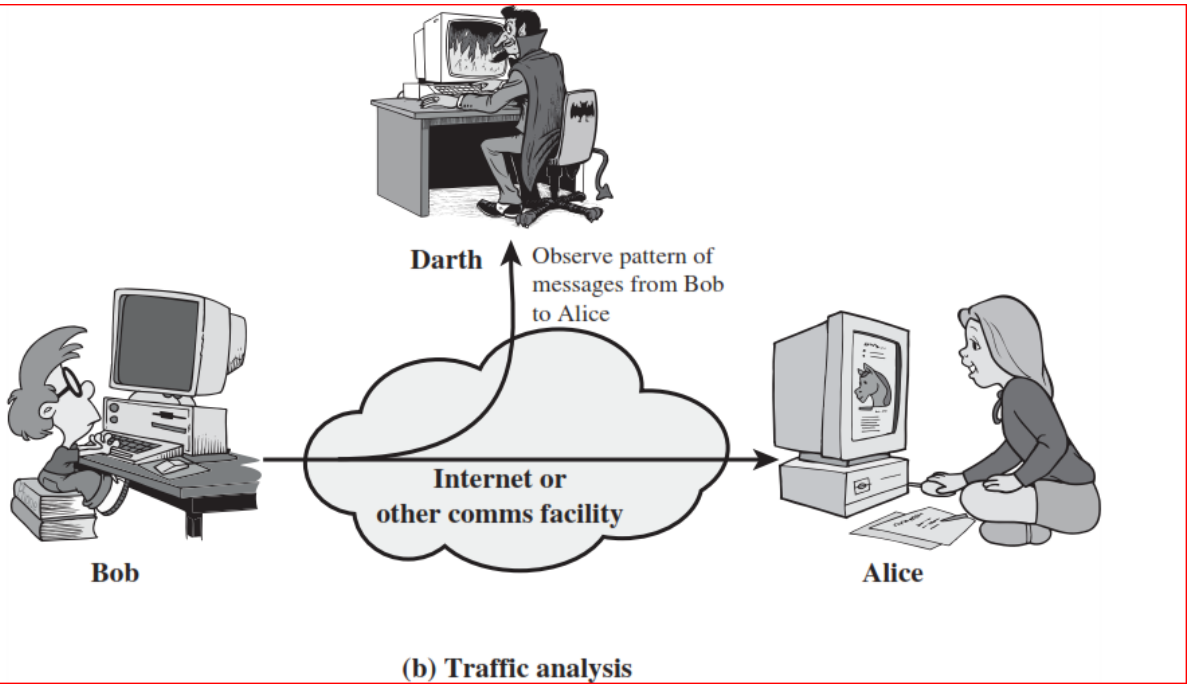
- A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information
- Prevent an opponent from learning the contents of these transmissions



(a) Release of message contents

(ii) Traffic Analysis

- Observe the pattern of these messages.
- The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place



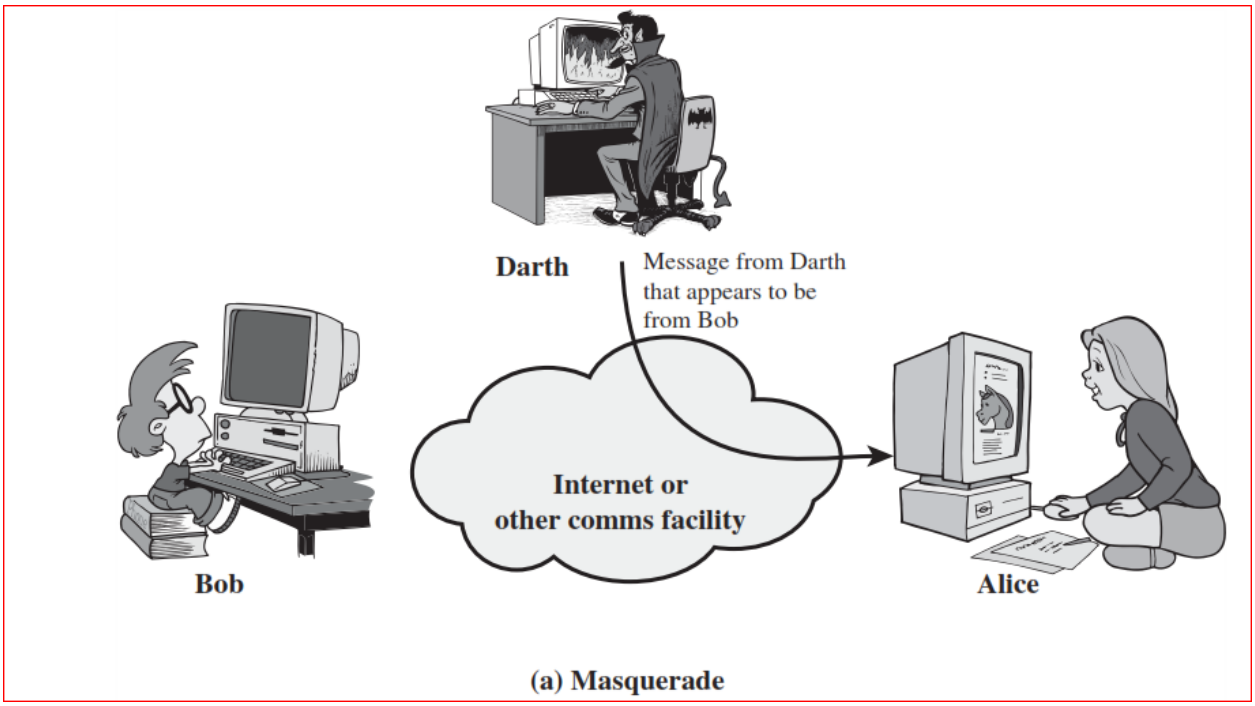
(b) Traffic analysis

Active Attacks

- Active attacks involve some modification of the data stream or the creation of a falsestream
- Detect and to recover from any disruption or delays caused by them
- Can be subdivided into four categories:
    - Masquerade
    - Replay
    - Modification of messages
    - Denial of service

(i) Masquerade

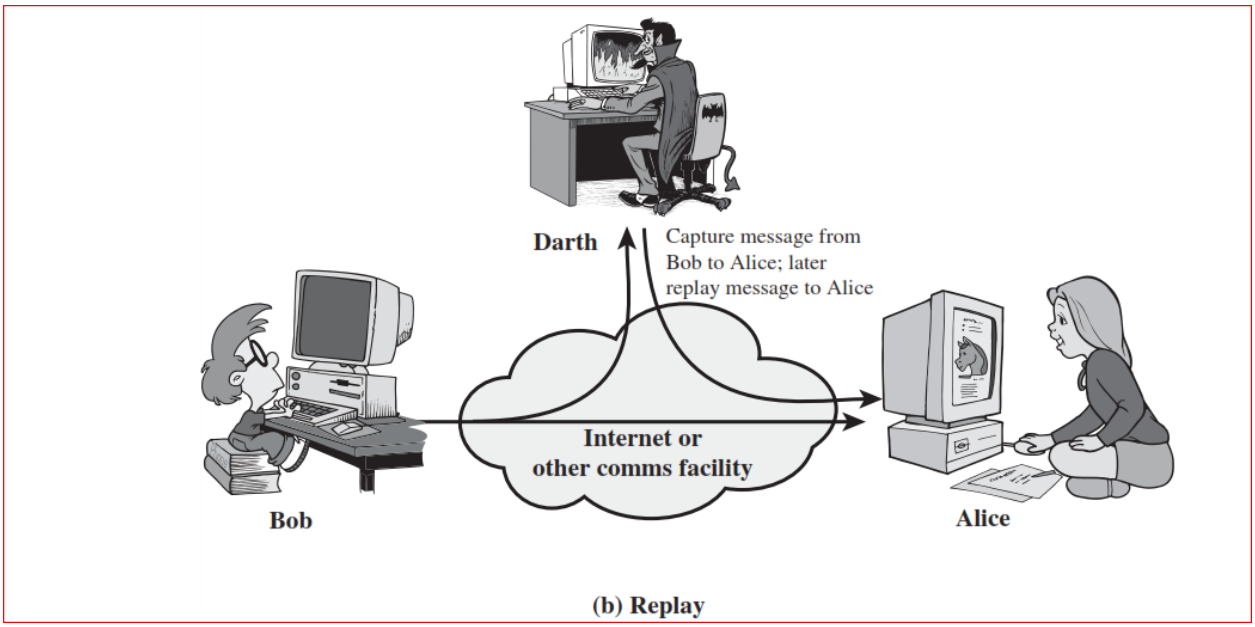
- One entity pretends to be a different entity.
- Usually includes one of the other forms of active attack



(a) Masquerade

(ii) Replay

- Authentication sequences can be captured and replayed after a valid authentication sequence
- Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



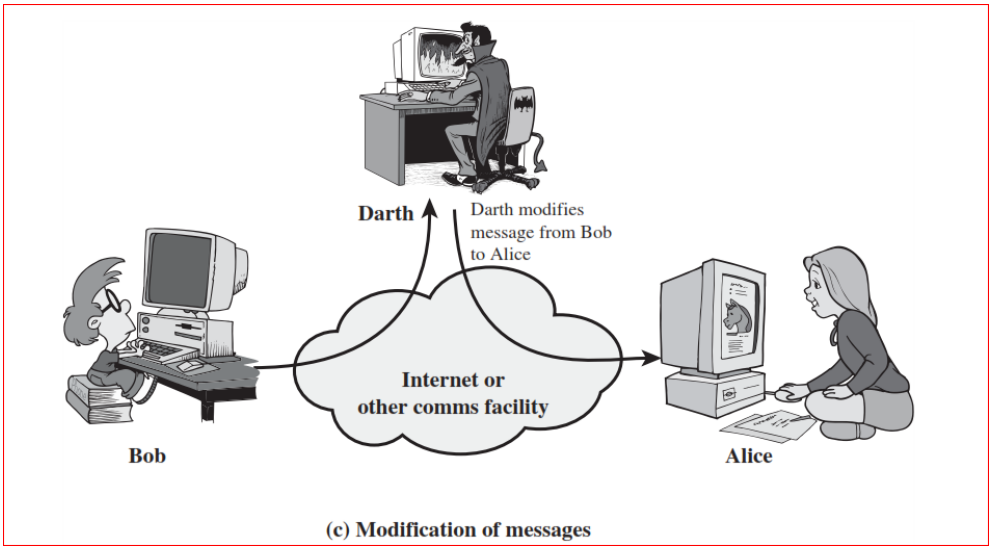
(b) Replay

(iii) Modification of Messages

- Some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect

  Example

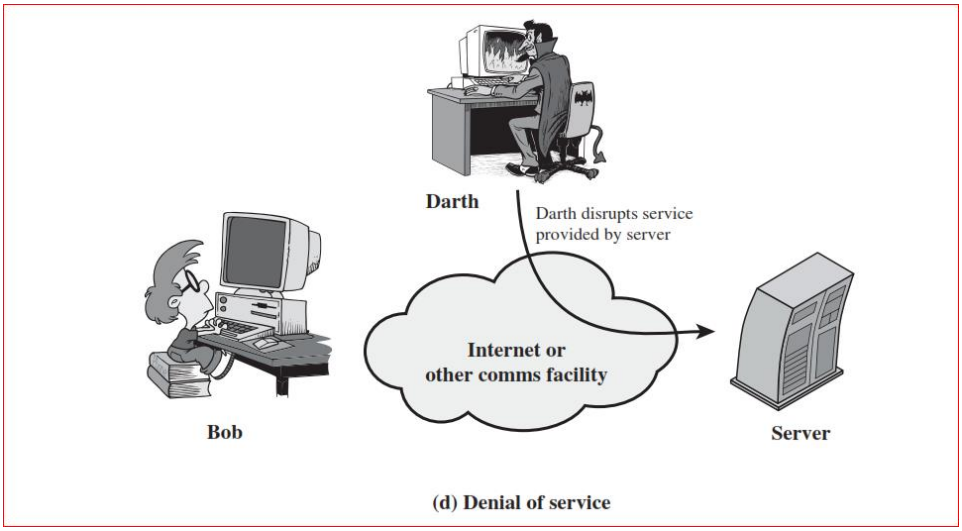
  A message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



(c) Modification of messages

(iv) Denial of Service

- Prevents or inhibits the normal use or management of communications facilities
- May have a specific target; for example, an entity may suppress all messages directed to a particular destination 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

1.3.2 SECURITY SERVICES

- X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of datatransfers.
- RFC 2828, defines as a processing or communication service that is provided by a systemto give a specific kind of protection to system resources;
- Security services implement security policies and are implemented by securitymechanisms.
- X.800 divides these services into five categories and fourteen specific 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.

1.3.3 SECURITY MECHANISMS

Table 1.3 lists the security mechanisms defined in X.800. The mechanisms are divided intothosethat are implemented in a specific protocol layer, such as TCP or an application-layer protocol, andthose that are not specific to any particular protocol layer or security service

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**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.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

1.4 A MODEL FOR NETWORK SECURITY

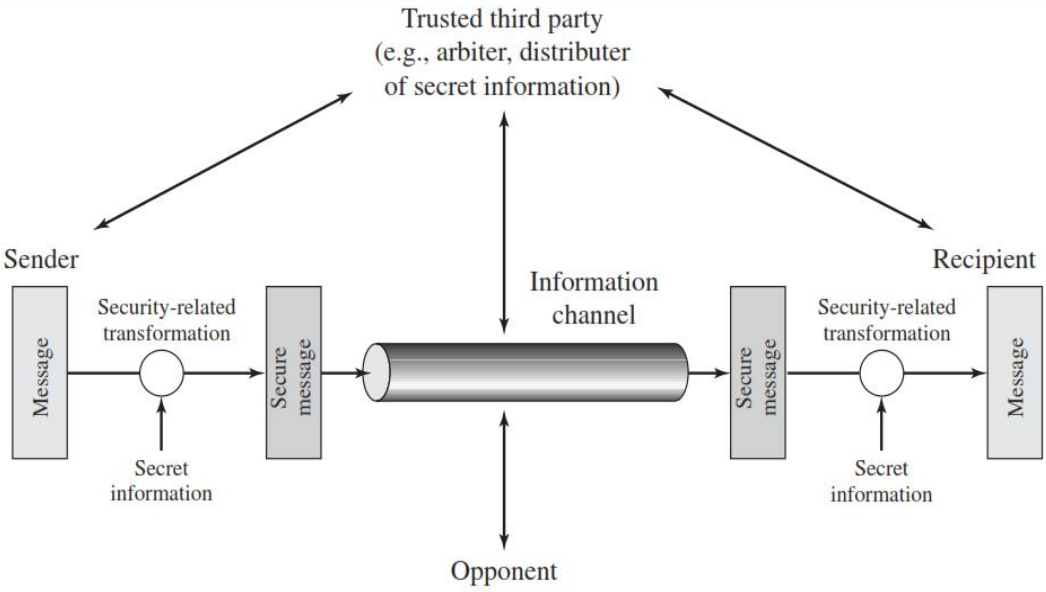


Figure 1.4 Model for Network Security

- A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange totake 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.
- All the techniques for providing security have two components:
  - A security-related transformation on the information to be sent.
    Examples: encryption of the message, addition of a code based on the contents
  - Some secret information shared by the two principals, unknown to the opponent
    Example: encryption key used in conjunction with the transformation
- A trusted third party may be needed to achieve secure transmission.
  - For distributing the secret information to the two principals
  - To arbitrate disputes between the two principals concerning the authenticity of a message transmission
- **Four basic tasks in designing a particular security service:**
  - Design an algorithm for performing the security-related transformation such that an opponent cannot defeat its purpose.
  - Generate the secret information to be used with the algorithm.
  - Develop methods for the distribution and sharing of the secret information.
  - 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

Network Access Security Model

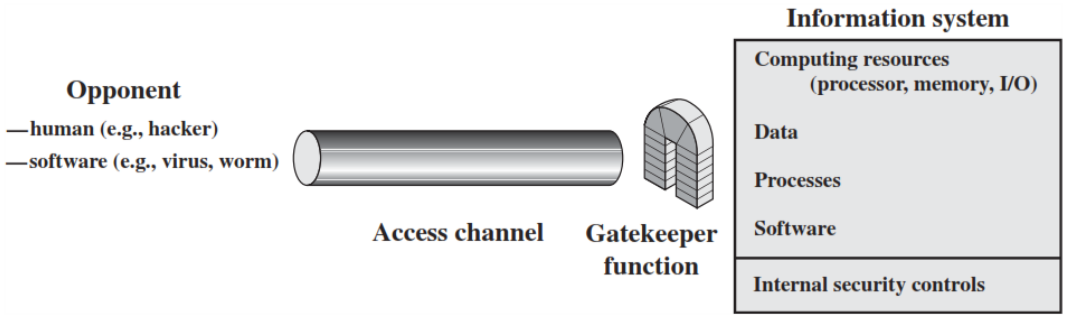


Figure 1.5 Network Access Security Model

- Protecting an information system from unwanted access from hacker, intruder hacker who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- Intruder can be a disgruntled employee who wishes to do damage or a Criminal who seeks to exploit computer assets for financial gain
- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers

Two kinds of threats:

- **Information access threats**: Intercept or modify data on behalf of users who should not have access
- **Service threats**: Exploit service flaws in computers to inhibit use by legitimate users Examples: Viruses and worms, spread using disks & inserted over network

1.5 CLASSICAL ENCRYPTION TECHNIQUES

Introduction

- **Symmetric encryption** is a form of cryptosystem in which encryption and decryption are performed using the **same key**. It is also known as **conventional encryption**.
- Symmetric encryption transforms plaintext into ciphertext using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext.
- The two types of attack on an encryption algorithm are **cryptanalysis**, based on properties of the encryption algorithm, and **brute-force**, which involves trying all possible keys.

- Traditional (precomputer) symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into ciphertext elements. Transposition techniques systematically transpose the positions of plaintext elements.
- Rotor machines are sophisticated precomputer hardware devices that use substitutiontechniques.
- Steganography is a technique for hiding a secret message within a larger one in such a waythat others cannot discern the presence or contents of the hidden message.
- An original message is known as the **plaintext**, while the coded message is called the ciphertext.
- The process of converting from plaintext to ciphertext is known as **enciphering orencryption**; restoring the plaintext from the ciphertext is **deciphering or decryption**.
- The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system or a cipher**.
- Techniques used for deciphering a message without any knowledge of the encipheringdetails fall into the area of cryptanalysis. **Cryptanalysis** is what the layperson calls "breaking the code." The areas of cryptography and cryptanalysis together are called **Cryptology**
- **Symmetric Cipher Model**
    - Cryptanalysis and Brute-Force Attack
- **Substitution Techniques**
    - Caesar Cipher
    - Monoalphabetic Ciphers
    - Playfair Cipher
    - Hill Cipher
    - Polyalphabetic Ciphers
    - One-Time Pad
- **Transposition Techniques**
    - Rail Fence Technique
    - Pure Transposition cipher
- **Steganography**

1.5.1 Symmetric Cipher Model

A symmetric encryption scheme has five ingredients

- **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 transformationson the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent ofthe 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 cipher texts. 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 cipher text and the secret key and produces the original plaintext
- Two requirements for secure use of conventional / symmetric encryption
    - We need a strong encryption algorithm - The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced eachciphertext
    - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable, do not need to keep the algorithm secret; weneed to keep only the key secret. The principal security problem is maintaining the secrecy of the key

Simplified Model of Symmetric Encryption

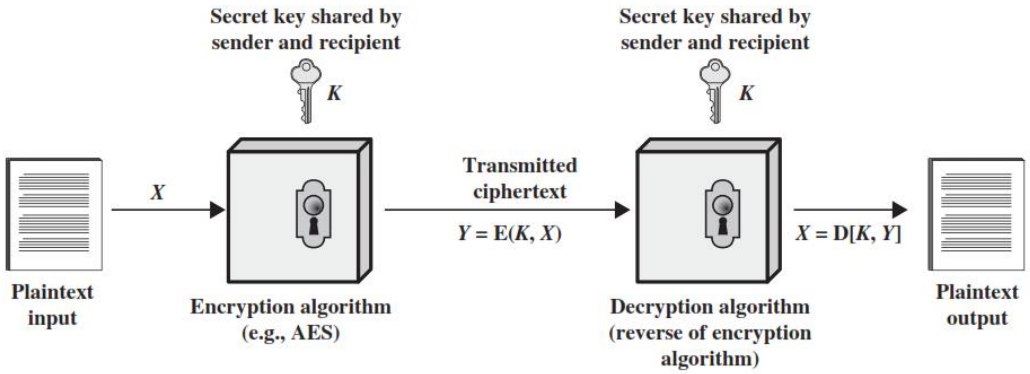
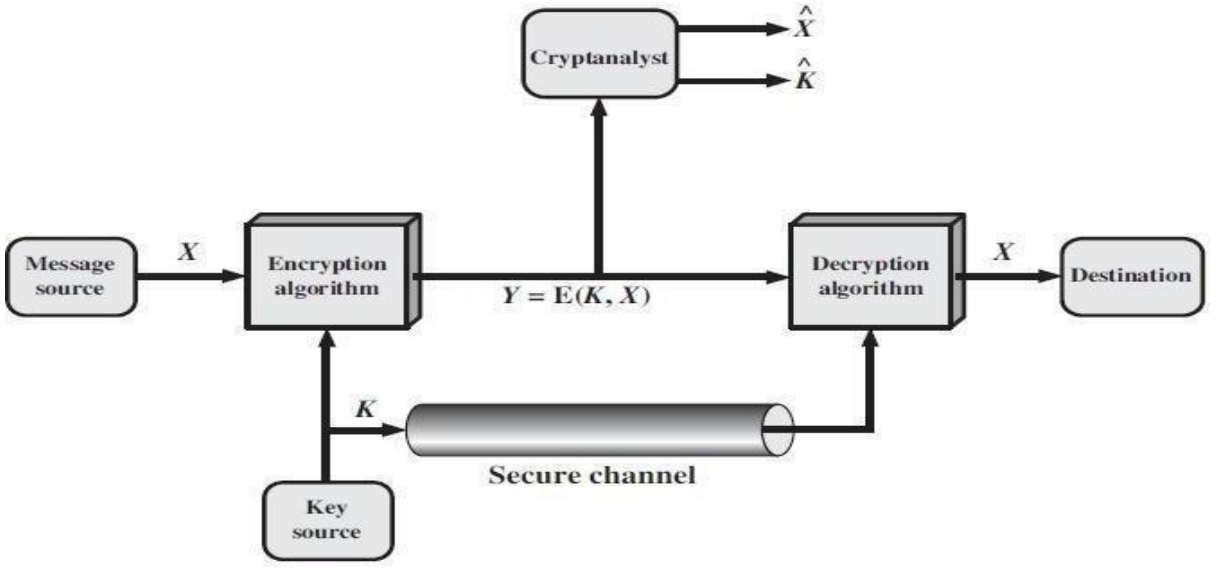


Figure 2.1 Simplified Model of Symmetric Encryption

Model of Conventional Cryptosystem

A source produces a message in plaintext, X = [X1, X2, ..., XM]. The M elements of X are letters in some finite alphabet. Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used. For encryption, a key of the formK = [K1, K2, ..., KJ] is generated. If the key is generated at the message source, then it must alsobe provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.



- With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y = [Y1, Y2, ..., YN]. We can write this as **Y = E(K, X).** This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K
- The intended receiver, in possession of the key, is able to invert the transformation: **X = D(K, Y)**.
- An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover X by generating a plaintext estimate.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

- **The type of operations used for transforming plaintext to cipher text.** All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.
- **The number of keys used.** If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
- **The way in which the plaintext is processed.** A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis and Brute-Force Attack

Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–cipher text pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Brute-force attack: The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

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 • 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 • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

1.5.2 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 cipher text bit patterns

1. Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. 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

Note that the alphabet is wrapped around, so that the letter following Z is A.

plain: 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

cipher: 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

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

For each plaintext P substitute the ciphertext letter C

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

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

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

where takes on a value in the range 1 to 25.The decryption algorithm is simply

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

Three important characteristics of this problem enabled us to use a brute force cryptanalysis:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable.

Cryptanalysis of Caesar Cipher

- ✓ only have 26 possible ciphers
- ✓ A maps to A,B,..Z
- ✓ Could simply try each in turn
- ✓ A brute force search
- ✓ Given cipher text, just try all shifts of letters
- ✓ Do need to recognize when have plaintext

Exercise:
Plain Text : civil engineering
Key : 7
Cipher Text : ?

Cipher Text : RTXYFRFENSLUJWXTSGFPMJNX
Key : 5
Plain Text : ?

2. 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. A **permutation** of a finite set of elements is an ordered sequence of all the elements of, with each element appearing exactly once. For example, if

S ={a,b,c} , there are six permutations of :abc, acb, bac, bca, cab, cba

In general, there are n! permutations of a set of elements, because the first element can be chosen in one of *n* ways, the second in n-1 ways, the third in n-2 ways, and so on.

Recall the assignment for the Caesar cipher:

plain: a b c d e f g h I j kl m n o p q r s t u v w x y z

cipher: 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

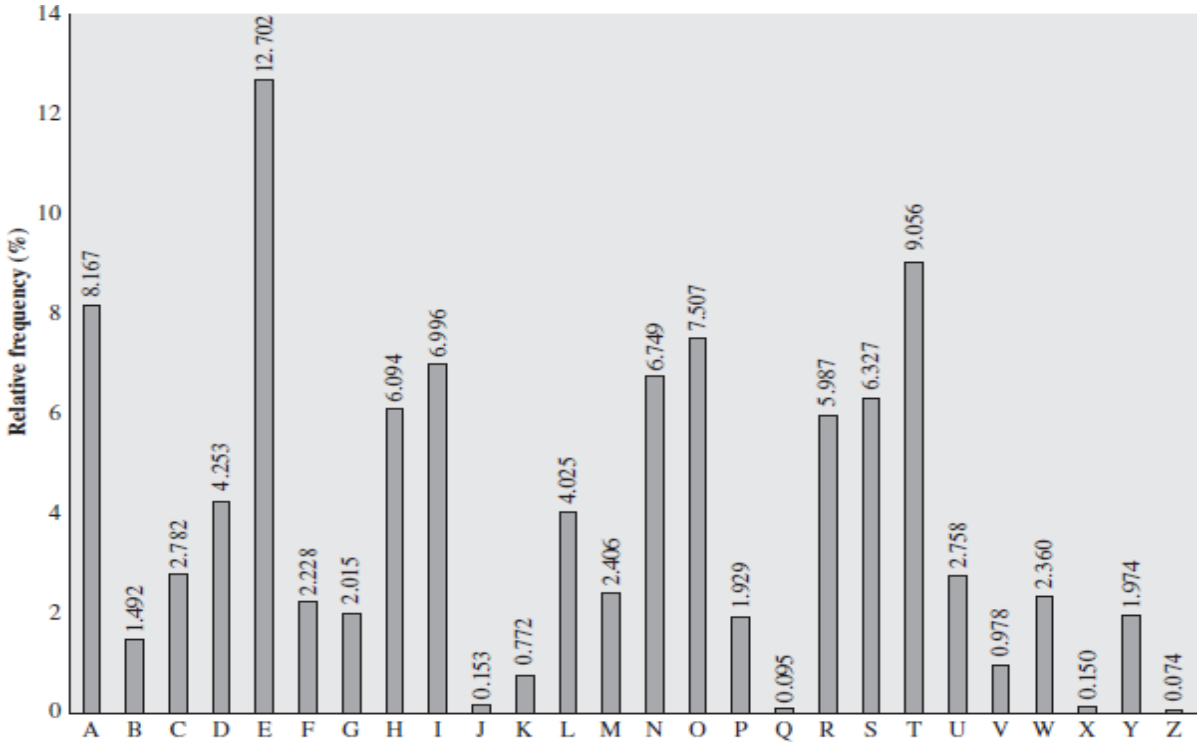
If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than $4*10^{26}$ possible keys. This is 10 orders of magnitude greater than the key space for DES and would seem to eliminate brute-force techniques for cryptanalysis. Such an approach is referred to as a **monoalphabetic substitution cipher**, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

The ciphertext to be solved is

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

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 Figure. If the message were long enough, thistechnique alone might be sufficient, but because this is a relatively short message, we cannot expect an exact match. In any case, the relative frequencies of the letters in the cipher text (in percentages) are as follows:

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				



Relative Frequencies of Letters in EnglishText

That 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 notice that the sequence ZWP appears in the ciphertext, and we can translate that sequence as "the." This is the most frequent trigram (three- letter combination). Next, notice the sequence ZWSZ in the first line. We do not know that these four letters form a complete word, but if they do, it is of the form th_t. If so, S equates with a.

So far, then, we have

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a       a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee  a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

Only four letters have been identified, but already we have quite a bit of the message. Continued analysis of frequencies plus trial and error should easily yield a solution from this point. The complete plaintext, with spaces added between words, follows:

it was disclosed yesterday that several informal butdirect contacts have been made with political representatives of theviet 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.

3. Playfair Cipher

- The best-known multiple-letter encryption cipher is the Playfair.
- The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword.
- **Playfair Key Matrix**
  - 5 × 5 matrix of letters constructed using a keyword
  - filling in the letters of the keyword (minus duplicates) from left to right and from top tobottom
  - filling in the remainder matrix with the remaining letters in alphabetic order.
  - The letters I and J count as one letter

- **Example matrix using the keyword MONARCHY**

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

In this case, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count asone letter. **Plaintext is encrypted two letters at a time, according to the following rules**

1. 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.
2. 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.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, withthe top element of the column circularly following the last. For example, mu is encrypted as CM.
4. 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 / JM.

Exercise:

Plain Text : civil engineeringKey : abishek
Cipher Text : ?
Note: The letters M and N count as one letter

Example: Given the key MONARCHY apply Play fair cipher to plain text "FACTIONALISM"

Solution

(p) FA CT IO NA LI SM
(c) IO DL FA AR SE LA
(d) FA CT IO NA LI SM

Security of Playfair Cipher

- Security much improved over monoalphabetic since have 26 x 26 = 676 digrams
- Would need a 676 entry frequency table to analyse and correspondingly more ciphertext
- It was widely used for many years eg. by US & British military in WW1.
- It can be broken, given a few hundred letters since still has much of plaintext structure

4. Hill Cipher

- Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929.
- This encryption algorithm takes successive M plaintext letters and substitutes for them M ciphertext letters.
- The substitution is determined by linear equations in which each character is assigned a numerical value (a=0, b=1, c=2, , z=25). For M=3, the system can be described as
- **C** = **PK** mod 26

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$$
$$(c_1\ c_2\ c_3) = (p\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

- where **C** and **P** are row vectors of length 3 representing the plaintext and ciphertext, and **K** is a 3 * 3 matrixrepresenting the encryption key. Operations are performed mod 26.

Example:

Plain Text : paymoremoney

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the Plain Text are represented by

$$\begin{vmatrix} 15 \\ 0 \\ 24 \end{vmatrix} \text{ then, } K \begin{vmatrix} 15 \\ 0 \\ 24 \end{vmatrix} = \begin{vmatrix} 375 \\ 879 \\ 486 \end{vmatrix} \text{ mod26 } = \begin{vmatrix} 11 \\ 13 \\ 18 \end{vmatrix} = \text{ LNS}$$

Cipher Text : LNSHDLEWMTRW

Exercise:

Plain Text : FINALYEAR

$$\begin{vmatrix} 2 & 5 & 3 \\ 3 & 1 & 4 \\ 9 & 7 & 6 \end{vmatrix}$$ Key :

Cipher Text : ?

Cipher Text : XAJOCVDAIUSGDAAUPIAGDGCSGDHAFQGSXI

Example

Encrypt the message “meet me at the usual place at ten rather than eight oclock” using the Hillcipher with the key ( ). Show your calculations and the result.Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

1) mathematically give each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2) 1st pair from plain text "me" => $\begin{pmatrix}12\\4\end{pmatrix}$

$$\begin{pmatrix}9 & 4\\5 & 7\end{pmatrix}\begin{pmatrix}12\\4\end{pmatrix} => \begin{pmatrix}9x12+4x4\\5x12+7x4\end{pmatrix} = \begin{pmatrix}124\\88\end{pmatrix} => mod\ 26 => \begin{pmatrix}20\\10\end{pmatrix} => \begin{pmatrix}u\\k\end{pmatrix}$$

3) 2nd pair fro plain text "et"

$$\begin{pmatrix}9 & 4\\5 & 7\end{pmatrix}\begin{pmatrix}4\\19\end{pmatrix} => \begin{pmatrix}9x4+4x19\\5x4+7x19\end{pmatrix} = \begin{pmatrix}112\\153\end{pmatrix} => mod\ 26 => \begin{pmatrix}8\\23\end{pmatrix} => \begin{pmatrix}i\\x\end{pmatrix}$$

4) Cipher text for "meet" is "ukix"

5) To get plain text from cipher text, we need to find the inverse of K

6) |A| = (9x7 – 5x4) => 43

7) Adj (A) => $\begin{pmatrix}7 & -4\\-5 & 9\end{pmatrix}$ => $\frac{1}{43}\begin{pmatrix}7 & -4\\-5 & 9\end{pmatrix}$ => $\frac{1}{17}\begin{pmatrix}7 & -4\\-5 & 9\end{pmatrix}$ ($\because 43\ \%\ 26 = 17$)

8) Find the multiplier for 17, using 17 x X = 1 mod 26 => X = 23

9) $\begin{pmatrix}161 & -92\\-115 & 207\end{pmatrix} => mod\ 26 => \begin{pmatrix}5 & -14\\-11 & 25\end{pmatrix} => \begin{pmatrix}\mathbf{5} & \mathbf{12}\\\mathbf{15} & \mathbf{25}\end{pmatrix}$ ($\because Add\ 26\ for - ive\ values$)

10) P = CK^{-1} = > For the ciper text of "uk",

$$\begin{pmatrix}5 & 12\\15 & 25\end{pmatrix}\begin{pmatrix}20\\10\end{pmatrix} = \begin{pmatrix}5x20+12x10\\15x20+25x10\end{pmatrix} => \begin{pmatrix}220\\550\end{pmatrix} mod\ 26 => \begin{pmatrix}12\\4\end{pmatrix} = \begin{pmatrix}m\\e\end{pmatrix}$$

Hence the plain text is “me”

5. Polyalphabetic Ciphers

- Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message.
- The general name for this approach is **polyalphabetic substitution cipher**. All these techniques have the following features incommon:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

VIGEN`ERE CIPHER

- The best known, and one of the simplest, polyalphabetic ciphers is the Vigenèrecipher.
- In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Each cipher is denoted by a key letter, which is the cipher text letter that substitutes for the plaintext letter a. Thus, a Caesar cipher with a shift of 3 is denoted by the key value.
- express the Vigenère cipher in the following manner. Assume a sequence of plaintext letters and a key consisting of the sequence of letters, where typically < .The sequence of ciphertext letters is calculated as follows

$$\begin{aligned} C = C_0, C_1, C_2, \ldots, C_{n-1} &= \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, \ldots, k_{m-1}), (p_0, p_1, p_2, \ldots, p_{n-1})] \\ &= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \ldots, (p_{m-1} + k_{m-1}) \bmod 26, \\ &\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \ldots, (p_{2m-1} + k_{m-1}) \bmod 26, \ldots \end{aligned}$$

- Thus, the first letter of the key is added to the first letter of the plaintext, mod 26, the second letters are added, and so on through the first letters of the plaintext. For the next letters of the plaintext, the key letters are repeated. This process continues until all of the plaintext sequence is encrypted. A general equation of the encryption process is

$$Ci = (pi + ki \bmod m) \bmod 26$$

Decryption is a generalization of Equation

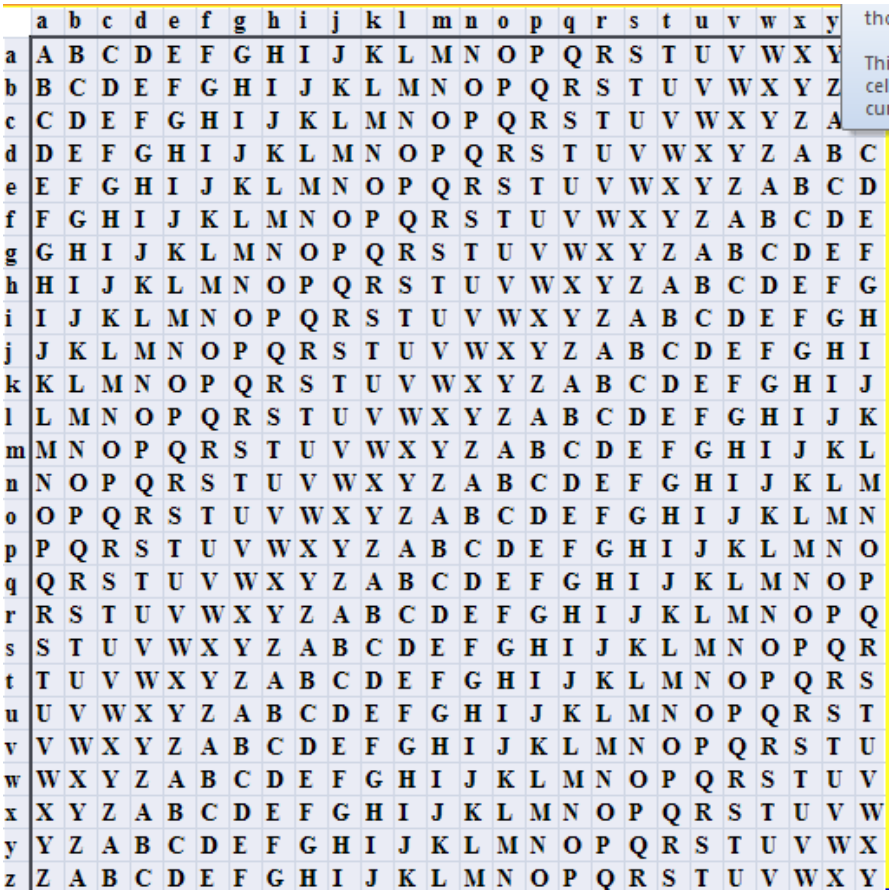
$$pi = (Ci - ki \bmod m) \bmod 26$$

- To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ



	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
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
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
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
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 Table Note : Rows represents Plaintext and Columns represents the Key

keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself.Vigenèreproposed what is referred to as an **autokey system**, in which a keyword is concatenated with the plaintextitself to provide a running key. For our example,

key:deceptivewearediscoveredsav plaintext:wearediscoveredsaveyourself

ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA

Exercise:

Plaintext : cryptography and network securityKey : sectionb

Ciphertext : ?

6. One Time Pad Cipher (or) Vernam Cipher

It is an unbreakable cryptosystem, described by Frank Miller in 1882, the one-time pad was reinvented by Gilbert Vernam in 1917 and it was later improved by the US Amry Major Joseph. It represents the message as a sequence of 0s and 1s. This can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0‟s and 1‟s of same length as the message.

Once a key is used, it is discarded and never used again. The system can be expressed as follows:

$$C_i = P_i \oplus K_i$$

C_i - i^{th} binary digit of cipher text

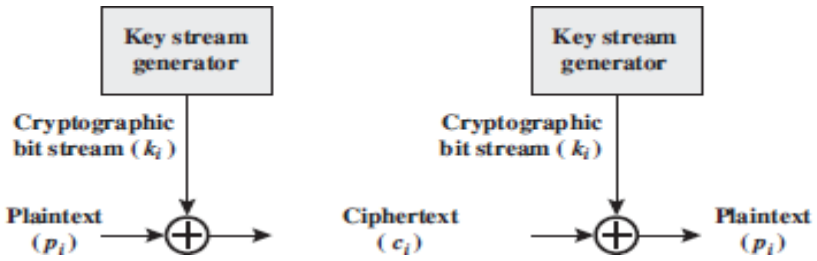
P_i - i^{th} binary digit of plaintext

K_i - i^{th} binary digit of key

$\oplus$ – exclusive OR opearaiton

Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus K_i$$



Example

Alice wishes to send the message “HELLO” to Bob. If key material begins with “XMCKL” and the message is “HELLO”, then use Vernam One Time Pad to Decrypt and Show the Encryption Process.

MESSAGE	H	E	L	L	O
POSITION	7	4	11	11	14

KEY	X	M	C	K	L
POSITION	23	12	2	10	11

OTP Encryption

H	E	L	L	O	Message
7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	Message

		)			
23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	Key

30	16	13	21	25	Message + Key
4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	Message + Key (mod 26)
E	Q	N	V	Z	Ciphertext

Note: If a number is larger than 25, then the remainder afer subtraction of 26 is taken in ModularArithmeticfashion

OTP Decryption

E	Q	N	V	Z	Ciphertext
4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	Ciphertext
23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	Key
-19	4	11	11	14	Ciphertext - Key
7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	Ciphertext - Key (mod 26)
H	E	L	L	O	Message

Note: If a number is negative then 26 is added to make the number positive

Example

Encryption

Plaintext is 00101001 and the key is 10101100, we obtain the ciphertext is,

Plaintext	00101001
Key	10101100
Ciphertext	10000101

Decryption

Ciphertext	10000101
Key	10101100
Plaintext	00101001

Advantages

- Encryption method is completely unbreakable for a cipher-text only known attack
- Chosen Plaintext (or) Ciphertext attacks is not possible

Disadvantages

- It requires a very long key which is expensive to produce and expensive to transmit.
- Once a key is used it is dangerous to reuse it for second message.

1.5.3 Transposition techniques:

A very different kind of mapping is achieved by performing some sort of permutation on theplaintext letters

1. Rail Fence Technique

All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher. The simplest such cipher is the **rail fence** technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

The encrypted message is **MEMATRHTGPRYETEFETEOAAT**

2. Pure Transposition Cipher

Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

The order of the columns then becomes the key to the algorithm

Example

```
K     4   3   1  2       7
e                5
y                6
:
```

Plaintext: a t t a c k p

o s t p o n e du n t i l t w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

i. Double Transposition

performing more than one stage of transposition

Example :if the foregoing message is reencrypted using the same algorithm

Key: 4 3 1 2 5 6 7

Input :

t t a
n a
p
t
m t s u o
a
o
d w c o i k
x
n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

1.5.4 Steganography

A plaintext message may be hidden in one of two ways.

- The methods of steganography conceal the existence of the message
- The methods of cryptography render the message unintelligible to outsiders by various transformations of the text

Various ways to conceal the message

Arrangement of words or letters within an apparently innocuous text spells out the real message

Character marking

Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Invisible ink

A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied

Pin punctures

Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon

Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Hiding a message by using the least significant bits of frames on a CD

- The Kodak Photo CD format's maximum resolution is 2048 by 3072 pixels, with each pixel containing 24 bits of RGB color information.
- The least significant bit of each 24-bit pixel can be changed without greatly affecting the quality of the image
- Thus you can hide a 2.3-megabyte message in a single digital snapshot

Number of drawbacks

- lot of overhead to hide a relatively few bits of information
- once the system is discovered, it becomes virtually worthless
- the insertion method depends on some sort of key
- Alternatively, a message can be first encrypted and then hidden using steganography

Advantage of steganography

- Can be employed by parties who have something to lose should the fact of their secret communication be discovered
- Encryption flags traffic as important or secret or may identify the sender or receiver assomeone with something to hide

1.6 FOUNDATIONS OF MODERN CRYPTOGRAPHY

Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational- complexity theory, and probability theory.

Characteristics of Modern Cryptography

There are three major characteristics that separate modern cryptography from the classicalapproach.

Classic Cryptography	Modern Cryptography
It manipulates traditional characters, i.e., lettersand digits directly.	It operates on binary bit sequences.
It is mainly based on 'security through obscurity'. The techniques employed for coding were kept secret and only the parties involved in communication knew about them.	It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.
It requires the entire cryptosystem for communicating confidentially.	Modern cryptography requires parties interested in secure communication to possess the secret keyonly.

1.6.1 Perfect security

- The effort one has to put in for cryptanalysis is a measure of strengrh or weakness of a cryptosystem.
- Issues:
  - Same encryption / decryption process is repeatedly used.
  - Cipher text (or) crypto text provides enough clues to identify plain text and encryption algorithm.
  - To carry out cryptanalysis the availability of plain text and cipher text is easily available. To avoid this encryption process is made more and more efficient.
- Let m,k,c be discrete random variables and M,K,C be values of random variables.
- A Crypto system with m,k,c,M,K,C asdefined is perfectly secure if and only if

$P(m/c)=P(m) \longrightarrow$ **eq1**

By Bayes Theorem

$P(m/c)=P(c/m)P(m) \ / \ P(c) \longrightarrow$ **eq2**

Eq1 becomes

$P(c/m)=P(\ c) \longrightarrow$ **eq3**

Hence perfect security implies that knowledge of m should not apply any difference to P(c)

either.

Shannon's Theorem:

For the specific case |M|=|K|=|C| shannon gave the important results.

1. For every m€M and c€C there is unique key k€K.
2. The scheme has perfect security if and only id every one of the keys is used with equal probability.

Consider c=c1,m=m1,keys k_i&k_j

$D(k_i(c1))=D(k_j(c1))=m1$

Assume keys k_1,k_2,k_3…..then

$D(k_1(c1))=m1$

$D(k_2(c2))=m2$

Consider

$P(m_i/c_1) = P(c_1/m_i)P(m_i) / P(c_1)$

$= P(c_1)P(m_i)/P(c_1)$ ⟶ from eq3

$P(m_i/c_i)=P(m_i)$

Also $P(c_1/m_i)$➔$p(k=k_i)$

This implies all key are to be used with equal probability

Example: Find the probability of crypto text .

Table 1: Encryption/ Decryption rules.

	M1	M2	M3	M4
K1	C1	C2	C3	C4
K2	C5	C4	C2	C1
K3	C4	C1	C2	C3

Table 2: Probability of message

Message	M1	M2	M3	M4
Probability	0.1	0.2	0.3	0.4

Table 3: Probability of keys

Key	K1	K2	K3
Probability	0.2	0.3	0.5

Solution:

P(C1) = P(M1K1)+P(M2K3)+P(M4K2)

= (0.1*0.2)+(0.4*0.3)+(0.2*0.5)

= 0.02+0.12+0.1

=0.24

Cryptotext	C1	C2	C3	C4	C5
Probability	0.24	0.28	0.26	0.19	0.03

1.6.2 Information Theory

- Consider an experiment with a number of possible outcomes.
- Outcome is called as Event.
- Let x be outcome and x_i be possible values of outcome.
- Before experiment is conducted the outcome of the event is unknown.
- Entropy is a measure of information content in x.
- Possible outcomes are$\{x_1,x_2 \ldots x_n\}$ and their probability be $\{p_1,p_2 \ldots p_n\}$.
- The quantity $\{-\log_2 p_i\}$ be the information content of x_i.
- The quantity $\{-P_i \log_2 P_i\}$ represents the contribution of x_i to the total information content or entropy.
- Total entropy:

$$H(x) = -\sum_{i=1}^{n} P_i \log_2 P_i$$

Example:

Assume let x be 3 bit number for 0 to 7.Then possible values are 000,001,010,011,100,101,110,111. Therefore the probability outcome is 1/8.Let us assume the information we received for the bit **b2b1b0** is **110**.we have partial information about event say b2=1.

Solution:

- ✓ This information has resolved some level of uncertainty by reducing possible outcome from 8 to 4. (say 100,101,110,111).
- ✓ There is **50%** reduction in uncertainty.
- ✓ If we assume b0=0, then uncertainty is **25%.**
- ✓ We know answer by 75%. This is how information theory works.

1.6.3 Product Cryptosystem

- Two of the first kinds of cryptosystems that we considered were simple substitution ciphers andpermutation ciphers.
- Each of them quickly proved vulnerable to attack.
- We now consider a newkind of cryptosystem that is based on them but which is considerably more difficult to attack
- A product cryptosystem is a block cipher that repeatedly performs substitutions and permutations, one afterthe other, to produce cipher text.

Example : DES and AES (Brief description in Unit II)

1.6.4 Cryptanalysis.

- Cryptanalysis is the science of cracking codes and decoding secrets.
- It is used to violate authentication schemes, to break cryptographic protocols, and, more benignly, to find and correct weaknesses in encryption algorithms.
- It may be used in information warfare applications - for example, forging an encrypted signal to be accepted as authentic.
- Competitors who have been able to discover the key will now want to use it to their advantage, therefore they will want to send bogus encrypted messages to the source in order to gain information or gain an advantage.
- It could also be used to pretend to be the source in order to send bogus information to others, who now will think that it came from the official source.

- **According to Diffie and Hellman -** Skill in the production of cryptanalysis has always been heavily on the side of the professionals, but innovation, particularly in the design of new types of cryptographic systems, has come primarily from amateurs.

- **Among the types of attacks are:**

    - Ciphertext only attacks
    - Known plaintext attacks
    - Chosen plaintext attacks
    - Chosen ciphertext attacks
    - Man-in-the-middle attacks
    - Side channel attacks

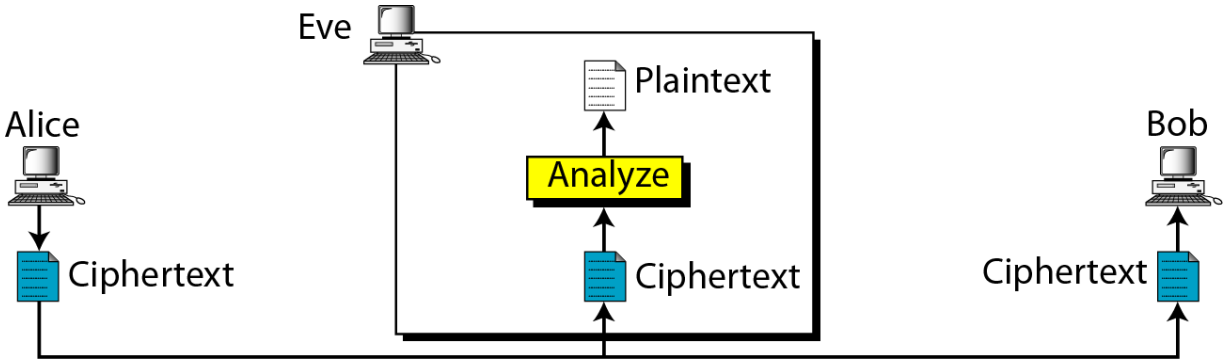
- Brute force attacks
- Birthday attacks

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 • 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 • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

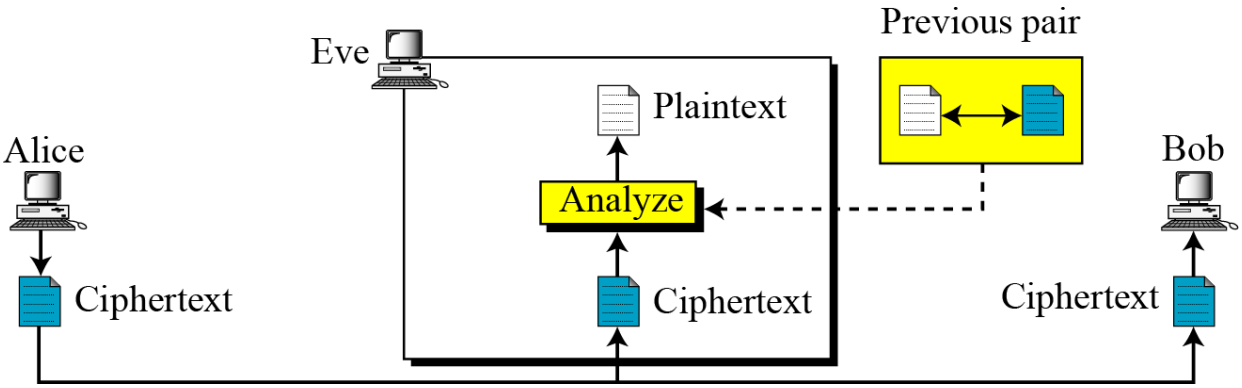
Ciphertext Only

A ciphertext only attack (COA) is a case in which only the encrypted message is available for attack, but because the language is known a frequency analysis could be attempted. In this situation the attacker does not know anything about the contents of the message, and must work from ciphertext only.



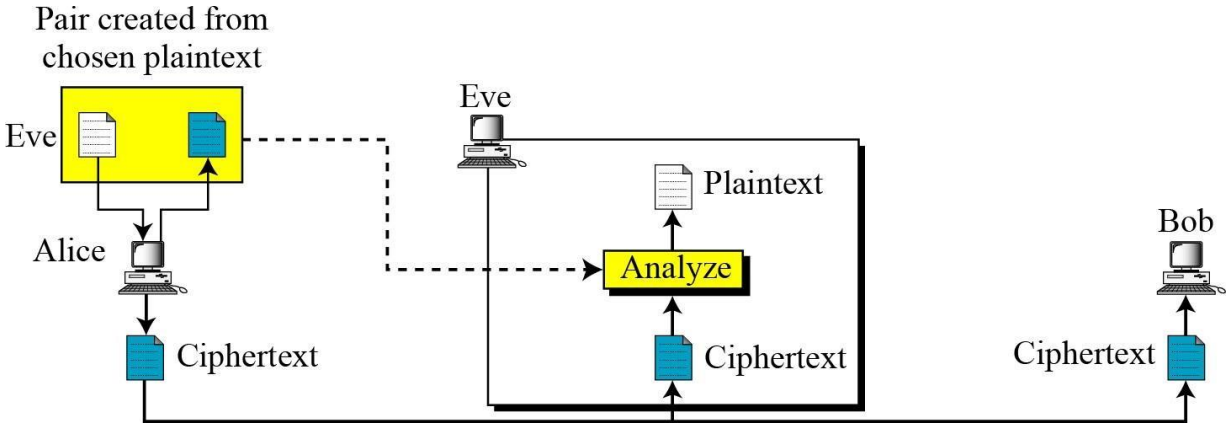
Plaintext Attack

In a known plaintext attack (KPA) both the plaintext and matching ciphertext are available for use in discovering the key.The attacker knows or can guess the plaintext for some parts of the ciphertext. For example, maybe all secure login sessions begin with the characters LOGIN, and the next transmission may be PASSWORD. The task is to decrypt the rest of the ciphertext blocks using this information.This may be done by determining the key used to encrypt the data, or via some shortcut.



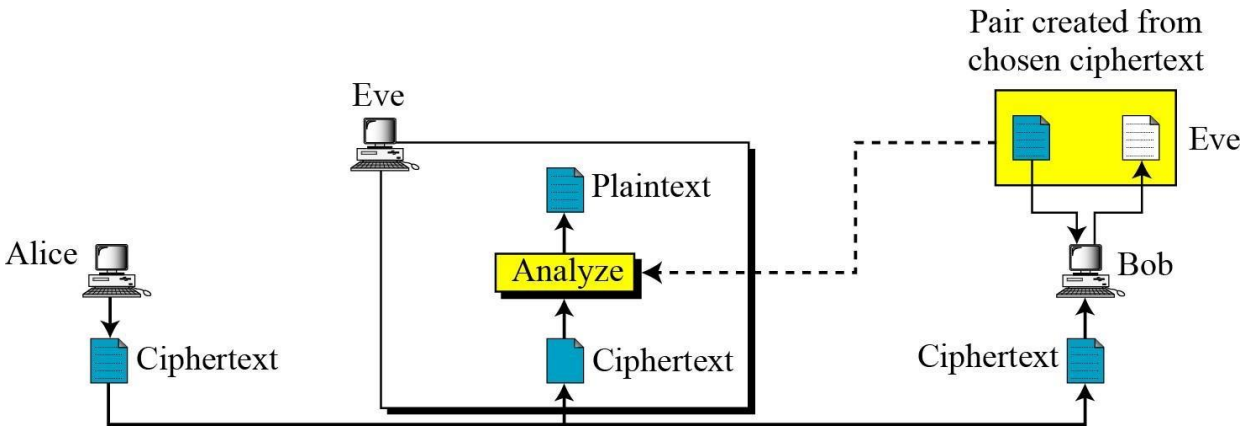
Chosen Plaintext Attack

A chosen plaintext attack (CPA) occurs when the attacker gains access to the target encryption device - if, for example, it is left unattended. The attacker then runs various pieces of plaintext though the device for encryption. This is compared to the plaintext to attempt to derive the key.In an adaptive chosen plaintext attack (ACPA), the attacker not only has access to the plaintext and its encryption, but can adapt or modify the chosen plaintext as needed based on results of theprevious encryptions.



Chosen Ciphertext Attack

In a chosen ciphertext attack (CCA), the cryptanalyst can choose different ciphertexts to bedecrypted and has access to the decrypted plaintext.This type of attack is generally applicable to attacks against public key cryptosystems.An adaptive chosen ciphertext attack involves the attacker selecting certain ciphertexts to be decrypted, then using the results of these decryptions to select subsequent ciphertexts. The modifications in the ciphertext help in deciphering the key from the decryptions.



Brute-force attack: The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.