

# Computer Security

---

## Chapter 1: Introduction

---

### Definitions

- **Security**: the quality of state if being secure (free from danger or to be protected from adversaries).
- **Threat**: bad things that might happen.
- **Vulnerability**: weakness in your defenses (point where a system is susceptible to attack).
- **Attacks**: ways in which the threat may be actualized.
- **Countermeasures**: are techniques for protecting computer or network system from cyber threats.
- **Computer security**: provisions and policies adopted to protect information and property against intruders and malicious software while allowing the information and property to remain accessible and productive to its intended users.
- **Network security**: provisions and policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network accessible resources.

### Types of vulnerabilities

- Physical vulnerabilities
- Natural vulnerabilities
- Hardware and software vulnerabilities
- Media vulnerabilities
- Communication vulnerabilities
- Human vulnerabilities

### Types of threats

- Natural
- Unintentional
- Intentional (80% by fully authorized users)

## Consequences of risks

- Failure/End of service.
- Reduction of Qos, (Denial of Service(DoS))
- Internal problems in enterprise
- Trust decrease
- Technology leakage
- Human consequences

## Countermeasures

- Authentication
- Encryption
- Auditing/inspect the quality of the system
- Administrative procedures
- Standards
- Physical security
- Laws
- Backups
- Removing or reducing vulnerability to prevent an attack and block a threat.

## Properties of secured system

- **Confidentiality**: information can only be accessible for reading by authorized parties. It requires that the system should verify the identity of a user.
- **Integrity**: information should be modified or altered only by authorized parties. Modification includes writing, changing, deleting, and creating the message that is supposed to be transmitted across the network.
- **Availability**: computer and network assets are only available to authorized parties or data are accessible when you need them.
- **Nonrepudiation**: provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. It's assurance that the **sender of information** is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

## Supplements to CIA

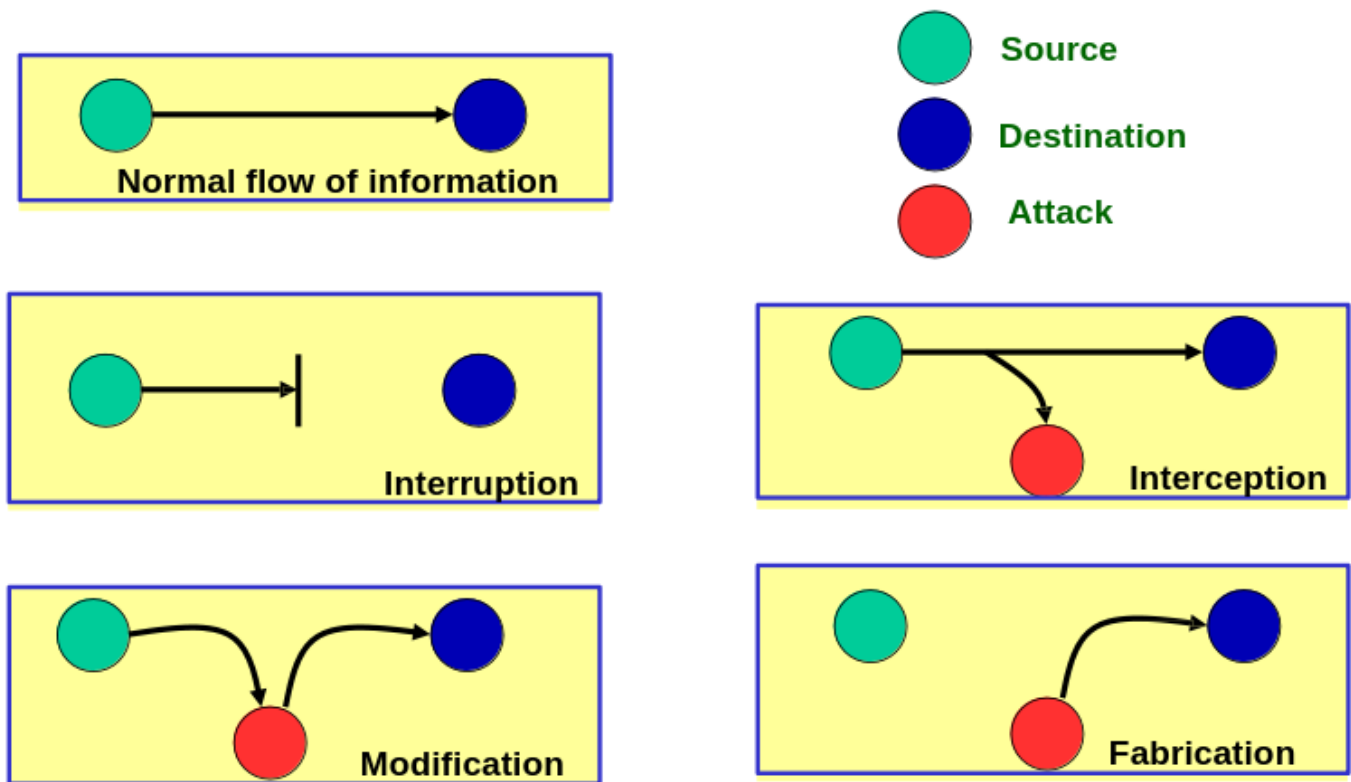
- **Authentication**: correctly identifying the communicating parties.
- **Authorization**: giving different access rights for different types of users
- **Accountability**: keeps track of user activity while users are logged in to a network by tracking information such as how long they were logged in, the data they sent or received, their Internet

Protocol (IP) address, the Uniform Resource Identifier (URI) they used, and the different services they accessed.

## Goals of security

- Prevention - preventing the system from being attacked.
- Detection - determining that an attack is underway, or has occurred and report it.
- Recovery - resumption of correct operation. It has two forms:-
  - To stop an attack and to assess and repair any damage caused by that attack.
  - The system continues to function correctly while an attack is underway but the system may disable nonessential functionality.

## Categories of attacks



- Interruption : An attack on availability
- Interception : An attack on confidentiality
- Modification : An attack on integrity
- Fabrication : An attack on authenticity

## Passive attacks vs Active attacks

- **Passive attacks:**
  - Attempt to learn or make use of the information without changing the content of the message and disrupting the operation of the communication. Example: Eavesdropping and Traffic analysis
  - Very difficult to detect.
  - Prevention methods are more effective than detection methods.
- **Active attacks:**
  - Attempts to interrupt, modify, delete, or fabricate messages or information thereby disrupting normal operation of the network.

- Example: Jamming , Impersonating (Masquerade) , Modification , Denial of Service (DoS) , and Message replay
- Very difficult to prevent.
- Detection methods are more effective than prevention methods.

## Internal vs External attacks

- **External attacks:** are carried out by hosts that don't belong to the network domain, sometimes they are called outsiders.
- **Internal attacks:** occur when malicious node from the network gains unauthorized access and acts as a genuine node and disrupts the normal operation of nodes.

## Network protocol & Security

- Network protocols are a set of rules and conventions that govern how data is transmitted and received over a network. These protocols define:
  - Format of data packets,
  - Error handling,
  - Addressing, and other aspects of network communication.

## TCP/IP protocol

- It is the foundation of modern networking. It consists of several layers, each with its own set of protocols.
  - i. **Application Layer:** This layer includes protocols like HTTP, FTP, SMTP, and DNS. It deals with application-level data and user interactions.
  - ii. **Transport Layer:** is responsible for end-to-end communication. It includes TCP for reliable, connection-oriented communication and UDP for connectionless communication.
  - iii. **Internet Layer:** is primarily governed by the IP. It is responsible for routing and addressing data packets to their destination across networks.
  - iv. **Link Layer:** includes protocols for the physical and data link layers of network communication. Ethernet and Wi-Fi are examples of link layer technologies.

## Attacks on different layer of TCP/IP model and their countermeasures

Layer	Attacks	Countermeasures
Application layer	E-mail bombing, Repudiation, data corruption, malicious code attack. Example: SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).	Input validation, output encoding, and parameterized queries.
Transport layer	Session hijacking, Altering checksum, Man in the Middle attack and SYN flooding.	Use Transport Layer Security (TLS) for encryption, employ firewalls and intrusion detection systems, and implement SYN/ACK cookies.
Network layer	IP spoofing, ICMP echo, Worm hole, black hole, gray hole, Byzantine, flooding, DDoS attacks, or routing attacks.	Implement packet filtering, use Access Control Lists (ACLs), and deploy intrusion detection and prevention systems (IDPS)
Data link layer	MAC address spoofing, ARP poisoning, or VLAN hopping Traffic analysis, disruption (E.g MAC IEEE 802.11 Wi-Fi)	Implement port security, use MAC address filtering, employ ARP inspection, and configure VLAN ACLs (Access Control Lists)
Physical layer	Wiretapping or eavesdropping on physical communication channels. Example: Jamming, interception, eavesdropping.	Use secure physical cabling and encryption technologies, like VPNs or TLS/SSL for higher-layer data protection.
Cross-layer attack	DoS, impersonation, replay, MiM attack.	Cross-layer traffic analysis

## Common security attacks and their countermeasures

Attacks	Countermeasures
Finding a way into a network	Firewalls
Exploiting software bugs, buffer overflows	Intrusion Detection Systems (IDS)
Denial of Service (DoS)	Access filtering, IDS
TCP hijacking	IPSec
Packet sniffing	Encryption (SSL, HTTPS)
Social problems	Education

## Malicious code

- A software written intentionally cause unanticipated or undesirable effects.
- Basic forms:
  - **Virus:**
    - Self-replicating software that attaches itself to other software.
    - Replicates within computer system, potentially attaching itself to every other program.
    - Innocuous, Humorous, Data altering, Catastrophic
    - Consists two parts:
      - Replicator - responsible for copying the virus to other executable Programs.
      - Payload - action of a virus (part of the virus that performs modification and corruption of data).
    - Anti-virus, proper firewall configuration and various scanners serve as pervention and detection techniques aganist virus.
  - **Worm:**
    - Computer program that can run independently, can propagate a complete working version of itself onto other host on a network, may consume computer resources destructively.
    - Stand-alone applications
    - Do not need a carrier program
    - Replicate by spawning copies of themselves.
    - More complex and harder to write than the virus programs.
    - Multitasking computers with open network standards are vulnerable.

- **Trojan horse:**

- A programs that appears to have a useful function, but also has a hidden and malicious purpose that evades security mechanism, sometimes by exploiting the legitimate authorization of the user who invokes the programs.
- A worm which pretends to be a useful program or virus purposely attached to a useful program prior to distribution.
- Untrained users are vulnerable.
- User training is one of the best prevention methods.

## **Authentication Mechanisms**

- Authentication is the process or action of verifying the identity of a user or process.
- Authenticator is an entity which is used to confirm the identity of a user.

## **Why do we need authentication?**

- To prevent attacks
- To revoke access from attackers
- To identify user's identity which required to allow access to confidential data.

## **How to authenticate a human to a machine?**

- Something the user knows
  - Passwords
    - Best practices
      - Choose passwords based on passphrase
      - Use password cracking tool to test for weak pwds
      - Require periodic password changes
    - Possible attacks
      - Denial of Service (DoS)
      - Dictionary attack : attacker pre-computes  $h(x)$  for all  $x$  in a dictionary of common passwords.
      - Other issues:
        - Too many passwords to remember
        - Failure to change default passwords
        - Social engineering
        - Bugs, keystroke logging and spyware

- Password cracking tools:
  - Password Crackers
  - Password Portal
  - L0phtCrack and LC4 (Windows)
  - John the Ripper (Unix)
- Something the user has
  - ATM and smart cards
  - Car key
  - 2-factor Authentication
- Something the user is
  - Biometrics
    - Desirable replacement for passwords.
    - Hard to forge
    - Hand Geometry:
      - Popular form of biometric
      - Suitable for authentication
      - Quick
      - Can't be used on very young and very old users
      - Relatively high equal error rate
    - Iris pattern:
      - Little or no genetic influence
      - Different even for identical twins
      - Pattern is stable through lifetime
      - Attackers could use photo of eye but it can be detected using scanner with light to be sure it's living iris.

# Chapter 2: Cryptography

---

## Basic terms

- **Cryptography**: the study of encryption.
- **Encryption**: process by which plain text is converted to cipher text.
$$C = E(P)$$
- **Decryption**: process of obtaining the plain text from the cipher text.
$$P = D(C)$$
- **Cryptography**: schemes for encryption and decryption.
- **Encryption algorithm**: technique or rules selected for encryption.
- **Key**: is secret value used to encrypt and/or decrypt the text.
- **Cryptanalysis**: study of “breaking the code”.
- **Cryptology**: cryptography and cryptanalysis.
- **Unconditional security**: when ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much computer power or time is available.
- **Computational security**: when decryption takes too long or too many resources more than the allocated.

## Characteristics of Cryptographic systems

- Operations used:
  - **Substitution** : replace (bit, letter, group of bits letters).
  - **Transposition** : rearrange the order.
  - **Product** : use multiple stages of both substitution and transposition.
- Number of keys used:
  - **Symmetric** : same key , secret-key, private-key.
  - **Asymmetric** : different key , public-key.
- Way in which the plain text is processed:
  - **Block cipher**
  - **Stream cipher**

## Substitution Ciphers

- **Caesar Cipher:**

- used by julius caesar.
- substitutes each letter of the alphabet with the letter standing three places further down the alphabet.

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

- Algorithm:

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

$$p = D(k, c) = (c - k) \bmod(26)$$

where k is secret key between 1 and 25.

- **Monoalphabetic Cipher:**

- rather than just shifting the alphabet monoalphabetic cipher could shuffle the letters arbitrarily. Each plaintext letter maps to a different random ciphertext letter with 26 letters long key.

$$E(x) = (ax + b) \bmod(26)$$

- $26! = 4 \times 10^{26}$  keys

- **Playfair Cipher:**

- a polyalphabetic cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
- the first digraph substitution cipher.
- Steps:
  - First create  $5 \times 5$  matrix and fill it using each character in the given key (no duplicate characters). Since the matrix can only contain 25 characters put i and j in the same cell.

Example: key = MONARCHY, plain text = INSTRUMENTS

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

- Split the given plain text to pair of letters:
  - If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter.  
Example: plain text = art -> "ar" "tz" where "z" act as bogus letter
  - Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.  
Example: plain text = hello -> "he" "lx" "lo" where "x" act as bogus letter
- For each pair of letters obtained in the second step, apply playfair cipher:
  - If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).
  - If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
  - If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
  - Using the above example we can apply playfair cipher like this:

Pair	Case	Cipher text
"IN"	Neither	"GA"
"ST"	Same row	"TL"
"RU"	Neither	"MZ"
"ME"	Same column	"CL"
"NT"	Neither	"RQ"
"SZ"	Neither	"TX"

$$C = E("INSTRUMENT") = "GATLMZCLRQTZ"$$

- Compared to monoalphabetic it's secured but can be easily broken if both plain text and cipher text are known.

- **Polyalphabetic ciphers:**

- uses multiple substitution alphabets.
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution.
- use a key to select which alphabet is used for each letter of the message:
  - use each alphabet in turn.
  - repeat from start after end of key is reached.

- **Vigenère Cipher:**

- simplest polyalphabetic substitution cipher.
- multiple Caesar cipher.
- Steps:
  - write the plaintext out.
  - write the keyword repeated above it.
  - use each key letter as a caesar cipher key.
  - encrypt the corresponding plaintext letter.

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

KEY: KEYKEYE  
 PLAIN: TRYTHIS  
 D

D V W D L G W

Finish  
 enciphering  
 (problem 1)

- The strength of the Vigenère cipher is that it is not susceptible to frequency analysis due to the fact that the cipher rotates through different shifts, so the same plaintext letter will not always be encrypted to the same ciphertext letter.
- A Vigenère cipher is difficult to crack using brute-force because each letter in a message could be encoded as any of the 26 letters. Because the encoding of the message depends on the keyword used, a given message could be encoded in  $26^k$  ways, where  $k$  is the length of the keyword.

- The primary weakness of the Vigenère cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the length of the key, then the ciphertext can be treated as interwoven Caesar ciphers, which, individually, can be easily broken. Repetitions in the ciphertext indicate repetitions in the plaintext, and the space between such repetitions hint at the length of the keyword.

## Transposition Ciphers

- Transposition ciphers differ from substitution cipher technique in addition to replace on alphabet with another they perform some permutation over the plain text alphabet.
- Used by modern encryption algorithms such as DES and 3DES.
- Steps:
  - write your plaintext message along the rows of a matrix of some size.
  - generate ciphertext by reading along the columns. The order in which we read the columns is determined by the encryption key.
- **Spartians Cipher (Spartan scytale):**
  - create  $key \times n$  matrix where  $n = \text{floor}(\text{length}/\text{key})$  then fill it with each letter in the plain text.

Exmaple: plain text = "Start the war today" key = 4,  $n = 16/4 = 4$

S	t	a	r
t	t	h	e
w	a	r	t
o	d	a	y

- combine each letter in the every column to get the cipher text.  
 $C = E(\text{"Start the war today"}) = \text{"stwottadahrarety"}$

- **Rail Fence Cipher:**

- Write the plaintext downwards on successive "rails" of an imaginary fence. When you get to the bottom start moving up.

Exmaple: plain text = "Start the war today" rails = 3

S				t				w		
	t		r		t		e		a	
		a				h				r

- Write the message line by line.

$$C = E(\text{"Start the war today"}) = \text{"stwt rteaahr"}$$

- **Columnar Transposition:**

- Write the message in rows of a fixed length, and then read out again column by column. The columns are chosen in some scrambled order. Both the length of the rows and the permutation of the columns are usually defined by a keyword.
- Any spare spaces are filled with nulls or left blank or placed by a character().

Exmaple: plain text = "Start the war today" key = "HACK", order of letter in the key = "4123"

H	A	C	K
3	1	2	4
S	t	a	r
_	t	h	e
_	w	a	r
_	t	o	d
a	y	_	_

$$C = E(\text{"Start the war today"}) = \text{"Sattwt yahaoredrd"}$$

- **Route Cipher:**

- The plaintext is first written out in a grid of given dimensions, then we read it off in a pattern given in the key.

Example: The key say: read message from top right corner down and to the left.

S	t	a	r
t	t	h	e
w	a	r	t
o	d	a	y

$$C = E("Start the war today") = "retyahrattadStwo"$$

## Crptanalytic Attacks

- Types of Attacks:
  - An attacker has only the ciphertext and his goal is to find the corresponding plaintext.
  - An attacker has a ciphertext and the corresponding plaintext and his goal is to find the key.
- Cryptanalytic attack exploits the characteristics of the algorithm.
- Brute Force Attack (BFA):**
  - the attacker tries to determine the key by attempting all possible keys.
  - time required to break the system by getting the secret key depends on the size of the

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/ $\mu$ s	Time Required at $10^6$ Decryptions/ $\mu$ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	$5.4 \times 10^{18}$ years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	$5.9 \times 10^{30}$ years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	$6.4 \times 10^6$ years

key.

- Ciphertext Only Attacks (COA):
  - In this method, the attacker has access to a set of ciphertext(s) but not the plain text.
  - COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack.
  - Modern cryptosystems are guarded against ciphertext-only attacks
- Known Plaintext Attack (KPA):
  - In this method, the attacker knows the plaintext for some parts of the ciphertext.
  - Know/suspect plaintext & ciphertext -> Find key or algorithm
  - The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method.

- Chosen Plaintext Attack (CPA):

- In this method, the attacker has the text of his choice encrypted. So he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key.
- select plaintext and obtain ciphertext -> select ciphertext and obtain plaintext -> select plaintext or ciphertext to en/decrypt.

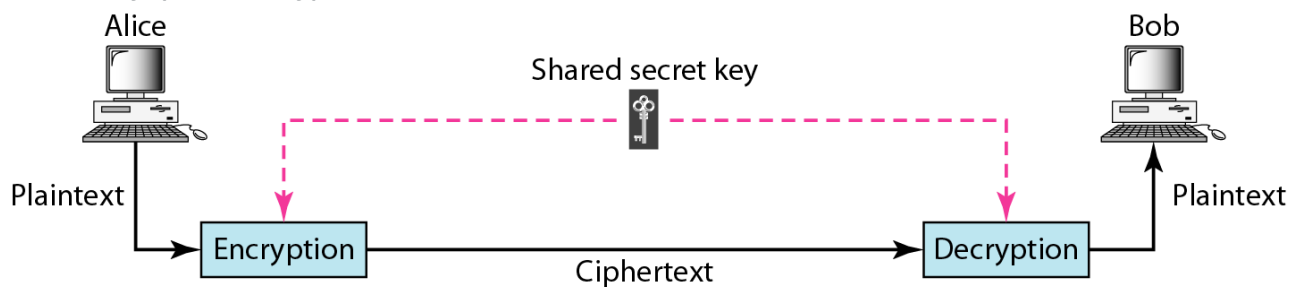
## Language Redundancy and Cryptanalysis

- Letters are not equally commonly used in English, E is by far the most common letter followed by T, R, N, I, O, A, S. Other letters like Z, J, K, Q, X are fairly rare.

## Categories of cryptography

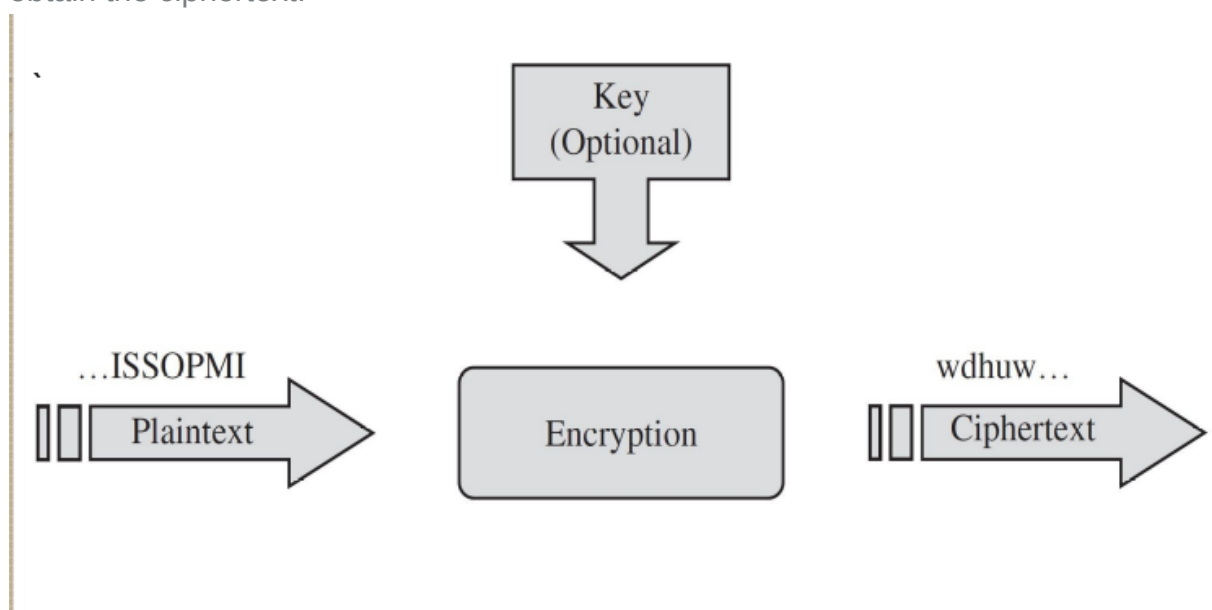
- Symmetric:

- same key (secret key) used between the sender and the receiver.



- Stream cipher:

- encrypt data one bit or one byte at a time.
- used if data is a constant stream of information.
- combines plaintext digits with a pseudo-random cipher digit stream (keystream) to obtain the ciphertext.



◦ Block cipher:

- operates on fixed length group of bits, called blocks, with an unvarying transformation.
- takes **n block of plain text as input** and **output a corresponding n block of cipher text**. Same thing applies for decryption.
- the exact transformation is controlled using **a second input** which is the **secret key**.

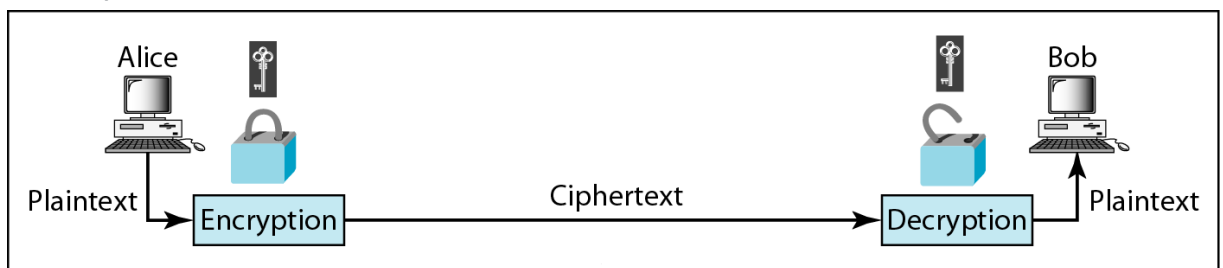
	Stream	Block
<b>Advantages</b>	<ul style="list-style-type: none"> <li>• <i>Speed of transformation.</i> Because each symbol is encrypted without regard for any other plaintext symbols, each symbol can be encrypted as soon as it is read. Thus, the time to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext.</li> <li>• <i>Low error propagation.</i> Because each symbol is separately encoded, an error in the encryption process affects only that character.</li> </ul>	<ul style="list-style-type: none"> <li>• <i>High diffusion.</i> Information from the plaintext is diffused into several ciphertext symbols. One ciphertext block may depend on several plaintext letters.</li> <li>• <i>Immunity to insertion of symbol.</i> Because blocks of symbols are enciphered, it is impossible to insert a single symbol into one block. The length of the block would then be incorrect, and the decipherment would quickly reveal the insertion.</li> </ul>
<b>Disadvantages</b>	<ul style="list-style-type: none"> <li>• <i>Low diffusion.</i> Each symbol is separately enciphered. Therefore, all the information of that symbol is contained in one symbol of ciphertext.</li> <li>• <i>Susceptibility to malicious insertions and modifications.</i> Because each symbol is separately enciphered, an active interceptor who has broken the code can splice pieces of previous messages and transmit a spurious new message that may look authentic.</li> </ul>	<ul style="list-style-type: none"> <li>• <i>Slowness of encryption.</i> The person or machine doing the block ciphering must wait until an entire block of plaintext symbols has been received before starting the encryption process.</li> <li>• <i>Padding.</i> A final short block must be filled with irrelevant data to make a full-sized block.</li> <li>• <i>Error propagation.</i> An error will affect the transformation of all other characters in the same block.</li> </ul>

◦ Shanon Substitution-Permutation ciphers:

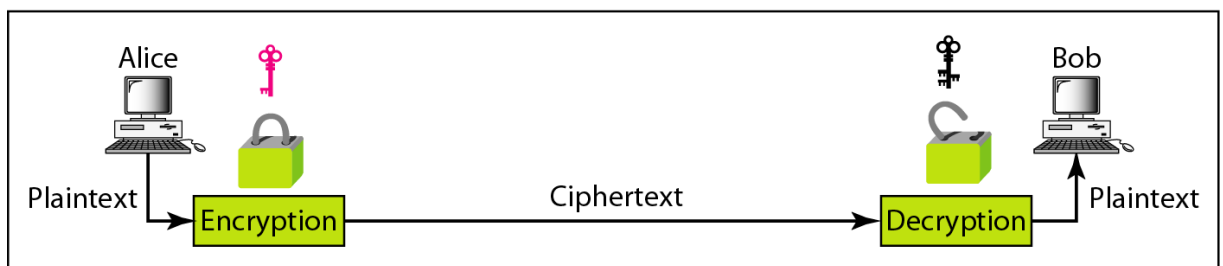
- contains two basic operations substitution (S-box) and permutation (P-box).
- **Diffusion** : dissipates **statistical structure of plaintext over bulk of ciphertext**.
- **Confusion** : makes relationship between ciphertext and key as complex as possible.
- **Characteristics of “GOOD” ciphers:**
  - The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
  - The set of keys and the enciphering algorithm should be free from complexity.
  - The implementation of the process should be as simple as possible.
  - Errors in ciphering should not propagate and cause corruption of further information in the message.
  - The size of the enciphered text should be no larger than the text of the original message.

- **Asymmetric:**

- uses two different keys private key (kept by the receiver) and public key (kept by the sender).



a. Symmetric-key cryptography



b. Asymmetric-key cryptography

## DES (Data Encryption Standard)

- DES encrypts 64-bit blocks by using a 56-bit key.
- Steps:
  - 56 bit of key produced by removing the 8 , 16 , 24 , 32 , 40 , 48 , 56 and 64 th bit of the original secret key.
  - 64-bit plain text block is handed over to an initial Permutation (IP) function.
  - The initial permutation is performed on plain text.
  - Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).
  - Now each LPT and RPT go through 16 rounds of the encryption process. 48 bit key generated from the 56 bit key in every round created by method called key transformation .
  - In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block

- The result of this process produces 64-bit ciphertext. ![DES-steps](media/DES-steps.png "steps in DES")

- Basic forms:

Form	Operation	Properties	Strength
<b>DES</b>	Encrypt with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
<b>Double DES</b>	Encrypt with first key; then encrypt result with second key	Two 56-bit keys	Only doubles strength of 56-bit key version
<b>Two-key triple DES</b>	Encrypt with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit keys	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
<b>Three-key triple DES</b>	Encrypt with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit keys	Gives strength equivalent to about 112-bit key about 72 quintillion ( $72 \times 10^{15}$ ) times as strong as 56-bit version

- Modes of operation:
  - Electronic Codebook (ECB) : Each 64-bit block is encrypted and decrypted independently.
  - Cipher Block Chaining (CBC) . Each 64-bit block depends on the previous one and uses an Initialization Vector (IV).
  - Cipher Feedback (CFB) . The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit.
  - Output Feedback (OFB) . Much like CFB, except that the encryption algorithm input is the output from the preceding DES.
  - Counter (CTR) . Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each subsequent block.
- weakness:
  - key size is small.
  - slower compared to AES and other algorithms.
  - vulnerable for exhaustive key search attack.

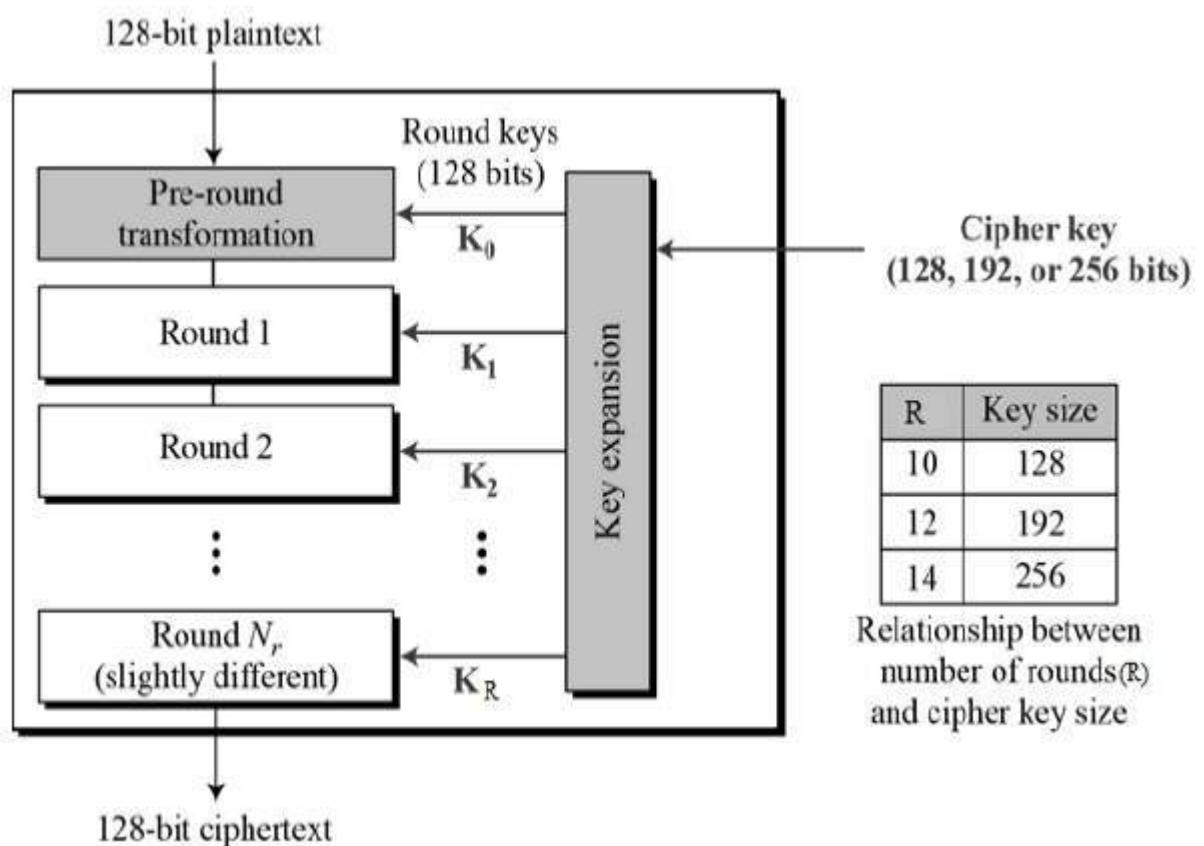
## AES (Advanced Encryption Standard)

- most popular and widely adopted symmetric encryption algorithm.
- introduced to replace DES.

- features:
  - symmetric key and symmetric block cipher.
  - relies on substitution-permutation network principle.
  - 128-bit data, 128/192/256-bit keys.
  - stronger and faster than Triple-DES.
  - provide full specification and design details.
  - software implementable in C and Java.
  - performs all its computations on bytes rather than bits.
  - variable number of rounds unlike DES.
- steps:
  - generates 16 byte from the 128 bit input using  $4 \times 4$  matrix.

```
[ b0 | b4 | b8 | b12 |
  | b1 | b5 | b9 | b13 |
  | b2 | b6 | b10 | b14 |
  | b3 | b7 | b11 | b15 ]
```

- total number of rounds and subkeys generated from the original symmetric key.



◦ each round comprises of 4 steps:

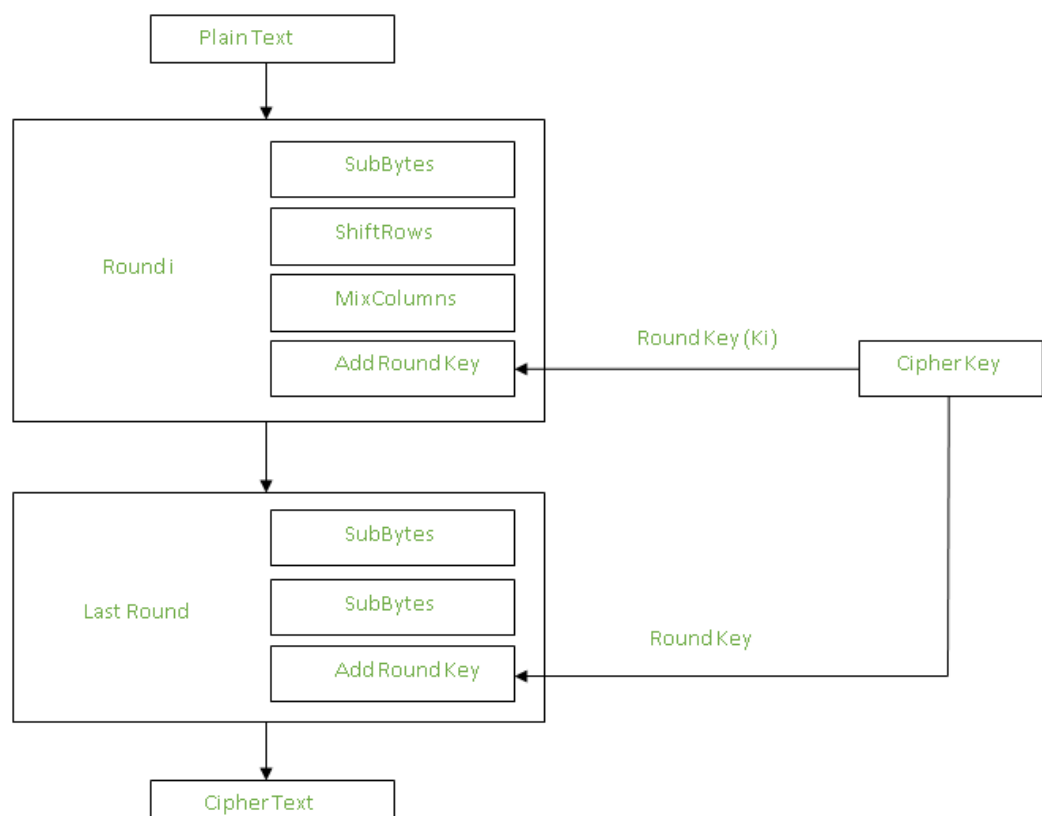
- SubBytes : performs substitution on each byte with another byte different from the original and the complement.
- ShiftRows : shifts a particular number of times.
  - The first row is not shifted.
  - The second row is shifted once to the left.
  - The third row is shifted twice to the left.
  - The fourth row is shifted thrice to the left.

[ b0   b1   b2   b3 ]		[ b0   b1   b2   b3 ]
b4   b5   b6   b7	->	b5   b6   b7   b4
b8   b9   b10   b11		b10   b11   b8   b9
[ b12   b13   b14   b15 ]		[ b15   b12   b13   b14 ]

- MixColumns : each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

[ c0 ]		[ 2 3 1 1 ]	[ b0 ]
c1	=	1 2 3 1	b1
c2		1 1 2 3	b2
[ c3 ]		[ 3 1 1 2 ]	[ b3 ]

- Add Round Key : resultant output of the previous stage is XOR-ed with the corresponding round key.



**DES vs AES**

	DES	AES
Developed	1977	2000
Key length	56 bits	128, 192 or 256 bits
Cipher Type	Symmetric block	Symmetric block
Block size	64 bits	128 bits
Security	Inadequate	Secure

**Issues with symmetric key cryptography**

- Large number of keys required if the number of communicating users increase.
- No support for digital signature.
- Security of exchange keys.

## Public key cryptography

- also known as asymmetric cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is secret (or private) and one of which is public.
- major parts:
  - Plaintext : message to be encrypted.
  - Encryption algorithm : performs substitutions and transformations to the plaintext.
  - Public and Private keys : a pair of keys, one for encryption and the other for decryption.
  - Ciphertext : this is the encrypted or scrambled message.
  - Decryption algorithm : generates the ciphertext and the matching key to produce the plaintext.

$$C = E(K_{pub}, P)$$

$$P = D(K_{priv}, C)$$

## Diffie-Hellman Mathematical Analysis

- Provided ability for messages to be exchanged securely without having to have shared some secret information previously.
- Inception of public key cryptography which allowed keys to be exchanged in the open.
- Avoided Man in Middle attack.

