UNIT-1

OVERVIEW OF COMPUTER SECURITY

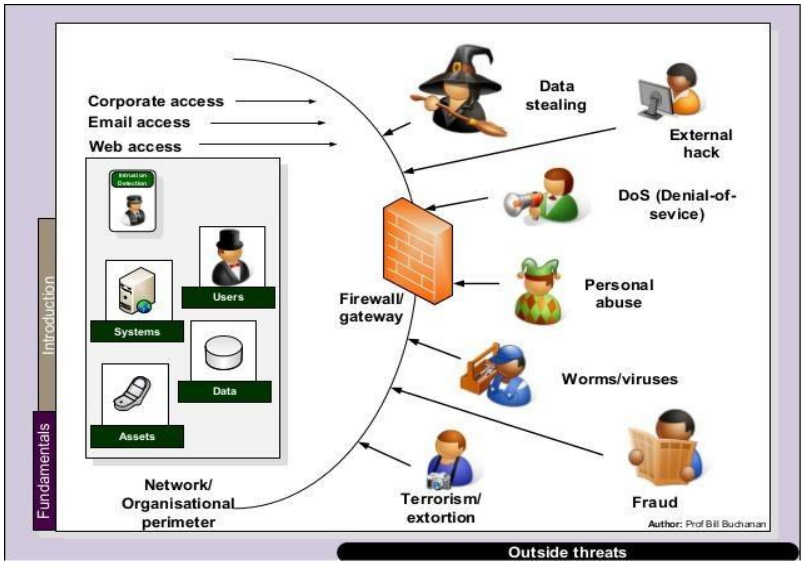
- A **computing system**: is a collection of hardware, software, data, and people that an organization uses to do computing tasks
- Computer security means protect our computing system

Main aspects are:

- Prevention:- Prevent your assets from being damaged
- Detection :- Detect when assets has been damage
- Reaction:- Recover your assets

Computer Security: - Ensuring the data stored in a computer cannot be read or compromised by an individual‘s without authorization.

- Most computer security measures involve data encryption and passwords.
- The purpose of computer security is to device ways to prevent the weaknesses from being



SECURITY CONCEPTS

Three Goals in Computing Security

Three goals of computer security are

1. Confidentiality
2. Integrity
3. Availability

•**Confidentiality**: ensures that computer-related assets are accessed only by authorized parties. Confidentiality is sometimes called secrecy or privacy.

-Difficult to ensure

- Easy to assess

Confidentiality is the ability to hide information from those people unauthorized to view it. It is perhaps the most obvious aspect of the CIA(Confidentiality, Integrity and Availability) triad when it comes to security; but correspondingly, it is also the one which is attacked most often.

Cryptography and Encryption methods are an example of an attempt to ensure confidentiality of data transferred from one computer to another.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online.

Data encryption is a common method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is becoming the norm.

Other options include biometric verification and security tokens, key fobs or soft tokens.

In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction.

Different approaches for achieving confidentiality are

- **Access control**: - specify who can access. One access control mechanism for preserving confidentiality is cryptography
- **Identification and Authentication**

Two concepts in confidentiality are

1. **Data Confidentiality**: - assures that confidential information is not disclosed to authorize individuals.
- Only the people who are authorized to do so can gain access to sensitive data. Imagine your bank records.
- You should be able to access them, of course, and employees at the bank who are helping you with a transaction should be able to access them, but no one else should.
2. **Privacy:** The right of individuals to hold information about themselves in secret, free from the knowledge of others

•**Integrity:** it means that assets can be modified only by authorized parties or only in authorized ways.

- Much difficult to measure

Two concepts in integrity are

1. **Data Integrity**:- Information and programs are changed only in authorized manner
2. **System Integrity**: - System performs its operation in unimpaired manner that means state of the system not changed.

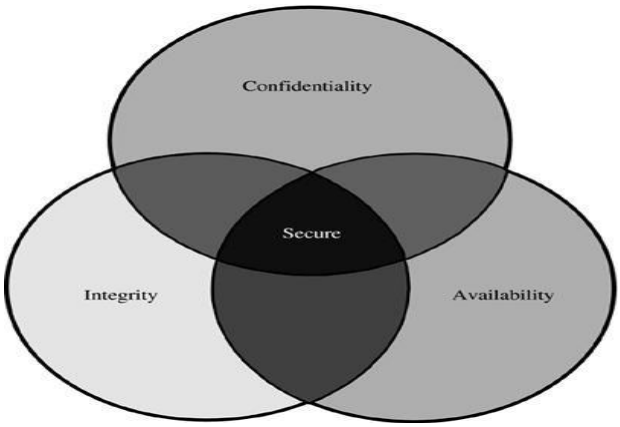
Integrity mechanisms fall into two classes: ***prevention*** **mechanisms and** ***detection*** **mechanisms**.

Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways.

Detection mechanisms do not try to prevent violations of integrity; they simply report that the data‘s integrity is no longer trustworthy. The mechanisms may report the actual cause of the integrity violation (a specific part of a file was altered), or they may simply report that the file is now corrupt.

•**Availability:** it means that assets are accessible to authorized users in all time

- Availability applies both to data and to service.
- Failure to this goal (availability)is known as Denial of service.
- Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all



One of the challenges in building a secure system is finding the right balance among the goals, which often conflict.

Along with three objectives system should also ensure

1. **Authentication**: Computer system be able to verify identity of user.

   Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

   Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID.

2. **Accountability**: Every individual who works with an information system should have specific responsibilities for information assurance.
3. **Non repudiation**: non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity of that message.

Digital signatures can offer non-repudiation when it comes to online transactions, where it is crucial to ensure that a party to a contract or a communication can't deny the authenticity of their signature on a document or sending the communication in the first place.

In this context, non-repudiation refers to the ability to ensure that a party to a contract or a communication must accept the authenticity of their signature on a document or the sending of a message.

NEED OF SECURITY

Why is computer security important?

Computer security is important, primarily to keep your information protected. It‘s also important for your computer‘s overall health, helping to prevent viruses and malware and allowing programs to run more smoothly. Security is needed due to following reason

1. Privacy:- It defines the right of individuals to hold information about themselves in secret, free from the knowledge of others
2. Accuracy: - Most of damages of data is caused by errors and omissions. An organization always needs accurate data for transaction processing, providing better service and making
3. Threats by dishonest employ
4. Computer Crimes:- When computer resources can be misused for unauthorized or illegal function
5. Threats for fire and Natural Disasters:- fire and natural disasters like floods, storms, lightening etc

ATTACKS

- Attack is the process of gaining the access of data by unauthorized user.
- It is an Act or attack that exploit vulnerability(Weakness of the system)

Definition - What does Attack mean?

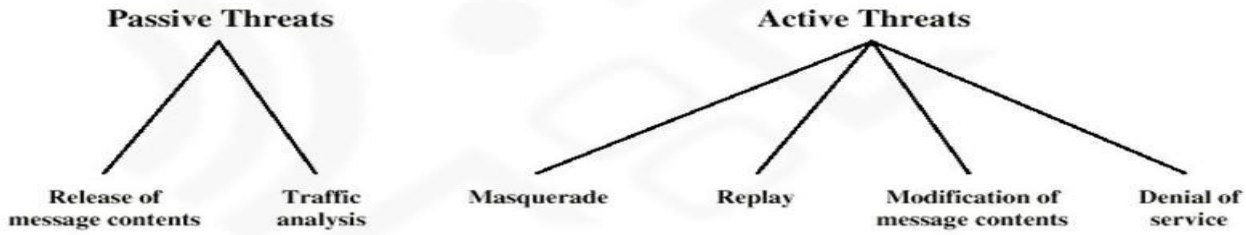
An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

Two types of attacks are

1. Passive attack:-data just accessed by third party, no modification, does not affect system resources
2. Active attack:- data will be modified

Attack Categories

Generally attacks may be categorized in ***passive*** and ***active*** attacks. While passive attacks can be defined as read-only attacks, active attacks include data generation, modification, or destruction.



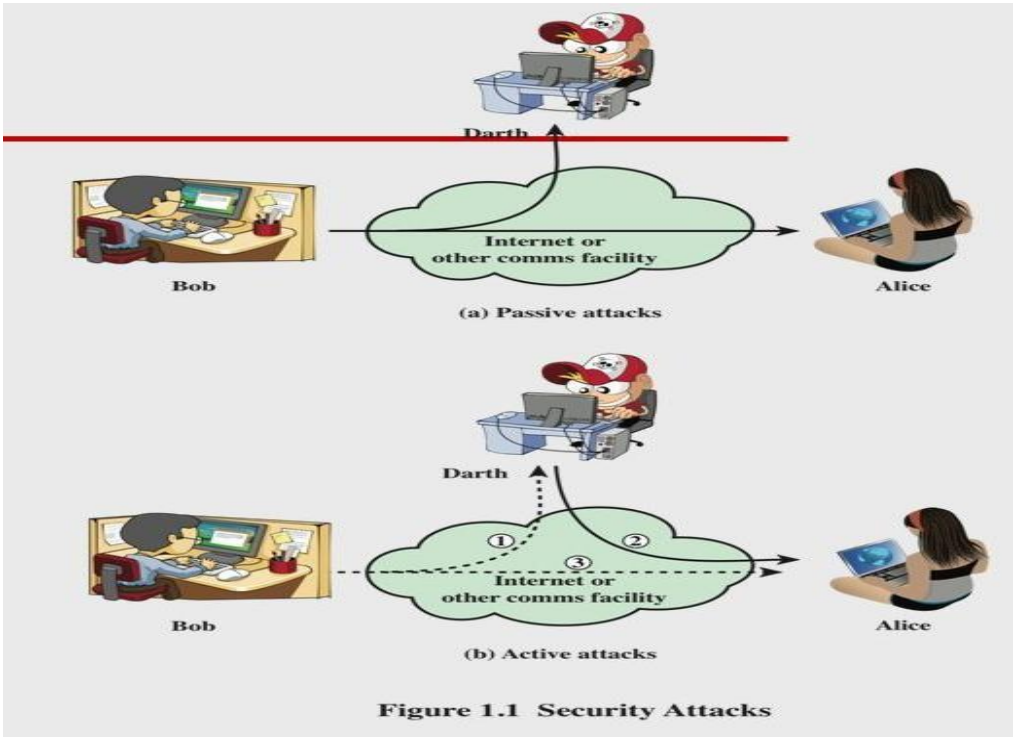


Figure 1.1 Security Attacks

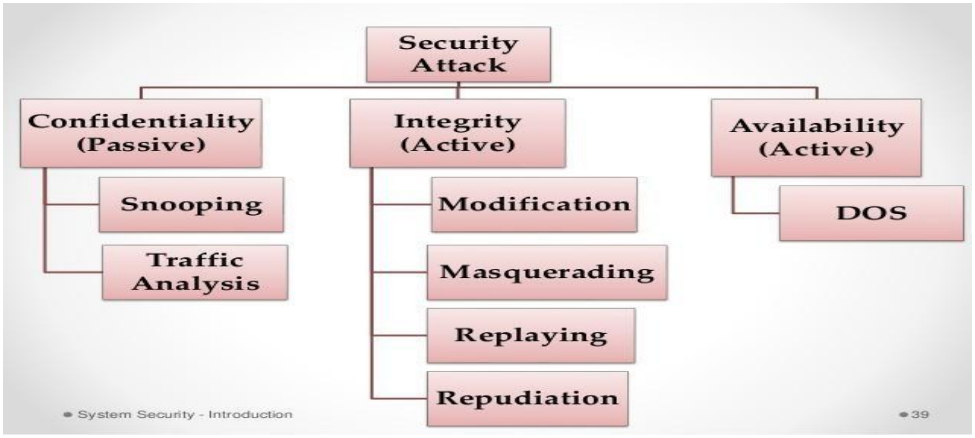
- **Passive Attacks**
  - **Release of message contents** for a telephone conversion, an electronic mail message, and a transferred file are subject to these threats
  - **Traffic analysis:-** By analyzing the traffic flow between sender and receiver third party access the data
- **Active Attacks**
  - **Masquerade** takes place when one entity pretends to be a different entity
  - **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - **Modification** of messages means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
  - **Denial of service** prevents or inhibits the normal use or management of communications facilities
    - Disable network or overload it with messages

Passive VS Active Attacks

Passive Attacks

- To obtain information that is being transmitted.
- E.g. Release of confidential information and Traffic analysis
- Difficult to detect
- Initiative to launch an active attack
- Interception
- Relieved by using encryption

- **Active Attacks**
  - Involve modification of the data stream or creation of a false stream
  - E.g. Masquerade, replay, message modification, denial of services
  - Potentially detected by security mechanisms
  - Interruption, Modification, Fabrication



1. **Masquerade attack**

Masquerade

A masquerade is a type of attack where the attacker act as an authorized user system in order to gain access to it or to gain greater privileges than they are authorized for.

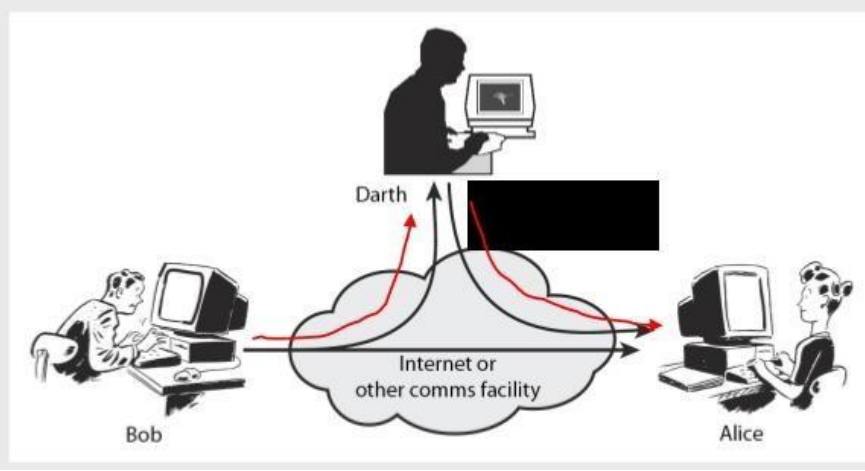
The third party sends the same message to the receiver and receiver receives it with the name of sender.

2. **Replay attack**

- Here receiver receives two messages. One from sender and another from third party.
- Receiver did not know which one is correct

3. **Data Modification attack**

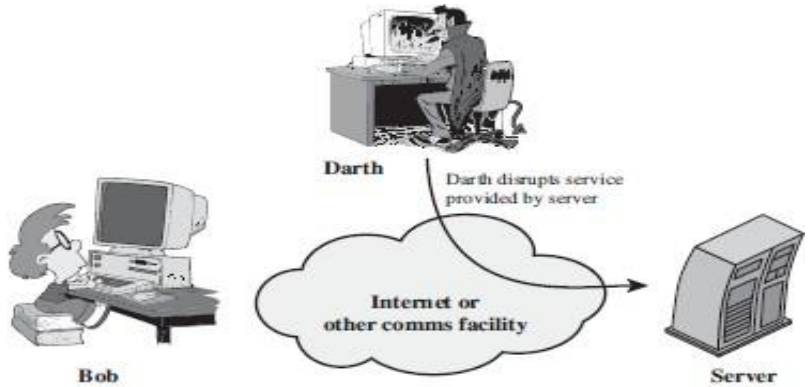
- Modification is integrity violation.
- An unauthorized party not only gains access to but tampers with an asset.
- This is an attack on the integrity.
- Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of a message being transmitted in a network.



4. **Denial of Service**
    - A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.
    - In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.
    - The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection.

- When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

- Here the third party interrupts (disrupts) the services sends by the server.
- Disruption of entire network either by disabling the network or by overloading it with message , so as to degrade performance



(d) Denial of service

SECURITY SERVICES:

1. **Confidentiality**: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. E.g. printing, displaying and other forms of disclosure.
2. **Authentication**: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
3. **Integrity**: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
4. **Non repudiation**: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
5. **Access control**: Requires that access to information resources may be controlled by or the target system.
6. **Availability**: Requires that computer system assets be available to authorized parties when needed.

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 that 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:

- **Connection Integrity with Recover**y: 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.

Non-Repudiation: 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:

According to X.800, the security mechanisms are divided into those implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. X.800 also differentiates reversible & irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted, whereas irreversible encipherment include hash algorithms and message authentication codes used in digital signature and message authentication applications.

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 certain 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 be 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.

A MODEL FOR NETWORK SECURITY

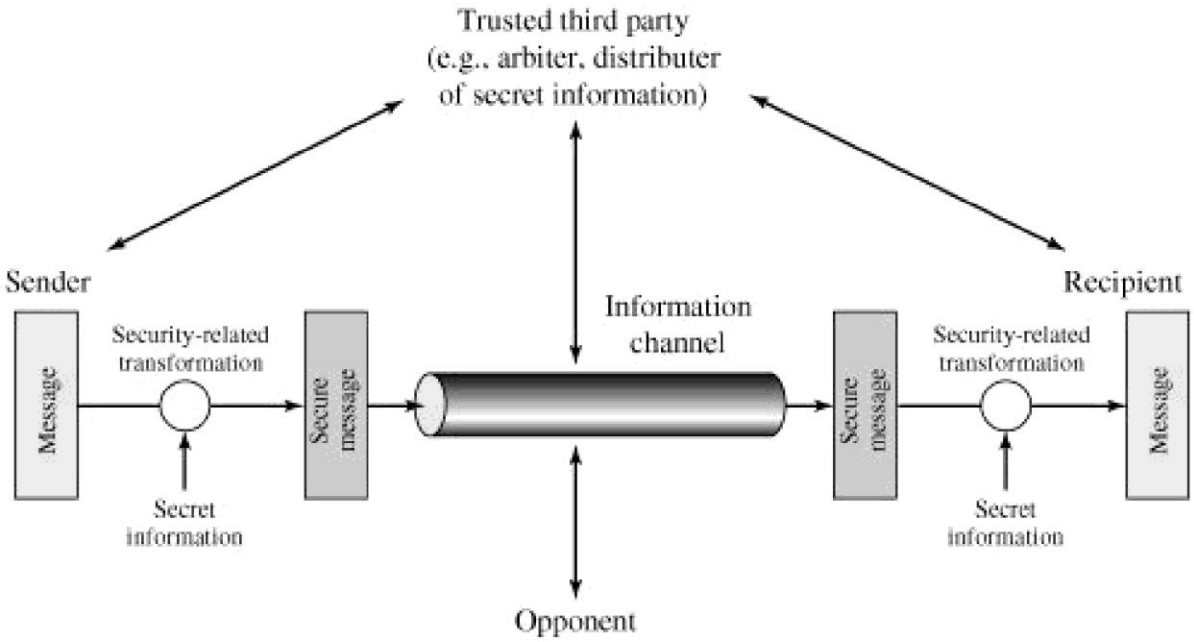


Figure. Model for Network Security

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 takeplace. 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. 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. All the techniques for providing security have two components:

A security-related transformation on the information to be sent. Examples include the

encryption of the message, which scrambles the message so that it is unreadable by

the opponent, and the addition of a code based on the contents of the message, which can be used to verify the

identity of the sender Some secret information shared by the

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

The general model shows that there are four basic tasks in designing a particular securityservice:

1. Design an algorithm for performing the security-related transformation. Thealgorithm 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 securityalgorithm and the secret information to achieve a particular security service.

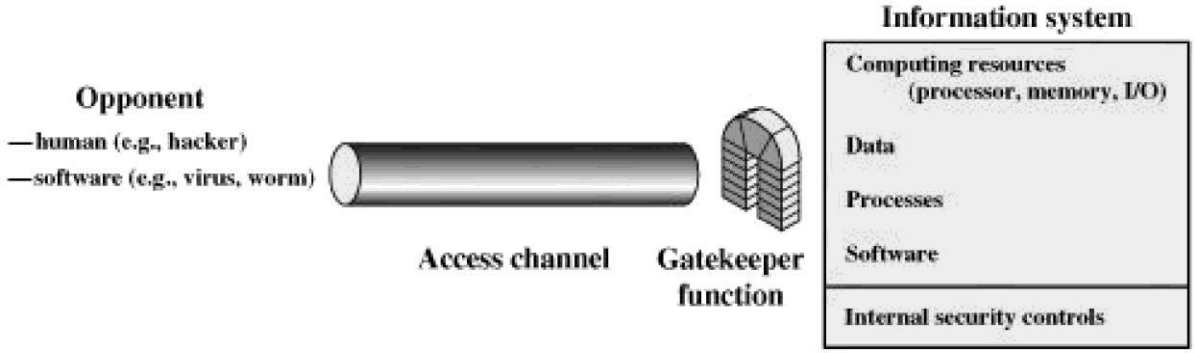


Figure: 1.6 Network Access Security Model

A general model is illustrated by the above Figure 1.6, which reflects a concern for protecting an information system from unwanted access. Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network. The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system. Or, the intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computerassets for financial gain.

CLASSICAL ENCRYPTION TECHNIQUES

- The Process of converting from plaintext to ciphertext is known **as enciphering or encryption.**
- Restoring the plaintext from the ciphetext is **deciphering or decryption.**
- The many schemes used for encryption constitute the area of study known as **cryptography.**
- Techniques used for deciphering a message without any knowledge of the enciphering details is known as **cryptanalysis.** It also known as **"Breaking the Code".**
- The areas of cryptography and cryptanalysis together are called **cryptology.**
- A **cryptanalyst** develops mathematical methods and codes that protect data from computer hackers. This involves the decryption of a cipher text into plain text in order to transmit a message over insecure channels.

Symmetric cipher model

- 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 cipher text using a secret key and an encryption algorithm.
- Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text.
- 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 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.
  - **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. 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.

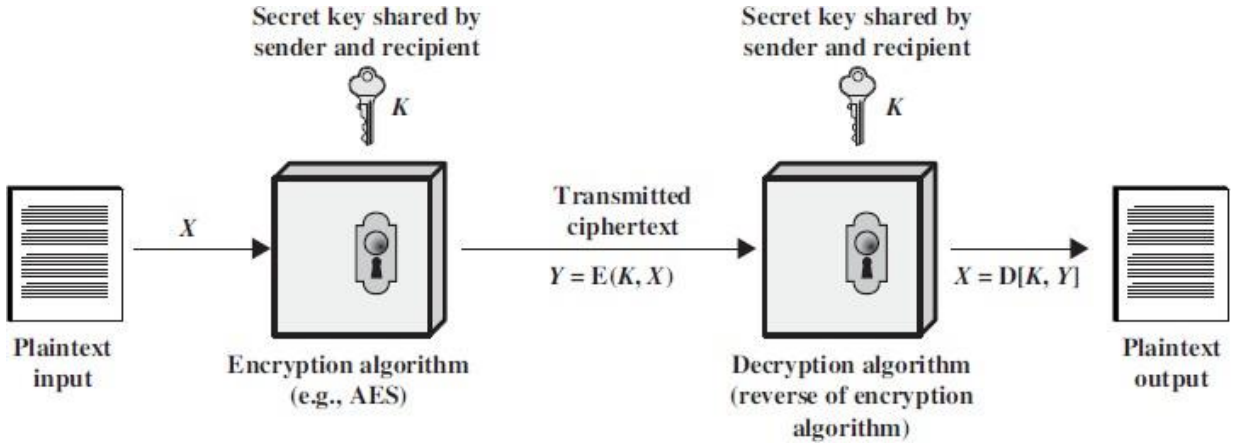
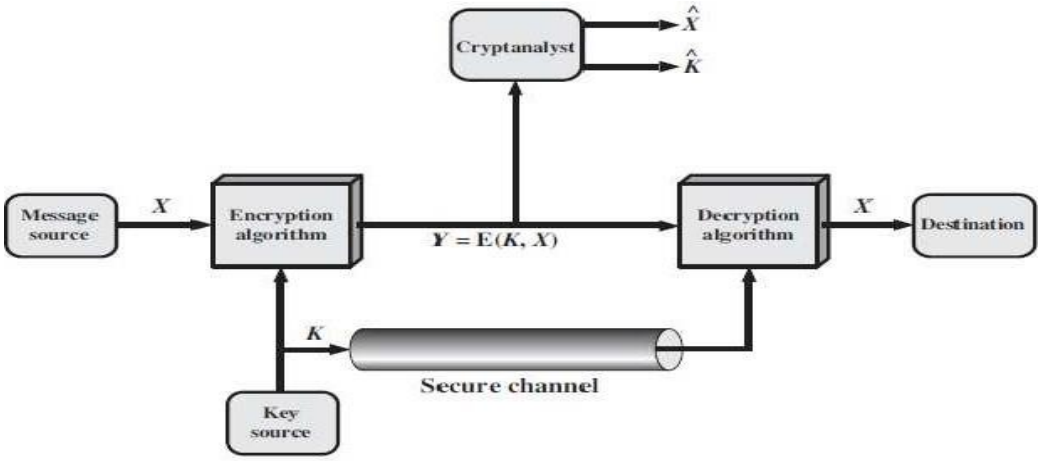


Fig: Simplified Model of Symmetric Encryption

Symmetric Cipher Model



- A symmetric cipher model are broadly contains five parts.
- **Plaintext:** This is the original intelligible message.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext. It takes in plaintext and key and gives the cipher text.
- **Secret key:** The key is a value independent of the plaintext and of the algorithm. Different keys will yield different outputs.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
- **Decryption algorithm:** Runs on the cipher text and the key to produce the plaintext.This is essentially the encryption algorithm run in reverse.

- Two basic requirements of encryption are:
  1. Encryption algorithm should be strong. An attacker knowing the algorithm and having any number of cipher text should not be able to decrypt the cipher text or guess the key.
  2. The key shared by the sender and the receiver should be secret.
- Let the plaintext be $X = [X1, X2,\ldots, X_M]$, key be $K = [K1, K2,\ldots, K_J]$ and the cipher text produced be $Y = [Y1, Y2,\ldots, Y_N]$. Then, we can write

$$Y = (K, \mathrm{X})$$

- Here E represents the encryption algorithm and is a function of plaintext X and key K.
- The receiver at the other ends decrypts the cipher text using the key.

$$\mathrm{X} = (K, Y)$$

- Here D represents the decryption algorithm and it inverts the transformations of encryption algorithm.
- An opponent not having access to X or K may attempt to recover K or X or both.
- 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 torecover by generating a plaintext estimate $\hat{X}$.
- If the opponent is interested in being able to read future messages as well then he will attempt to recover the key by making an estimate $\hat{K}$.

- Cryptographic systems are characterized along three independent dimensions.
  1. **The types of operations used for transforming plaintext to ciphertext.** All encryption algorithms are based on two general principles substitution, and transposition. Basic requirement is that no information be lost. Most systems referred to as product system, involves 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 encryption**. 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 process a block at a time and produce an output block for each input block. A stream cipher process the input element 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 simple plaintext-ciphertext pairs. This typeof attack finds characteristics of the algorithm to find a specific plaintext or to find key.
- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until plaintext is obtained. On average, half of all possible keys must be tried to achieve success.
- Based on the amount of information known to the cryptanalyst cryptanalytic attacks can be categorized as:
  - **Cipher text Only Attack:** The attacker knows only cipher text only. It is easiest to defend.
  - **Known plaintext Attack:** In this type of attack, the opponent has some plaintext-cipher text pairs. Or the analyst may know that certain plaintext patterns will appear in a message. For example, there may be a standardized header or banner to an electronic funds transfer message and the attacker can use that for generating plaintext-cipher text pairs.
  - **Chosen plaintext:** If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a *chosen-plaintext* attack is possible. In such a case, the analyst will pick patterns that can be expected to reveal the structure of the key.
  - **Chosen Cipher text:** In this attack, the analyst has cipher text and some plaintext-cipher text pairs where cipher text has been chosen by the analyst.
  - **Chosen Text:** Here, the attacker has got cipher text, chosen plaintext-cipher text pairs and chosen cipher text-plaintext pairs.
- Chosen cipher text and chosen text attacks are rarely used.
- It is assumed that the attacker knows the encryption and decryption algorithms.
- Generally, an encryption algorithm is designed to withstand a known-plaintext attack.

Substitution Techniques

It is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

Caesar cipher

- The encryption rule is simple; replace each letter of the alphabet with the letter standing 3 places further down the alphabet.
- The alphabet is wrapped around so that Z follows A.
- Generally Plain text is in lower case and Cipher text is Upper Case.
- Example:

  Plaintext: meet me after the party

  Ciphertext: PHHW PH DIWHU WKH

SDUWB

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

- Here, the key is 3. If different key is used, different substitution will be obtained.
- Mathematically, starting from a=0, b=1 and so on, Caesar cipher can be written as:

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

Encryption k=3 **$E(p) = (p + k) \bmod (26)$**	**Result**	**Cipher Text** **$D(C) = (C - k) \bmod (26)$**	**Result**
M=E(M)=(12+3)mod26	15=P	D(P)=(15-3)mod26	12=m
E=E(E)=((4+3)mod26	7=H	D(H)=(7-3)mod26	4=e
E= E(E)=((4+3)mod26	7=H	D(H)=(7-3)mod26	4=e
T=E(T)=((19+3)mod26	21=V	D(V)=(21-3)mod26	19=t

- This cipher can be broken
  - If we know one plaintext-cipher text pair since the difference will be same.
  - By applying Brute Force attack as there are only 26 possible keys.

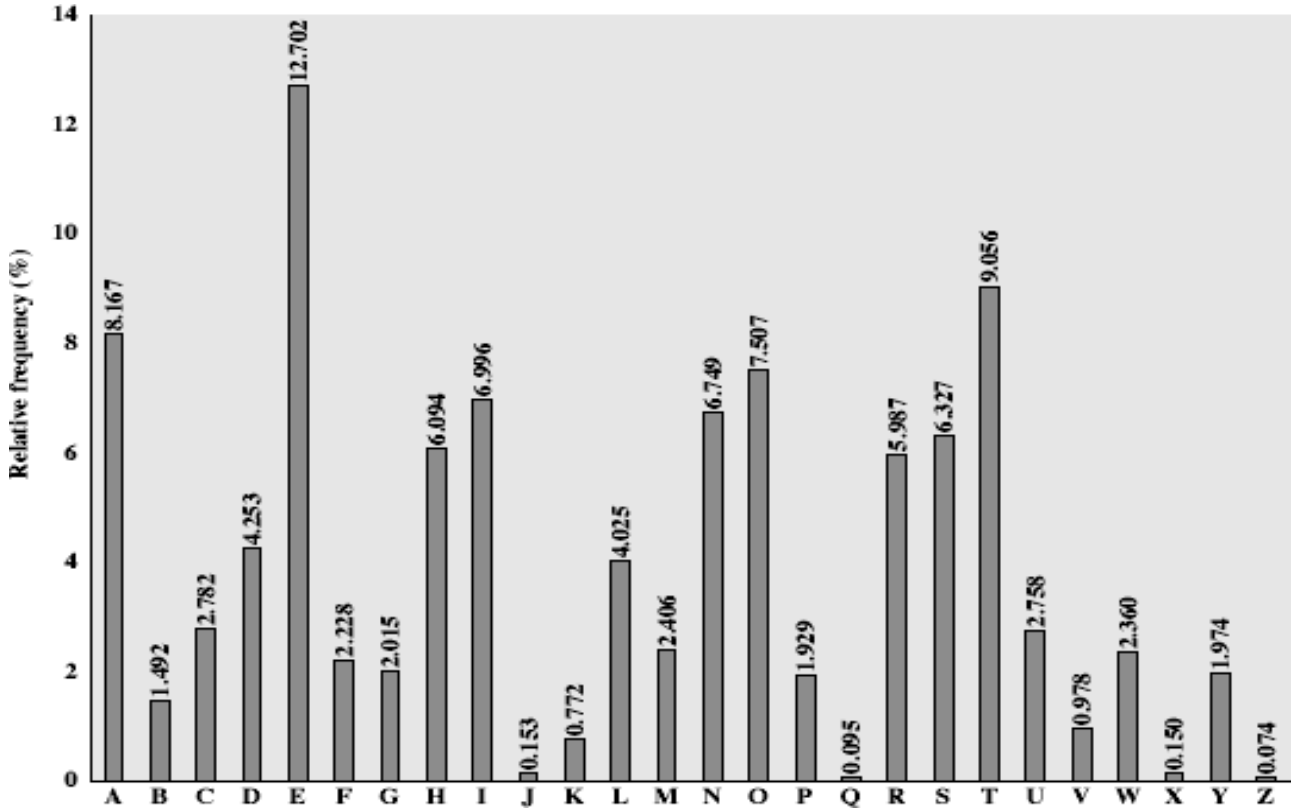
Example2:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
transforms "HELLO" to "KHOOR"

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

Monoalphabetic Substitution Cipher

- Instead of shifting alphabets by fixed amount as in Caesar cipher, any random permutation is assigned to the alphabets. This type of encryption is called monoalphabetic substitution cipher.
- For example, A is replaced by Q, B by D, C by T etc. then it will be comparatively stronger than Caesarcipher.
- The number of alternative keys possible now becomes 26!.
- Thus, Brute Force attack is impractical in this case.
- However, another attack is possible. Human languages are redundant i.e. certain characters are usedmore frequently than others. This fact can be exploited.
- In English ‘e’ is the most common letter followed by ‘t’, ‘r’, ‘n’, ’o’, ‘a’ etc. Letters like ‘q’, ‘x’, ‘j’ are less frequently used.
- Moreover, digrams like ‘th’ and trigrams like ‘the’ are also more frequent.
- Tables of frequency of these letters exist. These can be used to guess the plaintext if the plaintext is in uncompressed English language.
- The most common two letter combinations are called as **digrams**. e.g. th, in, er, re and an.
- The most common three letter combinations are called as **trigrams.** e.g. the, ing, and, and ion



Playfair Cipher

- In this technique multiple (2) letters are encrypted at a time.
- This technique uses a 5 X 5 matrix which is also called key matrix.

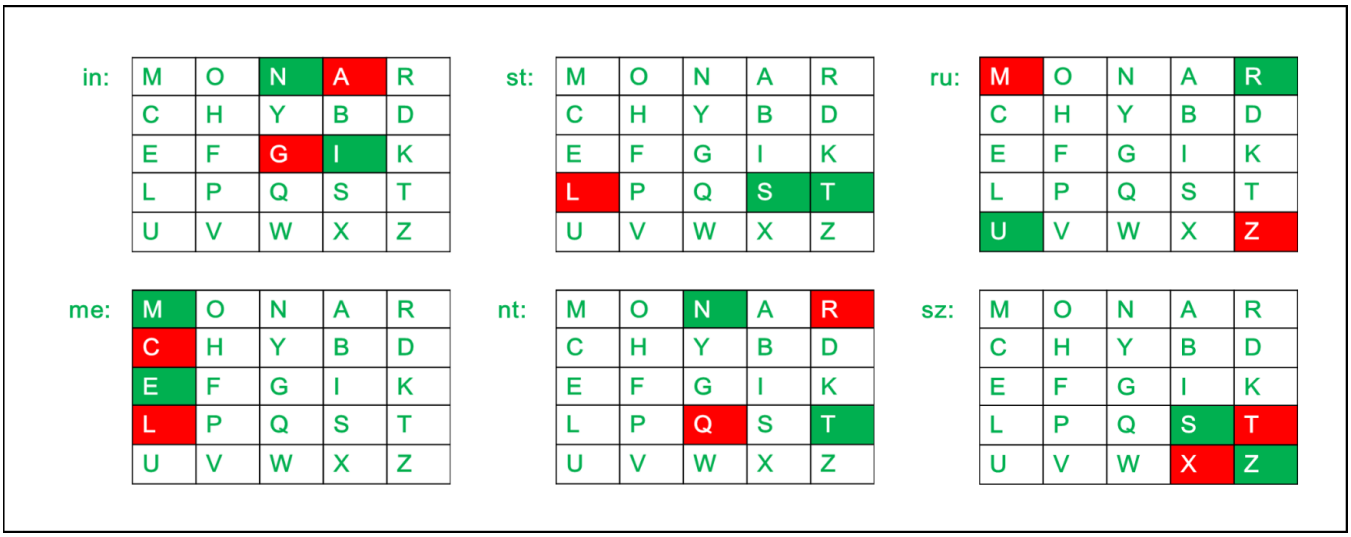
M	**O**	**N**	**A**	**R**
C	**H**	**Y**	**B**	**D**
E	**F**	**G**	**I/J**	**K**
L	**P**	**Q**	**S**	**T**
U	**V**	**W**	**X**	**Z**

- The plaintext is encrypted **two letters at a time**:
  - Break the plaintext into pairs of two consecutive letters.
  - If a pair is a repeated letter, insert a filler like 'X'in the plaintext, eg. "Balloon" is treated as "ba lx lo on".
  - If both letters fall in the same row of the key matrix, replace each with the letter to its right (wrapping back to start from end), eg. "AR" encrypts as "RM".
  - If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. "MU" encrypts to "CM".
  - Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. "HS" encrypts to "BP", and "EA" to "IM" or "JM" (as desired)
- Security is much improved over monoalphabetic as here two letters are encrypted at a time and hence there are 26 X 26 =676 diagrams and hence it needs a 676 entry frequency table.

However, it can be broken even if a few hundred letters are known as much of plaintext structure isretained incipher text.

```
Example 2:  PlainText: "instruments" keyword: monarchy
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'
cipher text : ga tl mz cl rq tx
```

*For both **encryption** and **decryption**, the **same key** is to be used.*



video link: https://www.youtube.com/watch?v=quKhvu2tPy8

Strength of playfair cipher Playfair cipher is a great advance over simple mono alphabetic ciphers. Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

Hill Cipher

source link

- This cipher is based on linear algebra.
- Each letter is represented by numbers from 0 to 25 and calculations are done modulo 26.
- This encryption algorithm takes m successive plaintext letters and substitutes them with m cipher text letters.
- The substitution is determined by m linear equations. For *m* = 3, the system can be described as:

$$c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \ mod\ 26$$
$$c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \ mod\ 26$$
$$c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \ mod\ 26$$

- This can also be expressed in terms of row vectors and matrices.

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

  Where **C** and **P** are row vectors of length 3 representing the plaintext and cipher text, and **K** is a 3 X 3 matrix representing the encryption key

- Key is an invertible matrix K modulo 26, of size m. For example:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad K^{-1} = \begin{pmatrix} 4 & 19 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- Encryption and decryption can be given by the following formulae:
  Encryption: $C = PK \ mod\ 26$
  Decryption: $P = CK^{-1} \ mod\ 26$

- The strength of the Hill cipher is that it completely hides single-letter frequencies.
- Although the Hill cipher is strong against a cipher text-only attack, it is easily broken with a known plaintext attack.
  - Collect m pair of plaintext-cipher text, where m is the size of the key.
  - Write the m plaintexts as the rows of a square matrix P of size m.
  - Write the m cipher texts as the rows of a square matrix C of size m.
  - We have that C=PK mod 26.
  - If P is invertible, then $K=P^{-1}C \bmod 26$,
  - If P is not invertible, then collect more plaintext-cipher text pairs until an invertible P is obtained.

The Vigenère cipher

- This is a type of polyalphabetic substitution cipher (includes multiple substitutions depending on thekey). In this type of cipher, the key determines which particular substitution is to be used.
- 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 follows:
  Key: *deceptivedecept*
  Plaintext: wearediscovered
  Ciphertext:
  ZICVTWQNGRZGVTW
- Encryption can be done by looking in the Vigenere Table where ciphertext is the letter key's row and plaintext's column or by the following formula:

$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

- Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.
- The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.
- Thus, the letter frequency information is obscured however, not all knowledge of the plaintext structure is lost.

Vernam Cipher

- This system works on binary data (bits) rather than letters.
- The technique can be expressed as follows:

$$C_i = P_i \oplus K_i$$

  Where
  P_i = i^{th} binary digit of plaintext.
  K_i = i^{th} binary digit of key.
  C_i = i^{th} binary digit of ciphertext.
  $\oplus$ = exclusive-or (XOR) operation
- Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.
- Decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus K_i$$

- The essence of this technique is the means of construction of the key.
- It was produced by the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword.

- Although such a scheme has cryptanalytic difficulties, but it can be broken with a very long ciphertext or known plaintext as the key is repeated.

One-Time Pad

- In this scheme, a random key that is as long as the message is used.
- The key is used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message.
- This scheme is unbreakable.
- It produces random output that bears no statistical relationship to the plaintext.
- Because the ciphertext contains no information whatsoever about the plaintext, there is simply no wayto break the code.
- For any plaintext of equal length to the ciphertext, there is a key that produces that plaintext.
- Therefore, if you did an exhaustive search of all possible keys, you would e d up with many legible plaintexts, with no way of knowing which the intended plaintext was.
- Therefore, the code is unbreakable.
- The security of the one-time pad is entirely due to the randomness of the key.
- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
    - There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
    - Another problem is that of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver.
- Because of these difficulties, the one-time pad is used where very high security is required.
- The one-time pad is the only cryptosystem that exhibits **perfect secrecy**.

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.