CB3491- CRYPTOGRAPHY AND CYBER SECURITY

UNIT I INTRODUCTION TO SECURITY

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

Introduction to Cryptography

Cryptography is derived from the Greek word “Kryptos” which mean “Hidden secrets” It is the practice and study of hiding information which is used to keep information Secret and safe.

Example: Julyes Caeser

Cryptography

- The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

Why Cryptography?

- Cryptography can reformat and transform our data, making it safer on its trip between computers.
- The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

Basic Terms in Cryptography

- **Plaintext** The original intelligible message
- **Cipher text** The transformed message
- **Cipher** An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.
- **Key** Some critical information used by the cipher, known only to the sender& receiver

- **Encipher** (encode) -The process of converting plaintext to cipher text using a cipher and a key
- **Decipher** (decode) the process of converting cipher text back into plaintext using a cipher and a key
- **Cryptanalysis** The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking

Cryptology Both cryptography and cryptanalysis

Network security

- Network security is any action an organization takes to prevent malicious use or accidental damage to the network's private data, its users, or their devices.
- The **goal** of network security is to keep the network running and **safe for all legitimate users.**
- **Network security** consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources
- There are so many ways that a network can be vulnerable.
- Hackers, leave private data exposed, including trade secrets and customers' private details.
- But attackers can do more than steal data
- Competent network security procedures keep data secure and block vulnerable systems from outside interference.

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- **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 networksour focus is on
- **Internet Security** which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information

OSI SECURITY ARCHITECTURE:

Its a sort of standard which was proposed by ITU-T, ITU stands for ie International Telecommunication unit and T is one of the sector of this telecommunication unit. X.800, is a standard that specifies s*ecurity Architecture for OSI.* OSI security architecture is simply a standard, which provides various services, requirements, mechanisms and attacks that helps the managers, industries, computer communication vendors, in such a way, that they can develop the security features for their products and services based on the definition of services and mechanisms of OSI.

Security architecture for OSI describes network security in 3 aspects.

- **Security attack**
- **Security service**
- **Security Mechanism**

- **Security attack** – Any action that compromises the security of information owned by an organization.
- **Security mechanism** – A mechanism that is designed to detect, prevent or recover from asecurity attack.
- **Security service** – A 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.

SECURITY ATTACKS

- Any action that compromises the security of information owned by an organization information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems often threat & attack used to mean same thing have a wide range of attacks

SECURITY ATTACKS

-Interruption
-Interception
-Modification
-Fabrication

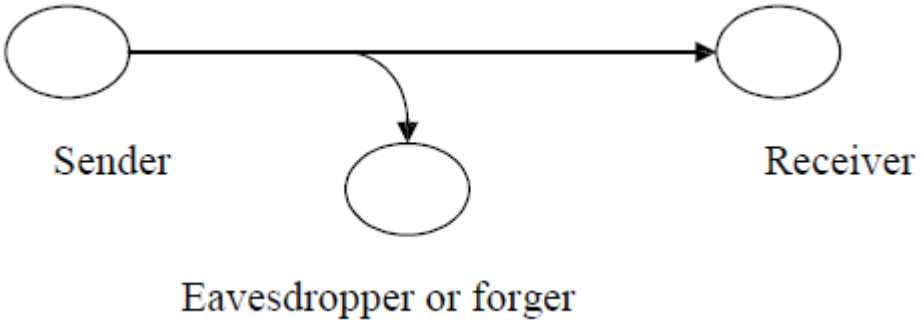
Interruption

- An asset of the system is destroyed or becomes unavailable or unusable.
- This is an attack on **availability**
- e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

Interception

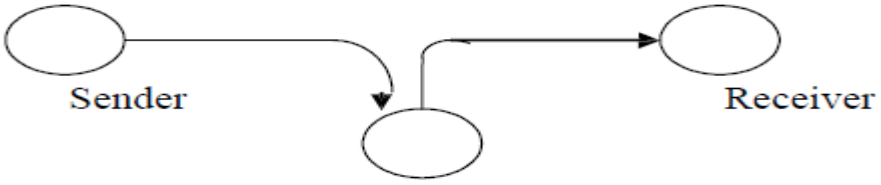
- An unauthorized party gains access to an asset.

- This is an attack on **confidentiality.**
- Unauthorized party could be a person, a program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files



Modification

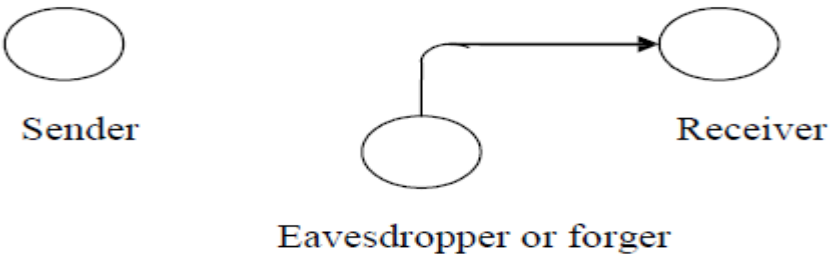
- An unauthorized party not only gains access to but tampers with an asset.
- This is an attack on **integrity**. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



Fabrication

- An unauthorized party inserts counterfeit objects into the system.
- This is an attack on **authenticity.**

e.g., insertion of spurious message in a network or addition



Cryptographic Attacks

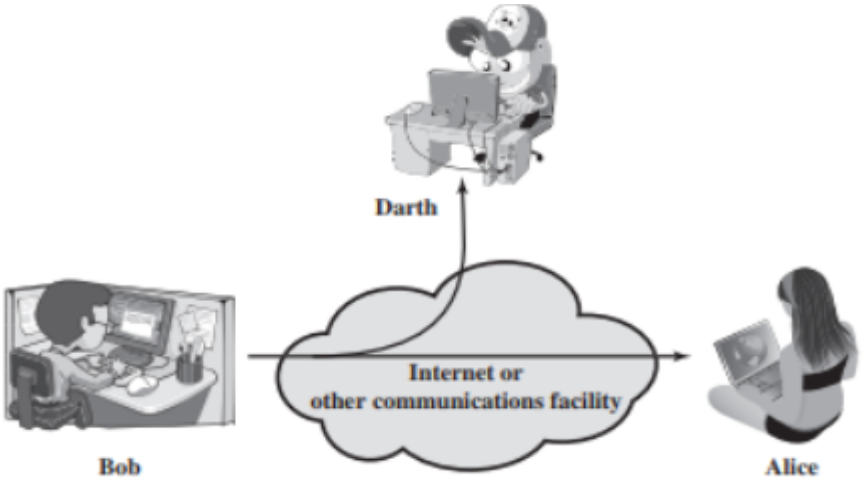
- **Passive Attacks**
- **Active attacks**

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.

Passive attacks are of two types:

- **Release of message contents**
- **Traffic analysis**



a. Passive attacks

Release of message contents

- A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.
- We would like to prevent the opponent from learning the contents of these transmissions.

Traffic analysis

- If we had encryption protection in place, an opponent might still be able to observe the pattern of the message.
- The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of communication that was taking place.

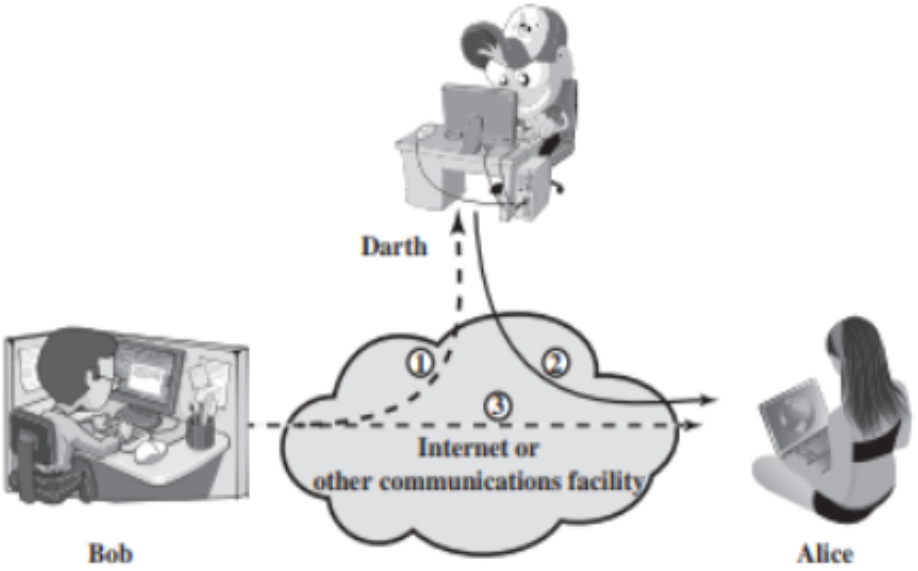
Passive attacks are very difficult to detect because they do not involve any alteration of data

Active attacks

- These attacks involve some modification of the data stream or the creation of a false stream.

These attacks can be classified in to four categories:

- **Masquerade**
- **Replay**
- **Modification of messages**
- **Denial of service**



(b) Active attacks

Masquerade

Masquerade is caused when an unauthorized entity pretends to be another entity. To clear this lets have an example. Alice and Bob are legal and legitimate users. Here comes the Tom and he masquerades or disguises himself as Alice and communicate with Bob on behalf of Alice. Now due to poor lack of authentication by chance Bob releases some confidential information like acc no and password.so that tom get access to those credentials again tom is going to get rich.

Replay

In replay attacks user captures a sequence of events or some data units and resends them. Lets have a look how replay attack work. Here we can see 3 entities Alice,Tom and Bank. Now Alice want to transfer 100$ to Tom.She initiates the transaction with the bank.Tom captures ths transaction and reinitiates another transaction in her name and this results in earning 200$.Here the bank doesn't know that the second transaction was initiated by Tom but not Alice.

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 (Figure 1.6c). For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file account.

Denial of service

- Prevents or inhibits the normal use or management of communication facilities.

  Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance

Security service

X.800 defines a security service which is implemented in a protocol layer so that it ensures adequate security of the systems or of data transfers.

Role of Network Security Services

- It enhance security of Data processing systems and information transforms of an organization
- It is mainly intended to **counter** security attacks

X.800 divides these services into five categories

- Authentication
- Access Control
- Availability
- Confidentiality
- Integrity
- Non-Repudiation

Authentication:

Authentication assures recipient that the message is from, the intended source .it identifies who is sender and who is receiver also it verifies whether the user is an authorized user.

It is categorized into two

Peer entity authentication

Data Origin Authentication

Peer entity authentication: used in association with a logical connection .It Verifies the identities of the peer entities involved in communication.ie both communication agent from source and destination .they can prove that we are the one communicating. Also it provides the confirmation of the identity of a peer entity in an association.

Data Origin Authentication:

Is useful where there is no connection. Provides the confirmation of the source of a data unit.

Access Control: access control is the ability to limit and control the access to host systems and applications via communications links. We need to ensure that only the authorized users are able to access the content. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be given to the individual.

Availability: Resources/applications must be available to authentic users all the time. For eg if I am logging in my account, I must be able to access my email services, my file services or even my network. And it is possible that someone can take out the connection, or can

delete some authenticated data or even destroy the system. This is called the denial of service attack. This must not happen. Resources must be made available to legitimate users.

Confidentiality: It states that only the sender and the receiver should have an access to the information. It is also known as privacy or secrecy of information.

Data Integrity: assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.

Non-Repudiation: 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.

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

Destination Nonrepudiation: Proof that the message was received by the specified party

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

Specific Security Mechanisms:

Incorporated into the appropriate protocol layer in order to provide some of the OSI security services, **Encipherment:** It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and encryption keys.

Digital Signature: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

Access Control: A variety of techniques used for enforcing access permissions to the system resources. **Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

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 once a breach of security is suspected.

Notarization: The use of a trusted third party to assure cert in properties of a data exchange

Pervasive Security Mechanisms

These are not specific to any particular OSI security service or protocol layer.

Trusted Functionality: That which is perceived to b correct with respect to some criteria

Security Level: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection: It is the process of detecting all the events related to network security.

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.

Security Recovery: It deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

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.	

Mechanism								
Service	**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			

A 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.

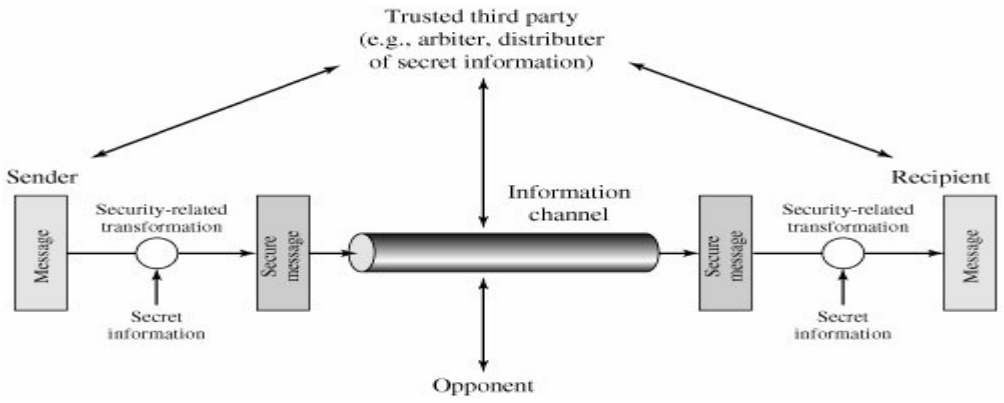


Figure 1.5. Model for Network Security

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. 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.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

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.

Network Access Security Model

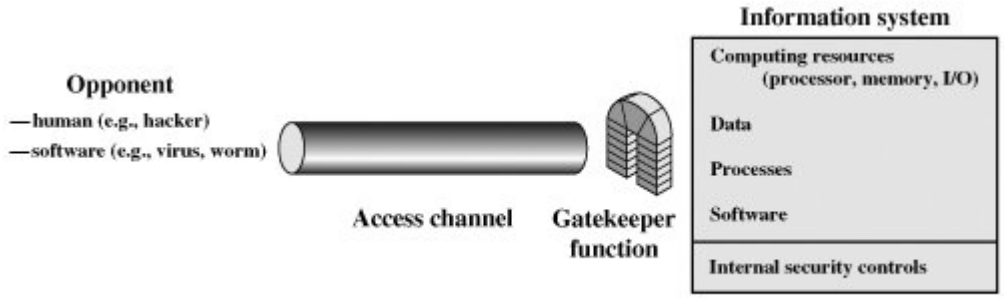


Fig:Network Access Security Model

In computer **security**, a **threat** is a potential negative action or event facilitated by a vulnerability that results in unwanted impact to a computer system or application.

Common Security Threats

- **Spam**.
- **Pharming**

- **Phishing**. ...
- Ransomware. ...
- **Computer worm**. ...
- **Spyware** / **Trojan Horse**. ...
- Distributed denial-of-service attack. ...

Another type attack is unwanted access 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. This type of attack is called software attack Programs can present two kinds of threats:

- **Information access threats** intercept or modify data on behalf of users who should not have access to that data.
- **Service threats** exploit service flaws in computers to inhibit/prevent use by legitimate users.

Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. For eg, A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.The security mechanisms needed to cope with unwanted access fall into two broad categories (see Figure 1.6).

The first category might be termed a **gatekeeper function**. It includes **password-based login procedures** that are designed to deny access to all but authorized users **and screening logic** that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Using this model requires us to:

– select appropriate gatekeeper functions to identify users

– implement security controls to ensure only authorized users access designated

information or resources

• **Trusted computer systems can be used to implement this model**

CLASSICAL ENCRYPTION TECHNIQUES

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 sys-tematically transpose the positions of plaintext elements.

Basic Terminologies:

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** or **encryption**;

Restoring the plain-text 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 enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is the art of breaking codes and ciphers Cryptanalysis is what the layperson calls “breaking the code.”

The areas of cryptography and cryptanalysis together are called **cryptology**.

SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has five ingredients (Figure 2.1):

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

• **Encryption algorithm:** The encryption algorithm performs various substitu-tions 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.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form:

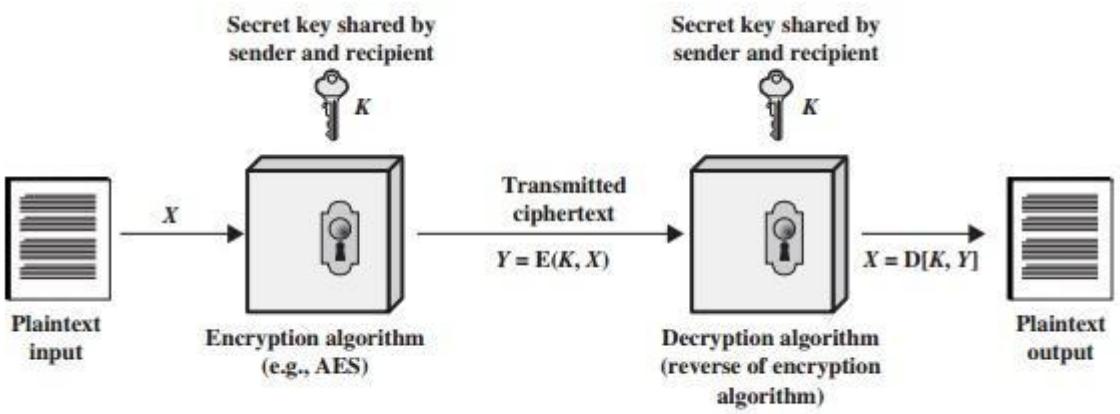


Figure 2.1 Simplified Model of Symmetric Encryption

2. The 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.

We assume that it is impractical to decrypt a message on the basis of the ciphertext *plus* knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret. This feature of symmetric encryption is what makes it feasible for widespread use. The fact that the algorithm need not be kept secret means that manufacturers can and have developed low-cost chip implementations of data encryption algorithms. These chips are widely available and incorporated into a number of products. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

Let us take a closer look at the essential elements of a symmetric encryp-tion scheme, using Figure 2.2. A source produces a message in plaintext, $X = [X_1, X_2, ... , X_M]$. 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 form $K = [K_1, K_2, ... , K_J]$ is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure chan-nel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

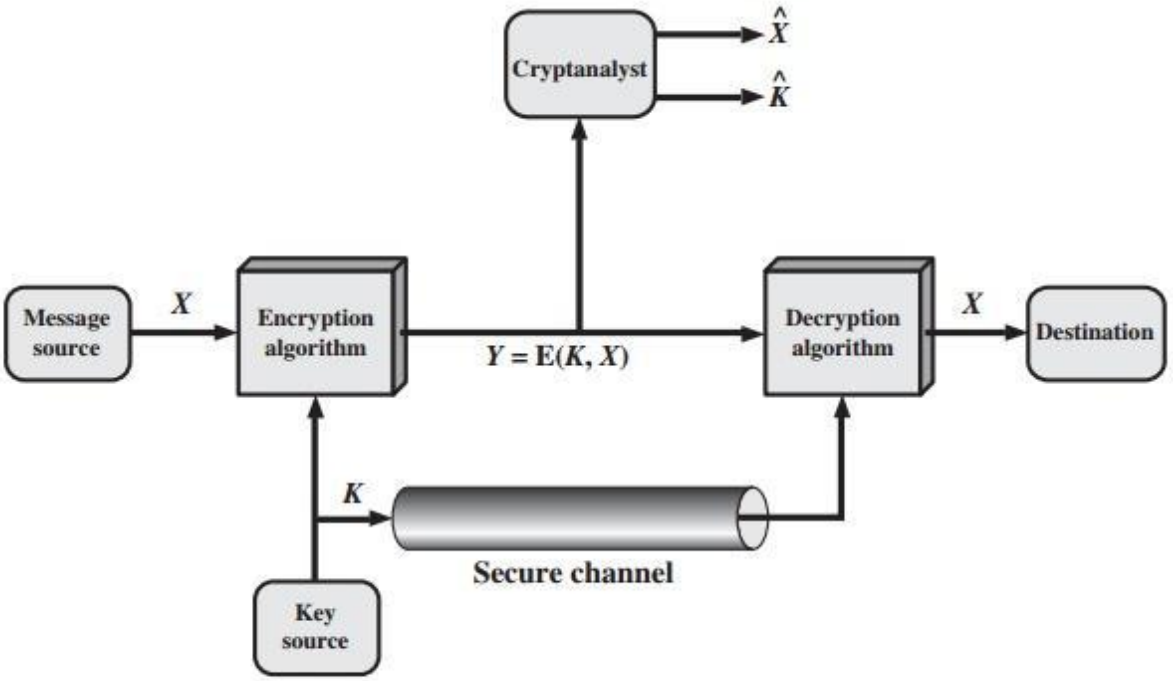


Figure 2.2 Model of Symmetric Cryptosystem

With the message X and the encryption key K as input, the encryption algo-rithm forms the ciphertext $Y = [Y_1, Y_2, ... , Y_N]$. 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 $X^{N.}$ Often, however, the opponent is interested in being able to read future messages as N well, in which case an attempt is made to recover K by generating an estimate K.

Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.** 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 informa-tion be lost (that is, that all operations are reversible). Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.
2. **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 encryp-tion. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
3. **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

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. There are two gen-eral approaches to attacking a conventional encryption scheme:

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–ciphertext 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. Cryptanalysis is the art of breaking codes and ciphers

- **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.

If either type of attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.

CLASSICAL ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques: substitution and transposition.

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. Substitution Techniques Falls in 7 categories

- Caesar Cipher or Shift Cipher
- Mono Alphabetic Cipher
- Playfair cipher
- Hill Cipher
- Vigenere Cipher
- Vernam Cipher
- One Time Pad Cipher

Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z‟ is „a‟.

For each plaintext letter p, substitute the cipher text letter c such that

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

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

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

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

Decryption: P = D(C) = (C-k) mod 26

Why Caesar Cipher is not Secure?

- It is a type of substitution **cipher** in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet
- The **Caesar cipher** offers essentially **no** communication security.
- It can be easily broken even by hand.

Monoalphabetic Cipher

- Arbitrary substitution is used
- It is based on the concept of permutation.
- If there are n elements then there are n! permutations i.e n(n-1)! Possibilities.
- Any cipher of 26 alphabetic characters, then there are 26! or greater than $4x10^{26}$ possible keys.

This approach is known as monoalphabetic substitution cipher because a single cipher alphabet is used per message

- Rather than just shifting the alphabet could shuffle (jumble) the letters arbitrarily.
- Each plaintext letter maps to a different random ciphertext letter
- Hence key is 26 letters long

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 k v q f i b j w p e s c x h t m y a u o l r g z n
Plaintext: i f w e w i s h t o r e p l a c e l e t t e r s
Ciphertext: w i r f r w a j u h y f t s d v f s f u u f y a

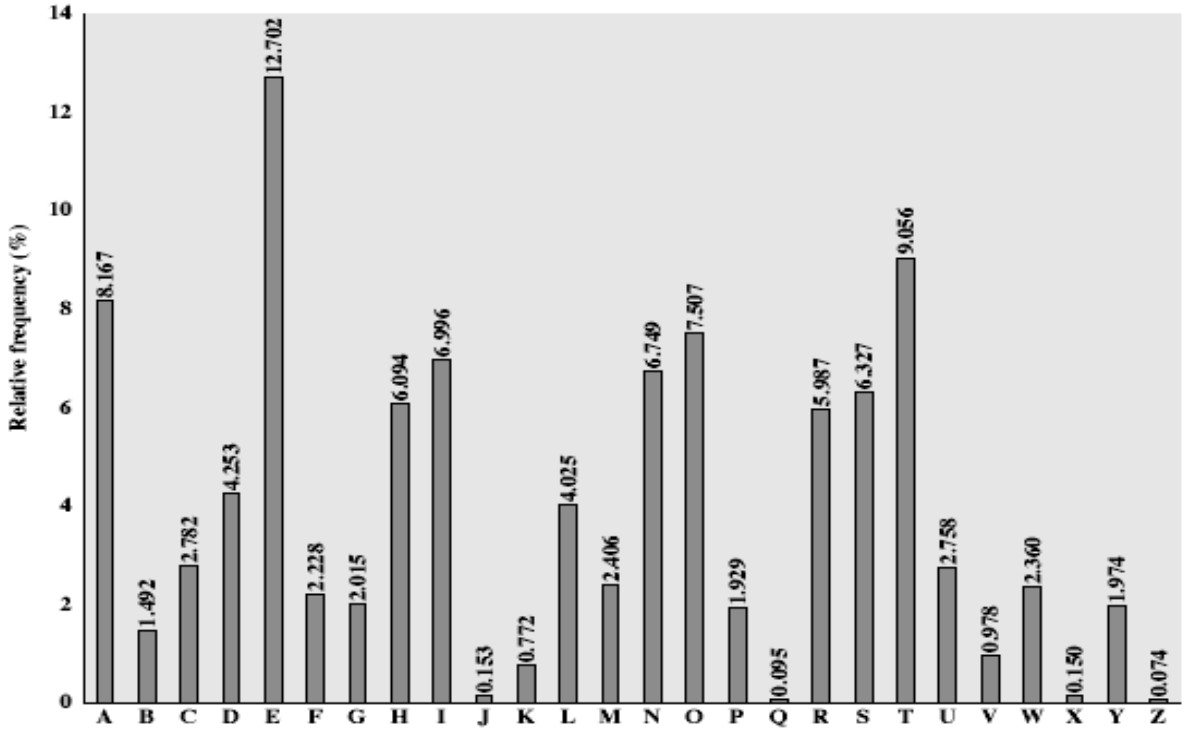
Problem of Monoalphabetic Cipher

- Given ciphertext:

UZQSOVUOHXMOPVGPOZPEVSG**ZW**SZOPFPESXUDBMETSXAIZVUEPHZHMDZS
HZOWSFPAPPDTSVPQU**ZW**YMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJ
UDTMOHMQ

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 1.9. If the message were long enough, this technique 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 ciphertext (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				



English Letter Frequencies

- Compare the relative frequency of letters with the standard distribution of English each letter can be replaced
- The Cipher text P and Z are the equivalents of plain letters e and t, but it is not sure.
- 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.

  Z W -> t h

  Z W **P** -> **t** h **e**

  Z W S Z -> t h a t

Playfair 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 cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „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 ofthe matrix with the remaining letters in alphabetical order.The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time

According to the following rules:

1. Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x".
2. 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 following the last.
3. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.

4. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

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

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Corresponding Plain text => ME ET ME AT TH ES CH O X OL HO US EX

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 cipher. All the techniques have the following features incommon. A set of related monoalphabetic substitution rules are used

A key determines which particular rule is chosen for a given transformation.

VIGENERE CIPHER

In this scheme, the set of related monoalphabetic substitution rules consisting of

26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesarcipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed.

	PLAIN TEXT															
KEY LETTERS		a	b	c	d	e	f	g	h	i	j	k	…	x	y	z
	a	A	B	C	D	E	F	G	H	I	J	K	…	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	…	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	…	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	…	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	…	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	…	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	…	D	E	F
	:	:	:	:	:	:	:	:	:	:	:	:	…	:	:	:
	x	X	Y	Z	A	B	C	D	E	F	G	H	…			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	…			X
	z	Z	A	B	C	D	E	F	G	H	I	J	…			Y

Figure:Vigenere Table

Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g., key = d e c e p t i v e d e c e p t i v e d e c e p t i v e

PT = w e a r e d i s c o v e r e d s av e y o u r s e l f

CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Expressed numerically, we have the following result.

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Decryption is equally simple. The key letter again identifies the row. The position of thecipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigenere cipher

o There are multiple cipher text letters for each plaintext letter.

o Letter frequency information is obscured

VERNAM CIPHER

- Key as long as and indepedent of the plaintext
- Works on binary data as opposed to letters
- Ci = Pi (XOR) Ki
- Where
  - Pi – ith binary digit of plaintext
  - Ki – ith digit of key
  - Ci – ith digit of ciphertext
  - Pi=Ci (XOR) Ki
- **Key needs to be long and random**

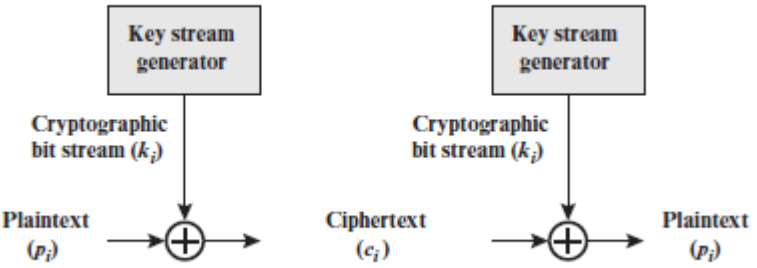


Figure 3.7 Vernam Cipher

```
SENDING
-------
message: 0 0 1 0 1 1 0 1 0 1 1 1 ...
pad:     1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR      ---------------------------
cipher:  1 0 1 1 0 0 0 1 1 1 0 0 ...

RECEIVING
---------
cipher:  1 0 1 1 0 0 0 1 1 1 0 0 ...
pad:     1 0 0 1 1 1 0 0 1 0 1 1 ...
XOR      ---------------------------
message: 0 0 1 0 1 1 0 1 0 1 1 1 ...
```

ONE-TIME PAD CIPHER

One-time pad cipher is a type of Vignere cipher which includes the following features:

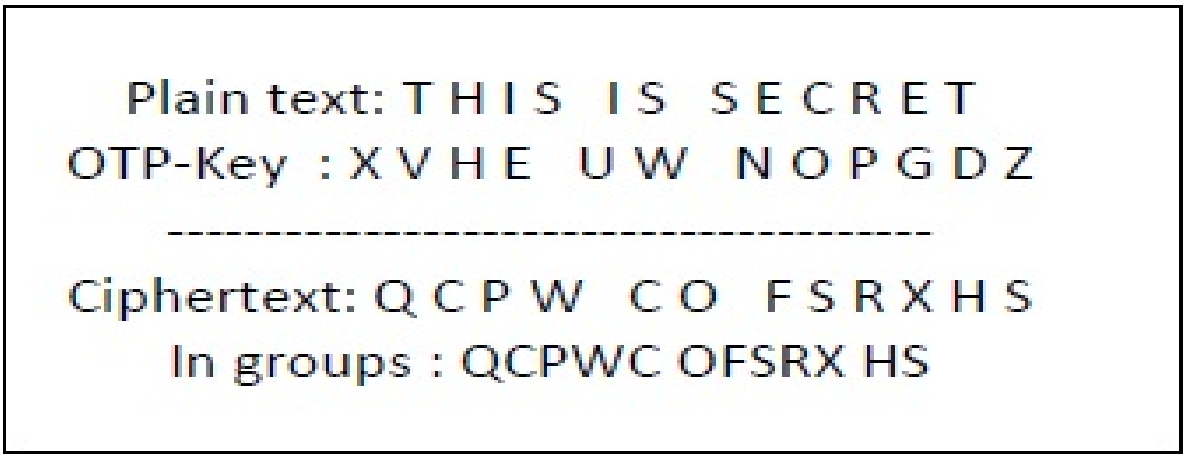
It is an unbreakable cipher.The key is **exactly same as the length of message which is encrypted.**The key is made up of random symbols.As the name suggests, key is **used one time only and never used again for any other message to be encrypted.**Due to this, **encrypted message will be vulnerable to attack for a cryptanalyst**.The key used for a one-time pad cipher is called **pad**

Why is it Unbreakable?

The key is unbreakable owing to the following features .The key is as long as the given message.The key is truly random and specially auto-generated. Each key should be used once and destroyed by both sender and receiver.There should be two copies of key: one with the sender and other with the receiver.

Encryption

To encrypt a letter, a user needs to write a key underneath the plaintext. The plaintext letter is placed on the top and the key letter on the left. The cross section achieved between two letters is the Cipher text. It is described in the example



Decryption

To decrypt a letter, user takes the key letter on the left and finds cipher text letter in that row. The plain text letter is placed at the top of the column where the user can find the cipher text letter.

HILL CIPHER

- Another interesting multiletter cipher is Hill cipher

Hill Algorithm:

Hill algorithm encrypts group of letters like digram, trigram etc. Here key and plaintext should be in the form of square matrix.

- Perform Encryption and Decryption using Hill Cipher for the message "PAY MORE MONEY"

  K= (17 17 5 21 18 21 2 2 19)

Encryption:

C=P*K mod26

The first three letters are represented by the vectors (15 0 24)

C= (15 0 4) (17 17 5 21 18 21 2 2 19)mod 26

= (17 17 11)

= (R R L)

Decryption:

P=C* K $^{-1}$mod 26

$k^{-1} = \frac{1}{|K|} adj(k)$

$|K|$= 17(342-42) -17(399-42) +5(42-36)

=17(300)-17(357) + 5(6)

=5100-6069+30

= -939mod 26

=23mod26

$|K|$=23

Adj(k)= adj(17 17 5 21 18 21 2 2 19)

Cofactor(17) =|18 21 2 19 | =300

Cofactor(17)= -|21 21 2 19 | =-357

Cofactor(5)=|21 18 2 2 | =78

Cofactor(21)=-|17 5 2 19 |=-313

Cofactor(18)=|17 5 2 19 |=313

Cofactor(21)=-|17 17 2 2 |=0

Cofactor(2)=|17 5 18 21 |=447

Cofactor(2)=-|17 5 21 21 |=-252

Cofactor(19)=|17 17 21 18 |=57

=$(300 \ -357 \ 78 \ -313 \ 313 \ 0 \ 447 \ -252 \ 57)^T$

adj(k)= $(300 \ -313 \ 447 \ -357 \ 313 \ -252 \ 78 \ 0 \ 57)$

$k^{-1} = \frac{1}{23}(300 \ -313 \ 447 \ -357 \ 313 \ -252 \ 78 \ 0 \ 57)$

$k^{-1} = 23^{-1}(300 \ -313 \ 447 \ -357 \ 313 \ -252 \ 78 \ 0 \ 57)$

23^{-1}=23*17=1mod26

=17$(300 \ -313 \ 447 \ -357 \ 313 \ -252 \ 78 \ 0 \ 57)$mod26

$k^{-1} = (300 \ -313 \ 447 \ -357 \ 313 \ -252 \ 78 \ 0 \ 57)$

$k^{-1} = (4 \ 9 \ 7 \ 15 \ 17 \ 6 \ 0 \ 0 \ 7)$

P= (17 17 11) (4 9 7 15 17 6 0 0 7)mod26

= (323 442 298) mod 26

= (15 0 24)

=PAY

TRANSPOSITION TECHNIQUES

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
```

This sort of thing would be trivial to cryptanalyze. A more complex scheme is to 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. For example,

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Thus, in this example, the key is 4312567. To encrypt, start with the column that is labeled 1, in this case column 3. Write down all the letters in that column. Proceed to column 4, which is labeled 2, then column 2, then column 1, then columns 5, 6, and 7.

STEGANOGRAPHY

Steganography is the practice of concealing a file, message, image, or video within another file,

The word **steganography comes** from Greek steganographia, which combines the words steganós (στεγανός), meaning "covered or concealed", and -graphia (γραφή) meaning "writing"

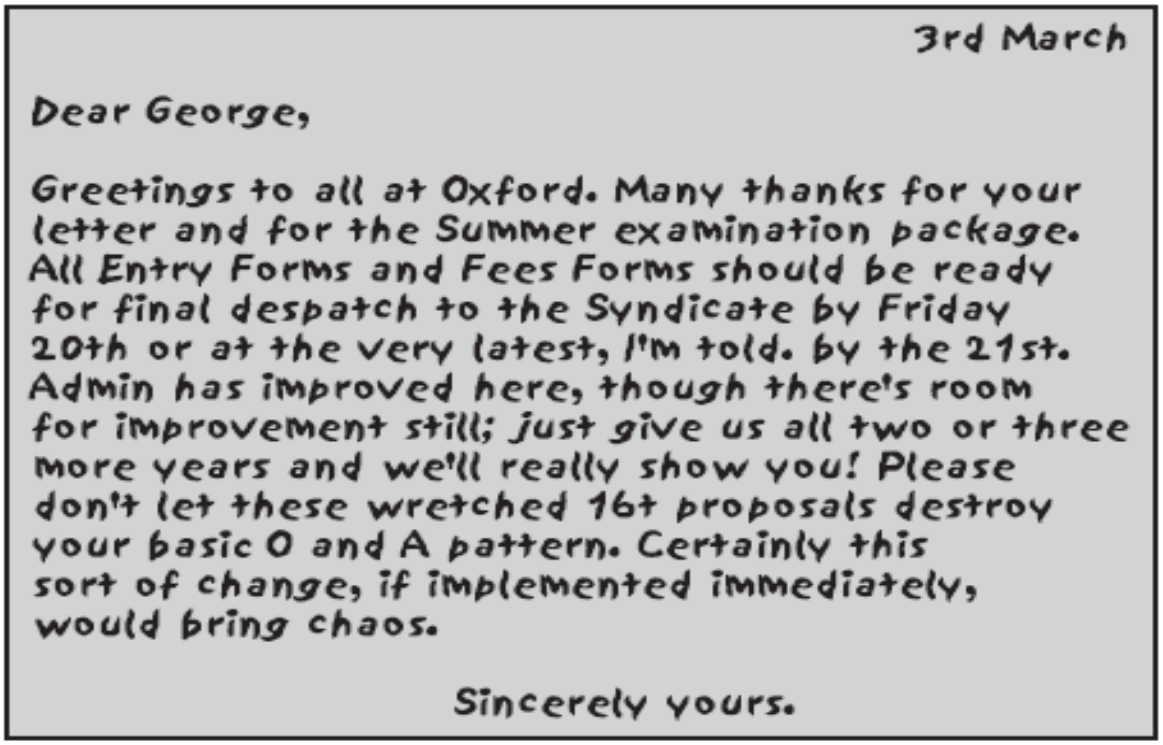
- Steganography is the technique of hiding secret data within an ordinary file or a message in order to avoid detection of data so that the secret data will be extracted only at its destination.
- The concept of steganography can be combined with encryption as an extra step for hiding or protecting data.
- A plaintext message may be hidden in one of two ways.
    - Steganography
    - cryptography
- The methods of **steganography** conceal (hide) the existence of the message, whereas the methods of cryptography render (provide/furnish)the message in non-readable format to outsiders by various transformations of the text.
- A simple form of steganography is an arrangement of words or letters within a text, spells out the real message. But is time-consuming to construct.
- For example, the sequence of first letters of each word of the overall message spells out the hidden message
- Big Rumble In New Greenland
- The War On
- Celebrity Acts Should End Soon
- Over Four
- Big Ecstatic Elephants Final

Here the steganography concept Hide message among irrelevant data

- This may Confuse the cryptanalyst

The Hidden message is BRING TWO CASES OF BEEF

Figure shows an example in which a subset of the words of the overall message is used to convey the hidden message i.e subset of words convey the hidden message



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Difference between Steganography and Cryptography

	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It's a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

Apart from these two techniques, various techniques are used in Steganography to maintain secure communication.

- **Character marking:** to hide the information the chosen letters are overwritten in pencil. The marked content is ordinarily not visible unless the paper is held at an angle to bright light.

- **Invisible ink:** A chemical or substances can be used for writing. but the actual content is invisible until heat or some chemical is applied to the paper.
- **Pin punctures:** In order to hide the information Small pin punctures are done over each character and is not visible unless the paper is held up in front of a light.
- **Typewriter correction ribbon:** Here the information is hidden between lines typed with a black ribbon. The results of typing with the correction tape are visible only under a strong light.

FOUNDATIONS OF MODERN CRYPTOGRAPHY

In modern cryptography we have numerous algorithm similar to traditional cyptography .we can name it as advanced method of traditional one. In modern cryptography too, we are going to learn some different kinds of algorithm.

- Modern encryption is the key to ,advanced computer and communication security.
- This stream of cryptography, is completely, based on the ideas of, mathematics such as number theory ,and computational complexity theory as well as concepts of probability.

This stream of algorithms are purely based on mathematics, here number theory plays an important role in security concepts. In maths the important part is number theory. i.e plays the important role in generating key, what is the use of this key, Key is used to lock my message, to protect it from third party i.e encrypt our mesage .In order to transfer data from sender to receiver in a secure manner RSA algorithm was used. Here key plays a vital role such that the key should be a large prime number such that the attacker couldn't identify the key.so it is impossible to break the code. Hence mathematical concepts are imposed in various cryptographic algorithms.

Characteristics of Modern Cryptography

Traditional Encryption	Modern Encryption

For making cipher text, manipulation is done in the characters of the plain text	For making cipher text operations are performed on binary bit sequence.
The whole of the ecosystem is required to communicate confidentially	Here only the parties who want to execute secure communication possess the secret key
These are weaker as compared to modern encryption	The encryption algorithm formed by this encryption technique is stronger as compared to traditional encryption algorithm.
It believes in the concept of security through obscurity	The security depends on the publicly known mathematical algorithm

Types of Modern Cryptography

- Different algorithm have come up with powerful encryption mechanisms incorporated in them . It promotes to two new ways of encryption mechanism of data security .They are
  - Symmetric key encryption

    Symmetric encryption is a type of **encryption** where only one **key** (a secret **key**) is used to both **encrypt** and decrypt electronic information. The entities communicating via **symmetric encryption** must exchange the **key** so that it can be used in the decryption process.
  - Asymmetric key encryption

    Asymmetric cryptography, also known as **public-key cryptography**, is a process that uses a pair of related **keys** -- one **public key** and one private **key** -- to **encrypt** and decrypt a message and protect it from unauthorized access or use.

Key:

It can be a number, word, phrase or any code that will be used for encrypting as well as decrypting any cipher text information into plain text and vice versa.

Security Services of Cryptography

- Confidentiality of Information

- Data Integrity
- Authentication
- Non-repudiation
- Availability
- **Confidentiality:** It states that only the sender and the receiver should have an access to the information. It is also known as privacy or secrecy of information.
- **Data Integrity**: assuring that data received is as sent (without any modification)ie message send by my friend must be received as it is without any modification

Authentication:

Authentication assures the recipient that the message is from, the intended source .it identifies who is sender and who is receiver also it verifies whether the user is an authorized user.

Non-Repudiation: When you have sent something you can't tell that you didn't sent and when you have receive some message you can't tell that you didn't receive anything.

Availability: Resources/applications must be available to authentic users all the time

Cryptography Primitives

- Cryptography primitives are the tools and techniques in cryptography that can be selectively used to provide a set of desired security services like Encryption, Hash Function ,Message Authentication Code(MAC) and Digital Signatures
- **Encryption**

  The process of converting information or data into a code, especially to prevent unauthorized access.
- **Hash Function**

  A hash function is a mathematical algorithm that takes an arbitrary amount of data as input and produces a fixed-size output of enciphered text .

The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

In general, the hash is much smaller than the input data.

For eg.it takes 512 bit as input and produces 128 bit hash code as output

- **Message Authentication Code(MAC)**

In cryptography, a **message authentication code** (**MAC**), sometimes known as a tag, is a short piece of information used to **authenticate** a **message**—in other words, to confirm that the **message** came from the stated sender (its authenticity) and has not been changed.

- **Digital Signatures**

A **digital signature** is a mathematical scheme, for verifying the authenticity of digital messages or documents. Here the message is encrypted by means of senders private key and this becomes the signature where in attached with the message. At the receiving end the the signature can only be decrypted by the senders public key, so that the receiver may able to verify the authenticity of message.

PERFECT SECURITY

- Perfect Secrecy(or information-theoretic secure)means that the cipher text conveys no information about the content of the plain text. However, part of being provable secure is that you need as much key material as you have plain text to encrypt**.**

.i.e if intruder gets my cipher text and he uses many techniques to get into it, even though he couldn't able to break the code. If this happens I can tell that my data is perfect data.i.e he is not able to get back my plaintext at any cost.

INFORMATION THEORY

- Mainly focus on the amount of data to be transmitted, how the data is transmitted, whether the data is transmitted through wired channel or wireless channel, how far it is secure? This field is the intersection of mathematics, statistics, computer science, physics, neurobiology, information engineering and electrical engineering,, natural language processing ,cryptography , neurobiology, human vision , the evaluation and function of molecular codes(bioinformatics),model selection in statistics , thermal

physics , quantum computing , linguistics , plagiarism detection , pattern recognition and anomaly detection. Actually it is a database or its similar to encyclopedia

PRODUCT CRYPTOSYSTEMS

A product cipher combines two or more transformations in a plaintext so that the resulting cipher is more secure than the individual components to make an resistant to cryptanalysis. The product cipher combines a sequence of simple transformations such as substitution(s-box), permutation(p-box) and modular arithmetic operations.In Caesar ciper, plafar cipher and so on we applied substitution technique's where as in Rail fence and row col technique permutation concepts were applied .Instead of applying a single technique alone, the combination could yield a system more powerful by applying substitution and permutation transformation .In Data Encryption Standard and the Advanced Encryption Standard product cipher technique is used .we will see them in the next unit.

CRYPTANALYSIS

Cryptanalysis is the art of trying to decrypt the encrypted messages, without the use of key. Various attacks are

- **Brute force attack:** This type of attack uses algorithms that try to guess all possible logical combinations of the plain text which are then ciphered and compared against the original cipher.
- **Dictionary attack:** This type of attack uses a wordlist in order to find a match of either the plaintext or key. In word list the data will be in the form of Jumbled words .Now the attacker may rearrange to get the original data. It is mainly used when trying to crack encrypted passwords.
- **Rainbow table attack:** Previously the computed hash values will be stored in the hash table**.** This type of attack compares the cipher text against precomputed hashes to find matches.

Other attacks using Cryptanalysis

- **Known-Plaintext Analysis (KPA):** Attacker decrypt ciphertext with known partial plain text.
- **Chosen-Plaintext Analysis (CPA):** Attacker arbitrarily selecting plaintext and generating some cipher text via the same algorithm technique.
- **Man-in-the-Middle Attack(MITM)** : Attack occurs when two parties use message or key sharing for communication via a channel that appears secure but is actually compromised