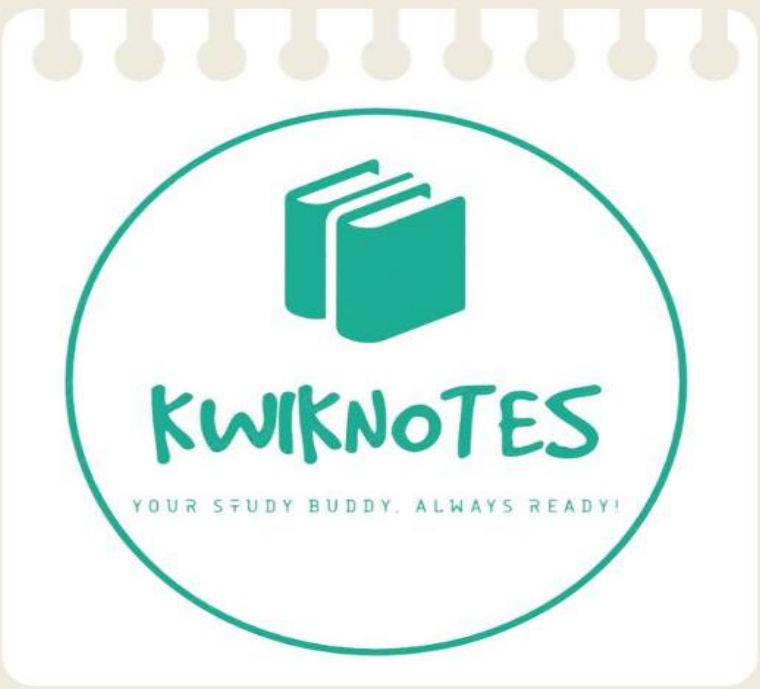


HANDWRITTEN NOTES

Download FREE Notes for Computer Science and related resources only at

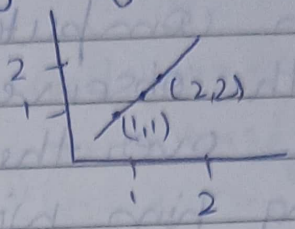
Kwiknotes.in

Don't forget to check out our social media handles, do share with your friends.

CG is creation of image by a computer Graphics are defined as any sketch or drawing that pictorially represent some meaningful information

COMPUTER GRAPHICS.

In Graphics any sketch, ~~joint~~, drawing, special artwork pictorialy depict an object to convey information instead of written description



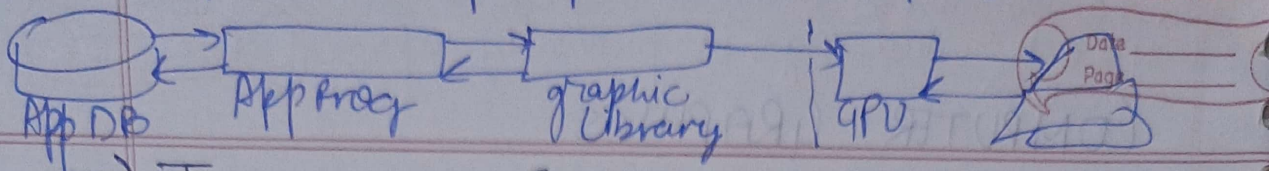
In computer graphics, pictures or graphic objects are presented as a collection of discrete picture elements called pixels.

- Pixel is the smallest addressable screen element
- It is the smallest piece of display screen which we can control
- The control is achieved by setting the intensity and color of pixil which compose the screen.
- Computer graphics is concerned with all the aspects of producing images using a computer. It concerns with the pictorial synthesis of real and imaginary objects with the help of computer based models.

Types of computer graphics

-> Non interactive computer graphics also called passive computer graphics / offline
- The observer has no control over the image.
- Examples - Static websites, logo & titles shown on tv, screen saver
- Involves 2 way communication b/w comp & user in interactive

components - Ip, processing, Display / output



→ Interactive Computer graphics
- also called online graphics.
- It involves a two way communication between computer and user.
- Here the observer is given some control over the object by providing him with an input device as per its requirements
- Video games, dynamic websites, special effects in movies, cartoons are all making use of interactive computer graphics.

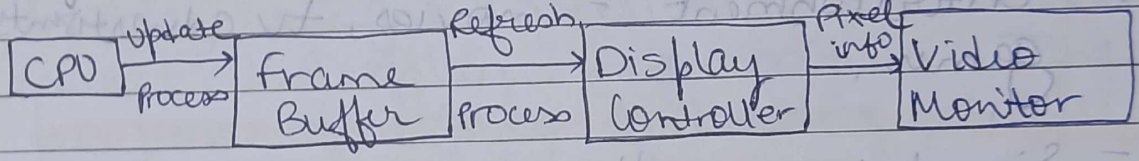
Components: buffer
- Digital Memory: It is also known as frame buffer. This is a place where images of pictures are stored as an array (matrix of 0 and 1, 0 represents darkness and 1 represents image or picture) Frame buffer is the video ram (VRAM) used to hold the image displayed on the screen. can be implemented using shift registers
- The amount of memory required to hold the image dependents primarily on the resolution of the screen image and also color depth used per pixel.
gas display → discharge
- TV monitor: Monitor helps us to view the display and they make use CRT (Cathode Ray Tube) technology
- Display Controler: It is an interface

3 Components - Digital Memory Buffer
DTG Display Controller, TV Monitor

between digital memory buffer and tv monitor
The main function of this is to pass the contents of frame buffer to the monitor

- The display controler reads each successive byte of data from frame buffer memory and converts zero's and one's (0's & 1's) into corresponding video signals.
- This signal is fed to tv monitor to produce a blank and white picture on the screen.

Digital controller acts as mediator b/w digital memory buffer



Applications of Computer Graphics.

- Graphical User interface (GUI) - typical components used in this are:
  - Menus, Icons, Scroll bars, buttons
  - 3rd interface.

- Plotting in business / graphs, curves, charts, bargraphs, pichart, etc

- Office automation. - all tools of MS office.

- Desktop publishing (DTP)
  Desktop publishing is the use of computer and specialized software to create documents for printing and the web.

Multimedia, Education & training, generating maps, visualization, Printing tech, GUI, Architecture Entertainment.

- Plotting in science and technology
- Commercial publishing and advertisements
- Science CAM / CAD
  These are eng applications
- Scientific visualizations & - using animation, understandings some patterns, (genetics, bio-technology
- Entertainment - movies, tv advertisments, games.
- Simulators - flight simulators, car racing simulators.
- Cartography - creation of maps, charts used in civil eng., zeological applications
- Multimedia - multimedia is content that uses combination of different content forms such as text, audio, images, animations, video and interactive content.

by Advantages of interactive Graphics:

- A better information recognition process
- It is possible to offer higher information density.
-

Display devices
video monitor based on CRT
It is a vaccum tube

- We can show object relationps
- Colors can be used
- Greater productivity achieved

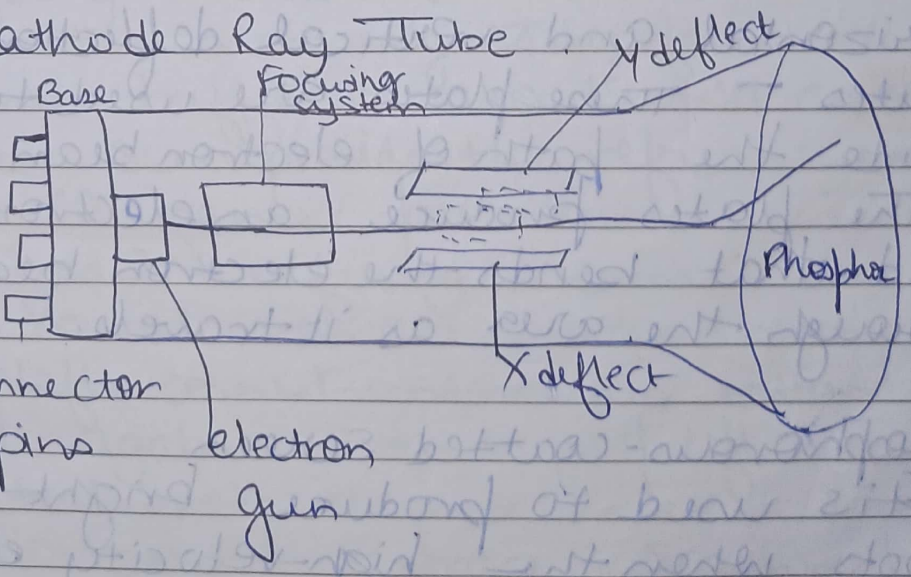
display devices are output devices used to represent info in form of images called VDU. Simplify information sharing.

Display devices in comp graphics
The display device is an output devices used to represent the information in the form of images
- Display systems are mostly called a video monitor or video display unit (VDU)

Display devices are designed to view, model, display information. The purpose of display technology is to simplify information sharing.

Examples - Cathode Ray Tube, Color CRT Monitor, Liquid Crystal Display (LCD), LED (Light Emitting diode Direct view storage Tubes (DVST), Plasma display.

1) Cathode Ray Tube



control grid - control flow of electrons.

- CRT is a technology used in tradional computer monitor and television.
- CRT is a particular type of vaccum tube that display images when an electron beam collides that display images when electron beam collides on the radiant surface.

Compnents of CRT.

- Electron gun - the electron gun is made up of several elements, mainly a heating filament (heater) and a cathode. The electron gun is a source of electrons, focused on a beam facing the CRT, generate negatively charged electron, accelerated towards phosphorus screen.

focusing and accelarating anodes
These anodes are used to produce a narrow and a sharply focused beem of electrons. To make, get clearpic

Horizontal and vertical deflection plates - These plates are used to guide the path of electron beam The plates produce an electromagetic field that bends the electron beam through the area as it travels.

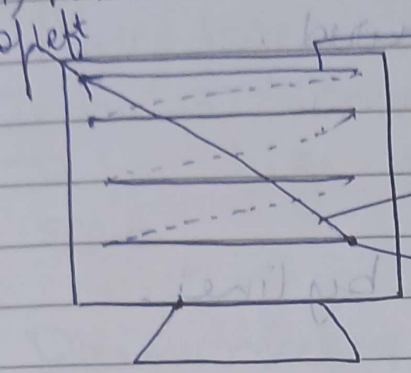
- Phosphorous-coatted screen
It is used to produce bright spots when the high-velocity electron beam hits it.

Matrix stored in Memory Buffer

29 Sep.

There are 2 ways to represent an object on screen / 2 ways to draw pic on screen

1) Radar Scan



Rectangular pattern of image capture. Entire screen is scanned. Employs CRT. Electron beam sweeps across the screen from top to bottom. One line at a time. Based on television technology

- Raster Scan is a scanning technique in which electron beam moves along the screen. It moves from top to bottom, covering one line at a time.
- A raster scan is based on pixel intensity controlled display as a rectangular box on the screen called Raster
- Picture description is stored in memory area called as refresh / frame buffer.

Raster can be explained as a rectangular collection of dots or points. A image is subdivided into various horizontal lines refered as scan lines further divided into pixels which help in processing image.

- Refresing means to redraw the information from the memory. Image formed called Raster image
- frame buffer is also known as Bit Map
- Raster scan provides the refresh rate of 60 to 80 frames per second.
- It has 2 refresing beams
  i) Vertical retrace: when beam starts from top left corner and reaches bottom right and again return to top left, it is called vertical retrace
  ii) Horizontal Retrace: Scanning from left to right, covering one line at a time

Refreshing done at 60-80 frames per sec

Contains 2-4 bits per pixel

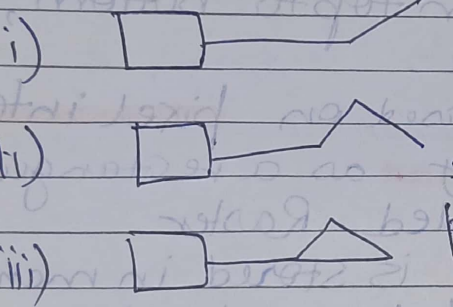
Advantages

1) Real image is drawn
2) Many colors can be produced
3) Dark scenes can be pictured.

Disadvantages

1) Less Resolution
2) It display pictures line by line.
3) It is more costly.

→ 2) Random Scan / Vector Scan



Beam of electron directed only to screen. Called vector scan as it display/draw a picture in form of one line at a time.

It is also known as ~~stroke~~ writing Display

In this electron beam points only to the area in which picture is to be drawn.

It uses an electron beam like a pencil to make a line image on the screen

The image is constructed from a sequence of straight line segments.

On the screen, each line segment is drawn by the beam to pass from one point to other. where its x and y

Coordinates define each point.
After compilation of picture drawing the refresh rate of is 30 to 60 frames per second.

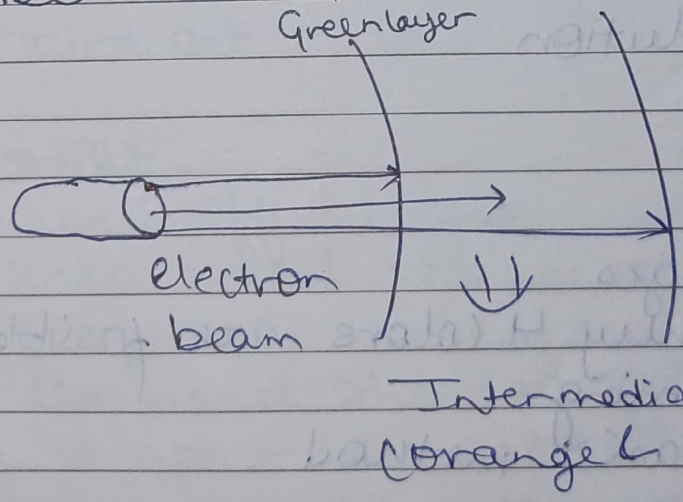
Advantages
- It draws smooth line
- It has high resolution compared to raster scan

Disadvantages
- It does only wire frame
- It creates complex scenes due to flicker

COLOR CRT MODEL

Basic idea behind colored crt model is to combine 3 basic colors - Red Green blue. By using these 3 colors we can produce millions of different colors

2 Basic color producing techniques are
1) Beam Penetration Method - Random Scan.



BPM is similar to simple CRT, but makes use of multicolor phosphorus no. of layers. Each layer responsible for 1 colour

This produces four colours only, red green orange yellow
slow beam - red, high beam - green.

- It is used with a random scan monitor for displaying pictures. There are 2 phosphorous layers - red and green are coated inside the screen. The color shown depends on how far the electron beam penetrates the phosphorous surface.

- A powerful electron beam penetrates the CRT, it passes through the red layer and excites the green layer within.

- A beam with slow electrons excites only the red layer.

- A beam with medium speed of electrons, a mixture of red and green light is emitted to display 2 or more colors.

Advantages of Beam penetration.

- Better Resolution
- Half Cost
- Inexpensive

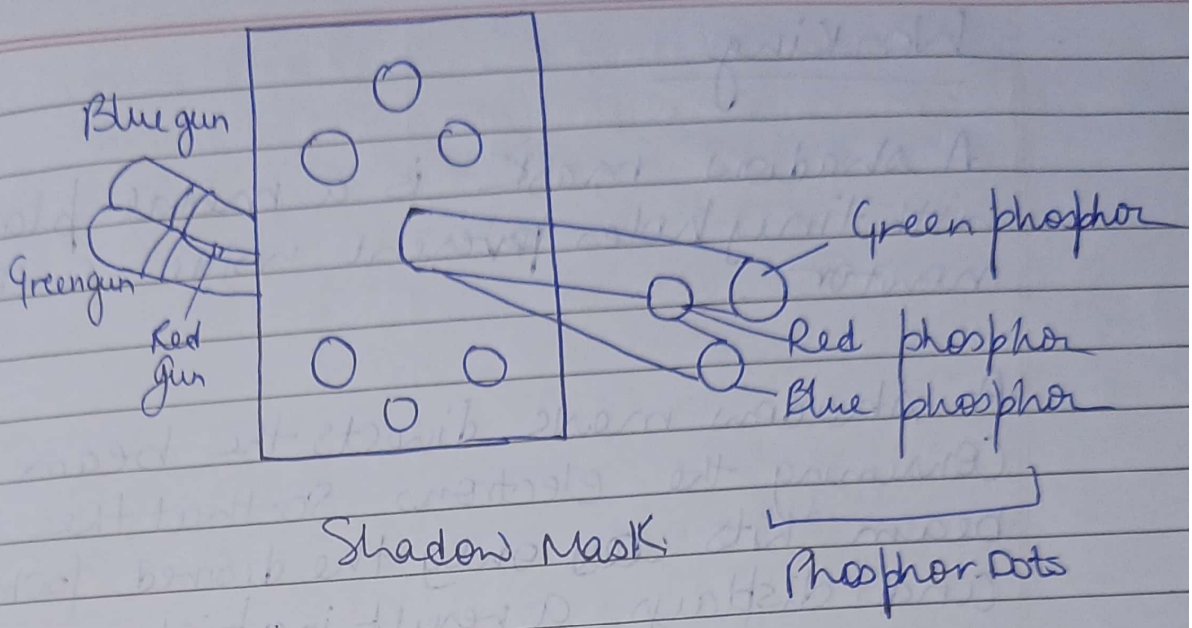
Disadvantages

- Mainly only 4 colors are possible
- Time consuming

* Shadow mask method.

used in Raster scan

Shadow Mask - Raster Scan



It is used with Raster scan Monitor for displaying pictures. It has more range of colors then the beam penetration method It is usid in television sets and monitors.

Structure Of Shadow Mask.

1. It has 3 phosphorous color dots at each position of the pixel
   a) ~~Red color~~ First Dot - Red Color
   b) Second Dot - Green Color
   c) Third Dot - Blue Color

~~Raster Dot~~

1. It has 3 diffirent guns each for one color
2. It has a metal screen or plates just before the phosphorous screen, named "Shadow mask"
3. It also has a shawdow grid just behind the phosphorous coated screen with tiny holes in a triangular shape

Working

A shadow mask is a metal plate with tiny holes present inside a color monitor.

A shadow mask directs the beam by consuming the electrons so that the beam hits only the desired point and displays a resulting picture

It has 3 different guns. These guns direct their beams to shadow mask, which allow them to pass. It is a task of a shadow mask to direct the beam on its particular dot on the screen and produce a picture on the screen.

A shadow mask can display a wider Range of pictures then beam penetration

Advantages

- Display a wider ranges pictures realistic images
- In-line arrangement of RGB color
- ~~Expensive~~

Interlacing

first pass) odd no scan the refresh
second pass) even no scan the refresh

Disadvantages
- Expensive
- Difficult to cover all beams on same hole

Raster Scan → Interlacing

In interlacing mode, the electron gun sweeps alternate lines on each pass. It is a description of how image is created. Pic created by scanning every alternate line. Allows faster Refresh Rate, cause flickering.

In the first pass, odd-numbered lines are refused and in the second pass, even no. lines are refreshed. This allow refresh rate to be doubled because only half the screen is redrawn at a time.

Interlacing is primarily used with the lower refreshing rates

Difference b/w Random & Rastar Scan

Random	Raster
· It draws only lines and characters	· It has ability to display areas filled with solid colors or patterns.
· It dont use interlacing	· Uses interlacing
· The beam is moved between the end points the graphics primitives	· The beam is moved all over the screen once scan line a time from top to bottom a then back to top
· Higher Resolution	· lower Resolution
· More expensive	· Less expensive

Uses monochrome or beam penetration type	Uses monochrome or shadow mask
Random display draws, and a continuous and smooth lines	Raster display can display mathematically smooth lines, polygons and boundaries of curved primitives
Editing is easy	Editing is difficult
Refresh ~~rate~~ rate depends directly on picture complexity	Independent of picture complexity
Scan conversion is not required	Scan conversion Required

LCD flat panel display technology used in TV & monitors. Use liquid crystal instead of cathode Ray

The LCD depends on light modulating properties of liquid crystals.

LCD is used in watches and portable computers

Support for large resolution & better pic quality

LCD requires AC power supply instead of DC, so it is difficult to use in circuits. Don't have refresh rate

Consume less power

It generally works on flat panel display technology. LCD consumes less power then LED. LCD screen uses the liquid crystal to tell pixels on or off.

lp

Liquid crystals are mixtures of solid and liquid. When the current flows inside it, its position changes to desired colors.

Advantages

1) Produce a bright image.
2) Energy efficient
3) Completely flat screen.

Disadvantages

1) Fixed Resolution
2) Lower contrast
3) More expensive

Display Device LED (Light emitting Diode)

- LED's are device which emmits when current passes through it. • LED is a semiconductor device.
- The size of LED is small, so we can easily make any display unit by arranging a large no. of LED's.
- LED consums more power compared to LCD. LED used in TV, smartphones, moto vehicles, traffic lights
- LED are powerful in structure, So they are capable of withstanding mechanical pressure; LED also works at high temperatures.

c-intercept
x-intercept

Ad

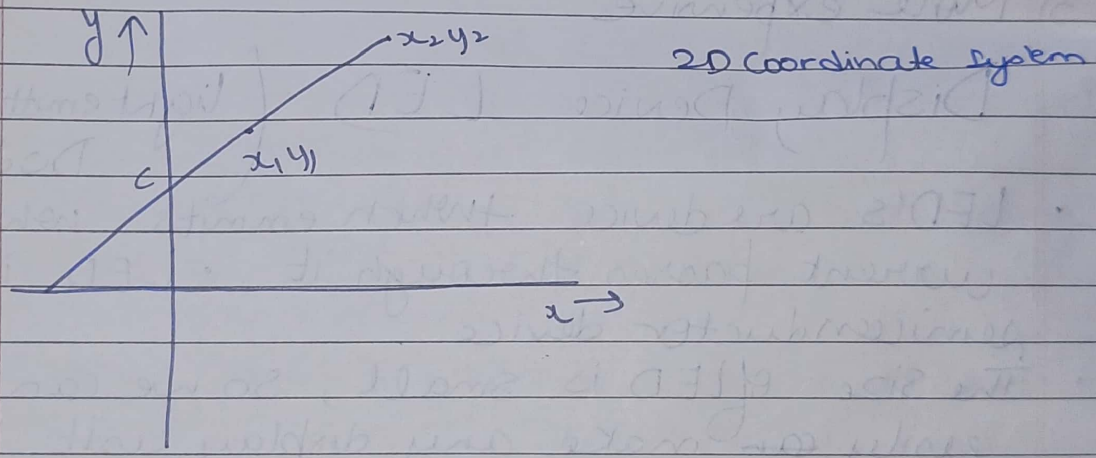
- Capable of handeling high temperature
- The intensity of light can be controlled
- low operational voltage

Dis

- More power consuming than LCD

6 oct

DDA Digital Differental Analyzer



a) Line - it is infinite in dimension
Part of a line is called line segment.
A line segment has 2 confined points or a line is collection of points

b) Line equation
i) $y = mx + c$ m = slope, c = intercept on y axis
ii) When 2 points are given

$$\frac{y-y_1}{x-x_1} = \frac{y_2-y_1}{x_2-x_1}$$

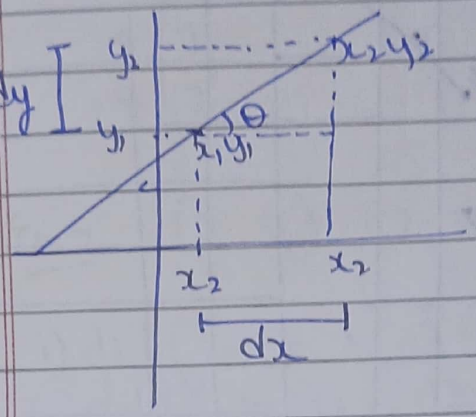
$\theta = m$

iii) Intercept

$$\frac{x}{a} + \frac{y}{b} = 1$$

In CG eq① is used. *//

c) Slope of line

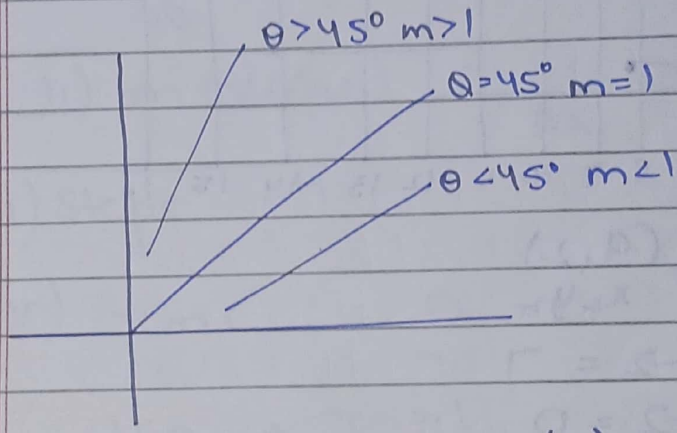


$$\theta = \frac{\Delta y}{\Delta x} \text{ or } \frac{dy}{dx}$$

$$\tan\theta = \frac{dy}{dx} \quad -(II)$$

$$m = \frac{dy}{dx} \quad -(I)$$

from ① & (II) $m = \tan\theta$



Case I : $\theta = 45°$ slope (m) will be 1

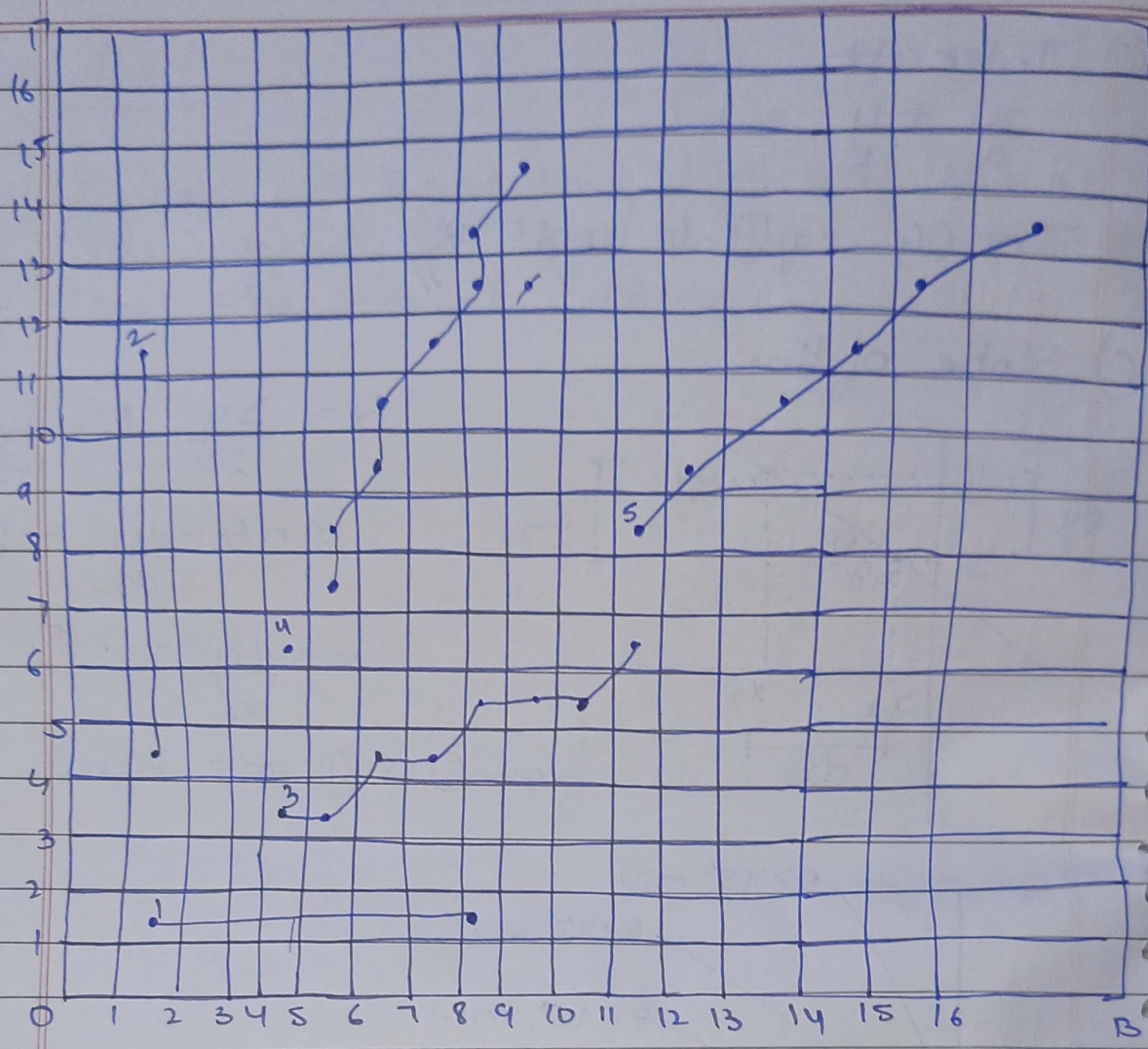
Case II : $\theta < 45°$ slope will be less than 1

Case III : $\theta > 45°$ slope will be greater than 1

in coordinate system.

Case I

When θ is 45 slope (m) is 1 in coordinate system



Ex-1 $(2,2)$ $(9,2)$
$x_1\ y_1$ $x_2\ y_2$

i) diff in $x = 9-2 = 7$
diff in $y = 2-2 = 0$

ii) m (slope) $= \frac{\Delta y}{\Delta x} = \frac{0}{7} = 0$

iii) Steps (max of $\Delta x, \Delta y$) $= 7$

iv) $x_{inc} = \frac{\text{diff in } x}{\text{steps}} = \frac{7}{7} = 1$

$y_{inc} = \frac{\text{diff in } y}{\text{steps}} = \frac{0}{7} = 0$

inc by 1 → inc by 0.

x	y
2	2
3	2
4	2
5	2
6	2
7	2
8	2
9	2

Ex 2 (2, 5) (2, 12)

i) diff in x = 2 − 2 = 0.
diff in y = 12 − 5 = 7.

ii) m (slope) = $\frac{\Delta y}{\Delta x} = \frac{7}{0} = \infty$

iii) Steps = 7

iv) x inc = $\frac{0}{7} = 0$

y inc = $\frac{7}{7} = 1$.

v)

x	y
2	5
2	6
2	7
2	8
2	9
2	10
2	11
2	12

Ex-3 (5,4) (12,7)

i) $\Delta x = 7$
$\Delta y = 3$

$m = \frac{\Delta y}{\Delta x} = \frac{3}{7} = 0.4$

Steps = 7

$x_{inc} = \frac{7}{7} = 1$

$y_{inc} = \frac{3}{7} = 0.4$

x	y	Roundoff	
5	4	4	(5,4)
6	4.4	4	(6,4)
7	4.8	5	(7,5)
8	5.2	5	(8,5)
9	5.6	6	(9,6)
10	6.0	6	(10,6)
11	6.4	6	(11,6)
12	6.8	7	(12,7)

Case I when $m < 1$

$x_{K+1} = x_K + 1$

$y_{K+1} = y_K + m$

Case II $m > 1$

Ex-4 (5,7) (10,15)

$\Delta x = 10 - 5 = 5$

$\Delta y = 8$

steps = 8

$m = \frac{\Delta y}{\Delta x} = \frac{8}{5} = 1.6$

$x_{inc} = \frac{\Delta x}{steps} = \frac{5}{8} = 0.6$

$y_{inc} = \frac{\Delta y}{steps} = \frac{8}{8} = 1$

0.6 1

Round	x	y	Points
5	5	7	5,7
6	5.6	8	6,8
6	6.2	9	6,9
7	6.8	10	7,10
7	7.4	11	7,11
8	8.0	12	8,12
9	8.6	13	9,13
9	9.2	14	9,14
10	9.8	15	10,15

Case II when $m > 1$

$x_{k+1} = x_k + \frac{1}{m}$

$y_{k+1} = y_k + 1$

5/ Case III $m > 1$

(12, 9) (17, 14)

$\Delta x = 17 - 12 = 5$

$\Delta y = 14 - 9 = 5$

$m = \frac{5}{5} = 1$

Steps = 5

$x_{inc} = \frac{\Delta x}{steps} = \frac{5}{5} = 1$

$y_{inc} = \frac{5}{5} = 1$

x	y	
12	9	12, 9
13	10	13, 10
14	11	14, 11
15	12	15, 12
16	13	16, 13
17	14	17, 14

Self

In a 2 dimensional plane, if we connect two points (x_1, y_1) and (x_2, y_2) we get a line segment. But in CG, we cannot directly join any 2 coordinate points, for that we should calculate intermediate point coordinates and put a pixel for each intermediate point of desired colour.

Algorithm

if (dx

dy

if (a

else

xin

yinc

for (

y

DDA

algorith

scan co

In this

at eac

steps

Advan

1) It is

direc

mult

dete

y

poss

indi

Algorithm DDA (x_1, y_1, x_2, y_2)

```
{ dx = x2 - x1
  dy = y2 - y1
  if (abs (dx) > abs (dy))
        steps = abs (dx)
  else
        steps = abs (dy)
  xinc = dx / steps;
  yinc = dy / steps;
  for (i = 1 ; i <= steps ; i++) {
        putpixel (x1, y1);
        x1 = x1 + xinc;
        y1 = y1 + yinc;
  }
}
```

DDA stands for Digital Differential Method algorithm. It is an incremental method of scan conversion of line. In this method calculation is performed at each step by using results of previous steps.

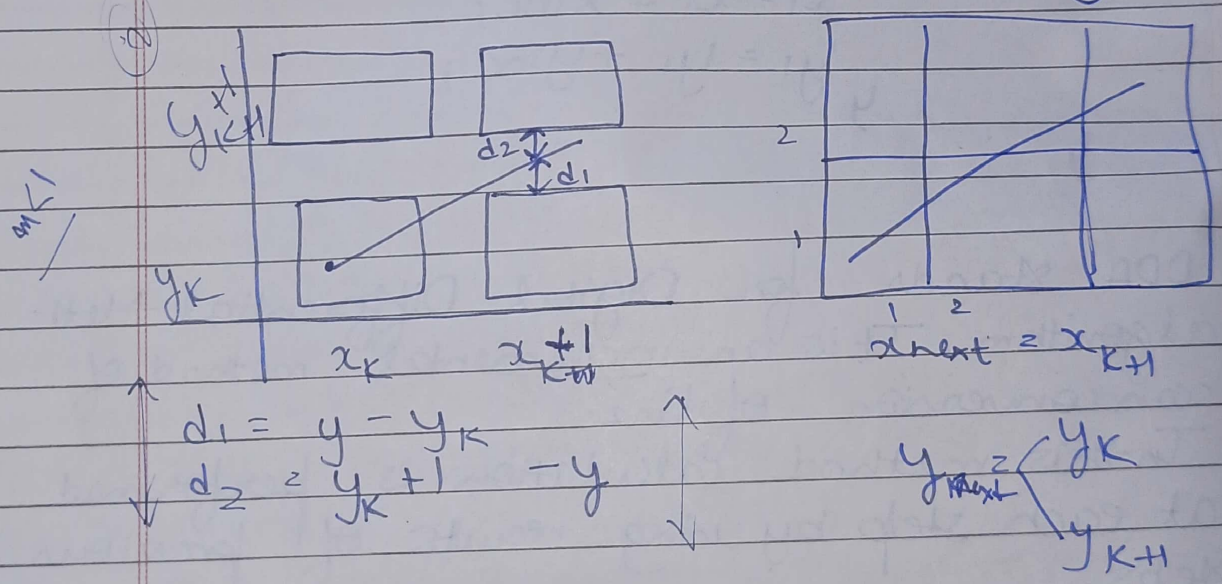
Advantage:

1) It is a faster method than method of using direct line equation 2) This method doesn't use multiplication theorm. 3) It allows us to detect the change in the value of x and y, so plotting of same point twice is not possible. 4) This method gives overflow indication when a point is repositioned

Disadvantage

1) It involves floating point additions, rounding off is done, accumulations of roundoff errors cause accumulation of errors
   Poor endpoint accuracy.
2) Rounding of operation and floating point operations consumes a lot of time. It is more suitable for generating line using software but it is less suited for hardware implementation

Bresenham Line Drawing



$d_1 = y - y_k$

$d_2 = y_{k+1} - y$

$y_{next} = \begin{cases} y_k \\ y_{k+1} \end{cases}$

The line is passing through (1, 2) and (2, 2) to decide which pixel will be choosen Bresenham derivation is used.

$y = mx + c$

$y = m(x_k + 1) + c$

$d_1 = y - y_k = m(x_k + 1) + c - y_k$

$d_2 = y_{k+1} - y = y_{k+1} - [m(x_k + 1) + c]$

$= y_{k+1} - m(x_k + 1) - c$

if $d_1 - d_2 < 0 \Rightarrow y_k$

if $d_1 - d_2 > 0 \Rightarrow y_k + 1$

let us calculate $d_1 - d_2$ and define decision parameter

$d_1 - d_2 = m(x_k + 1) + c - y_k - [y_k + 1 - m(x_k + 1) - c]$

$= m(x_k + 1) + c - y_k - y_k - 1 + m(x_k + 1) + c$

$= 2m(x_k + 1) - 2y_k + 2y_k + 2c - 1$

$\because m = \frac{\Delta y}{\Delta x}$

$= 2\frac{\Delta y}{\Delta x}(x_k + 1) - 2y_k + 2c - 1$

Multiply Δx both sides

$\Delta x(d_1 - d_2) = \Delta x\left[\left(2\frac{\Delta xy}{\Delta x}(x_{k+1}) - 2y_k + 2c - 1\right]\right.$

$\Delta x(d_1 - d_2) = 2\Delta y(x_k + 1) - 2\Delta x y_k + 2c\Delta x - \Delta x$

$\underbrace{\Delta x(d_1 - d_2)}_{p_k} = 2\Delta y x_k - 2\Delta x y_k + \underbrace{2\Delta y + 2c\Delta x - \Delta x}_{\text{constant}}$

$p_k = 2\Delta y x_k - 2\Delta x y_k$

$p_{next} = 2\Delta y x_{next} - 2\Delta x y_{next}$

$p_{next} - p_k = 2\Delta y x_{next} - 2\Delta x y_{next} - 2\Delta y x_k + 2\Delta x y_k$

$= 2\Delta y (x_{next} - x_k) - 2\Delta x (y_{next} - y_k)$

if $p_{next} - p_k < 0 \Rightarrow$ Remain on y_k

if $p_{next} - p_x > 0 \Rightarrow$ Remain on $y_k + 1$

$p_{next} - p_k = 2\Delta y (x_{k+1} - x_k) -$

~~$2\Delta x (y_{k+1} - y_k)$~~

$p_{next} = p_k + 2\Delta y$ ——— (I)

Case II:

$p_{next} - p_k = 2\Delta y (x_{k+1} - x_k) - 2\Delta x (y_{k+1} - y_k)$

$p_{next} = p_k + 2\Delta y - 2\Delta x$ ——— (II)

$\because y_1 = mx_1 + c$

$y_1 = \frac{\Delta y}{\Delta x} x_1 + c$

$c = y_1 - \frac{\Delta y}{\Delta x} x_1$

$p_k = 2\Delta y x_k - 2\Delta x y_k + 2\Delta y + 2\Delta x c - \Delta x$

$= 2\Delta y x_k - 2\Delta x y_k + 2\Delta y + 2\Delta x \left[y_1 - \frac{\Delta y x_1}{\Delta x} \right] - \Delta x$

$= 2\Delta y x_k$

$- 2\Delta y x_1 - 2$

$p_k = 2\Delta$

DDA

Q (2, 5) an

$\Delta x =$

$\Delta y =$

$m = \frac{\Delta}{}$

Steps

xinc

yinc

$= 2\Delta y x_k - 2\Delta x y_k + 2\Delta y + 2\Delta x y_1 - 2\Delta y x_1 - \Delta x$

$- 2\Delta y x_1 - 2\Delta x y_1 + 2\Delta y + 2\Delta x y - 2\Delta y x_1 + x$

$p_x = 2\Delta y - \Delta x$

DDA

Q (2,5) and (2,12)

$\Delta x = 0$

$\Delta y = 7$

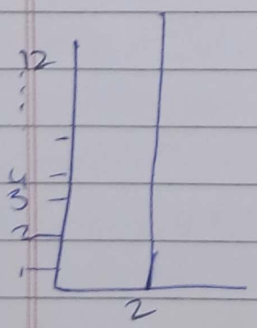
$m = \frac{\Delta y}{\Delta x} = 0$

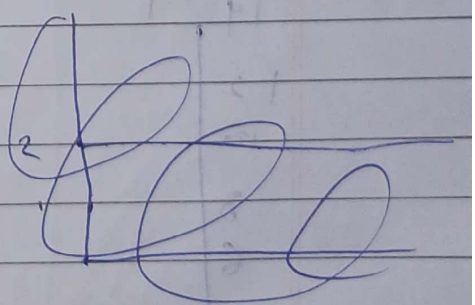
Steps = 7

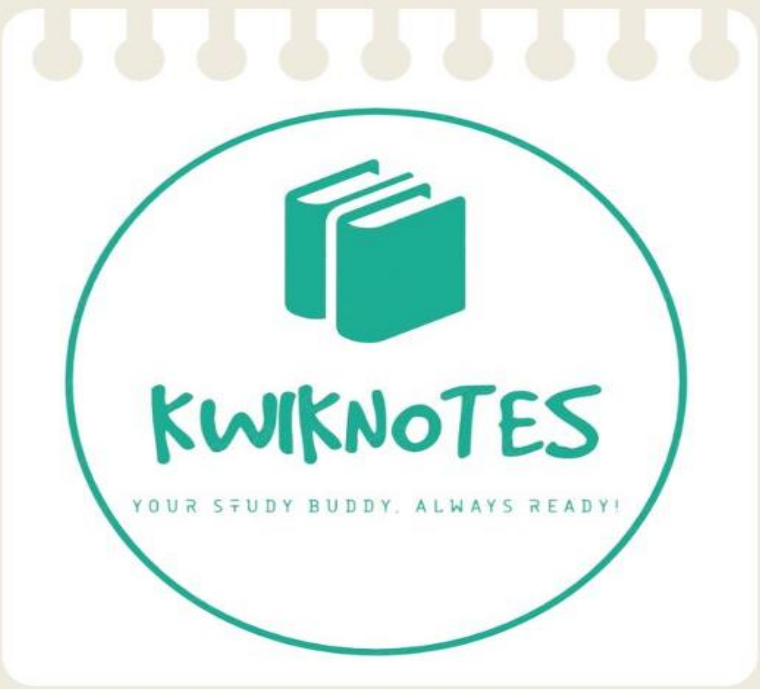
$x_{inc} = \frac{\Delta x}{steps} = \frac{0}{7} = 0$

$y_{inc} = \frac{\Delta y}{steps} = \frac{7}{7} = 1$

x	y
2	5
2	6
2	7
2	8
2	9
2	10
2	11
2	12







HANDWRITTEN NOTES

Download FREE Notes for Computer Science and related resources only at

Kwiknotes.in

Don't forget to check out our social media handles, do share with your friends.

Cyber Security

branch of CS

It is the practice of protecting critical systems. It helps to protect Organisations and individual from cyber attacks
It is a technique of protecting internet connected system such as computer, mobile, electronic system, etc from malicious attacks known as Cyber security.
Cyber is technology that includes systems n/w, programs & data.

Also called Electronic Info Security or info technology Security.

Cyber Law

Also called internet laws protect people from crimes through internet.
These are included in Info Technology Act 2000

Cyber law offers legal protection for people who are using internet.

Threat

It relates to the security of comp being compromised. A threat can lead to an attack.
It can harm / violate comp systems / h/w, etc.

Cyber Threat

It reflects the Risk of experiencing a cyber attack.
These are malicious attacks performed by individuals with harmful intent, whose goal is to steal data, cause damage or disrupt computing system.

ex- Phishing attack, SQL injection, Ransomware - as - a service, IOT

Aeroline
Date: / /
Page No:
visit us at www.aerolineproducts.com

Attempt to exploit or to steal info & money and are developing capabilities to disrupt, destroy or break essential services.

Malware
is a file or code typically derived our a n/w, that infects, exposes & steals or conduct virtually any behaviour an attacker wants. Desig to harm/steal or n/w.
- Computer virus - Ransomeware - Worms - Trojan Horse.

Trojan Horse
It is a type of malware that donloads onto a comp disguised as a legitimate program. It appears to be Harmless
It can't Replicate like virus & worm
It hides itself in a program.
Provide unauthorized access to comp, send files, delete files or make unwanted changs.

CRYPTOGRAPHY

It is a technique of securing information & communications through use of codes so that only authorized user can access the information

Crypt - hidden Graphy - writing

It is obtained through mathematical concepts and a set of Rules based calculation known as algo to convert message so that it is hard to decode

Plain text $\xrightarrow{\text{Algo}}$ Cipher text

Features
- Confidential
- Authentication
- Non - Repudiation
- Integrity

Encryption is an important part of cryptography. method by which users can convert plain text to cipher or coded text using some algo to hide info's true meaning.

Plain text $\xrightarrow{\text{Encryption}}$ Cipher text

- Symmetric
- Assymtric

Cypher text

It is the encrypted text which is a result of encryption algo over plain text. Can't be read until converted to plain text with a key

OSI Security Arch.

Security & safety are the main pillars of cyber technology.
OSI (Open System Interconnection) Security Architecture defines a systematic Approach to provide security at each layer. It defines Security Services & mechanisms that can be used at each seven layers of model to ensure transmissio of data securely over n/w.

These servica & mechanism ensure confidentiality, integrity, availability of data.

Three Concept.

1) Security Attack

It is an attempt by a person or entity to gain unauthrized access or disrupt or compromise

Aeroline
Date: / /
Page No:
visit us at www.aerolineproducts.com

Security of a system, network/device.

Set of actions a person take to gain any unauthorized acess which cause damage
These type of actions put org's safety at Risk.
2 categories

Passive Attack -
It is a type of attack that dosnot alter system or data. In this third party intruder tries to access message/content/data being sharld by Sender & Receiver by intruptiy n/w.
Attack observe/monitor network without actively disrupting or altering
- Eavesdropping - listening to comm b/w two or more parties by packet Sniffing or non intrusive
- Traffic Analysis - involve analyzing n/w traffic & metadata. Here can't reading but understand pattern & length.

Active Attacks

It involve the attacker actively or disrupting / altering system, n/w, device Generally focused on causing damage or disruption, rather than gathering info

Here sender, receiver have no idea that message is altered by third party

- Masquerade - where attacks pretends to be authorized sender to gain access
- Replay - in which attacker intercepts a transmitted msg
- Modification of message
- Denial of Service (DOS)

2) Security Mechanism

It is a means of protecting a system, n/w or device against unauthorized access

A mechanism designed to detect & prevent or recover from security attack.
Responsible for protecting a system against security threat

These can be implemented within system, on network, or to provide CIA

- Encipherment (Encryption)

- Digital signature - Create unique, verifiable identifier for digital doc or message by using cryptography

- Traffic padding - used to add extra data to n/w to hide true content

- Routing control - selection of secure Routers for transmission

3) Security Services

It refers to different Services available for maintaining security & safety of org

Security mechanism are used to ~~prevent~~ implement security services

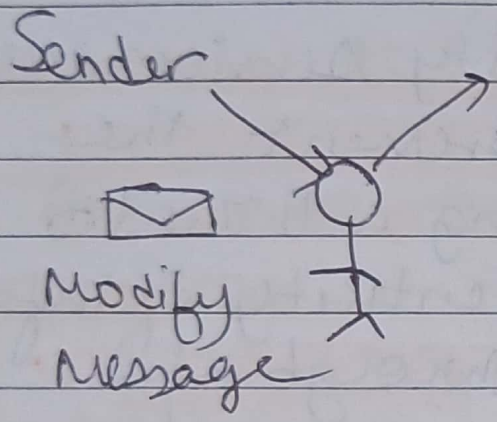
Help to prevent potential security risk

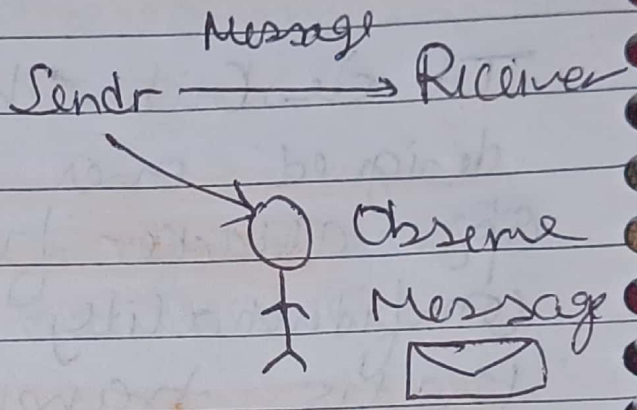
5 typs

- Authentication - verify user to grant access
- Access control - determine who is allowed to access resource
- Data confidentiality - for protection of info
- Data integrity - use of techinques to ensure data is not tempered
- Non Repudiation - Create verifiable Record of origin

Confidentiality (access)
Integrity (Accuracy)

Active v/s Passive





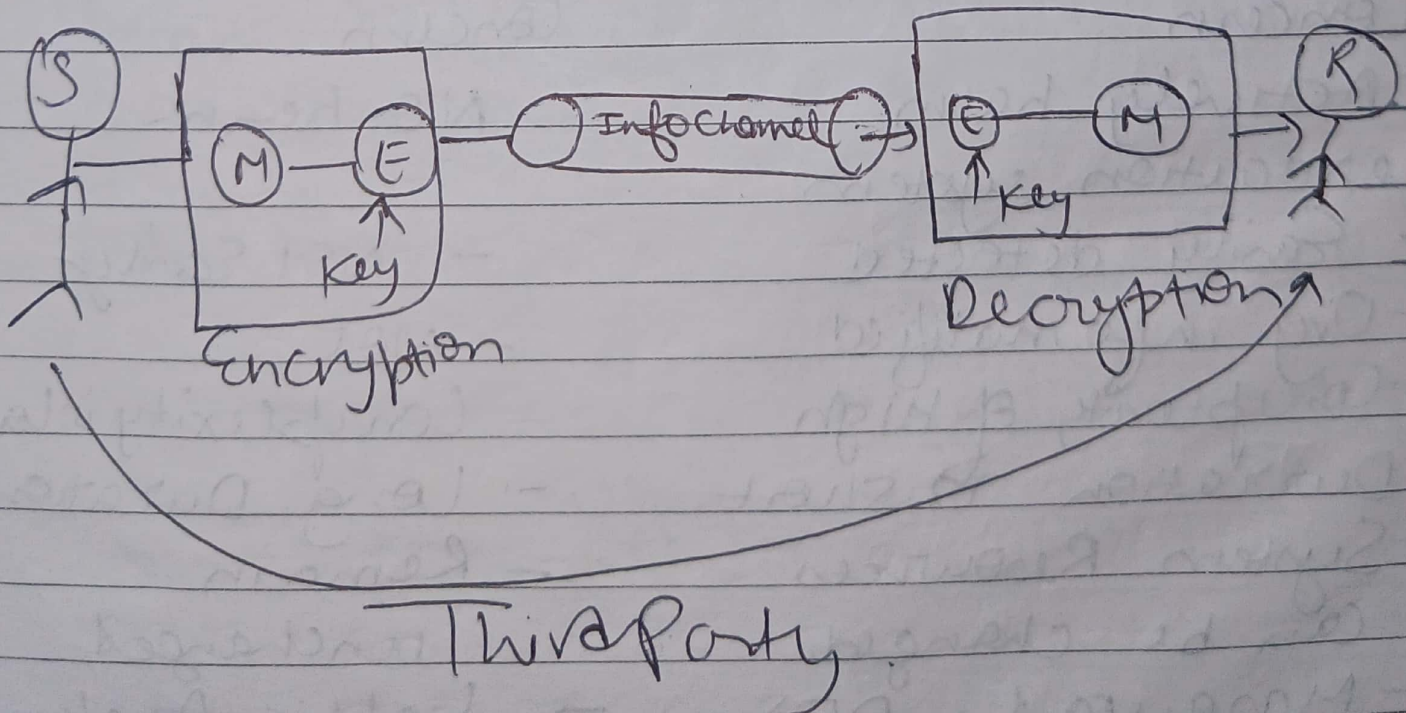
- Modification of msg
- Danger to integrity & Availability
- Prevention is main concern
- Actively harm execution system
- Easily detected
- Org info modified
- Complexity of High
- Duration is short
- System Resources can be changed
- Masquerade, DOS Mod of Message

NO modification
- Danger to Confidentiality
- Detection is main Concern
NO harm
- NOt Easily
- NOt
- Complexity is low
- Long Duration
- Remain unchanged
- traffic Analysis

Network Security Model

It describes how security services are designed over n/w to prevent the attacker from causing a threat to confidentiality or authenticity of info that is transmitted through n/w

It can be achieved through firewalls Access control, Virtual Private n/w (VPN) etc.



logical channel

When we send data from source to Destination, it require a communication channel to send a message

A trusted third parted maybe needed to achieve secure transmission

Any security service has 3 components:
1) Security Related transformation on info to send
2) Some secret info shared by 2 parties, unknown to attacked
3) A trusted third party to achieve secure trans. It may be responsible to provide info, settle disputes

One Key used

Symmetric Cryptography

Type of cryptography which uses single key to encrypt & decrypt.
Symmetric encryption is called a "secret key" encryption because the key must be secret from third parties

Ex - AES, DES, 3DES

Ingredients

1) Plain text - org message or data that is fed to algo as input

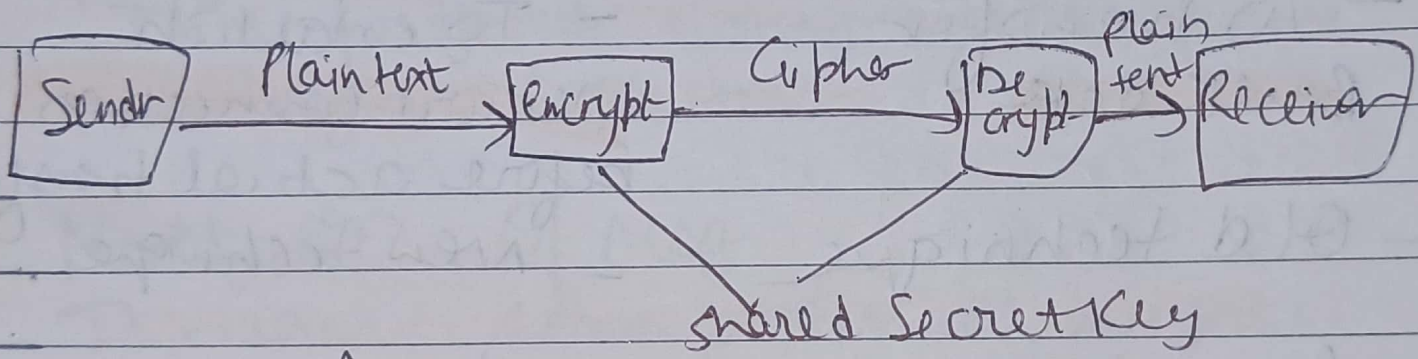
2) Encryption Algo - Set of mathematical calculation performed on plain text to convert to cipher

3) Secret key - also an input to encryption. Exact transformation & substitution depen

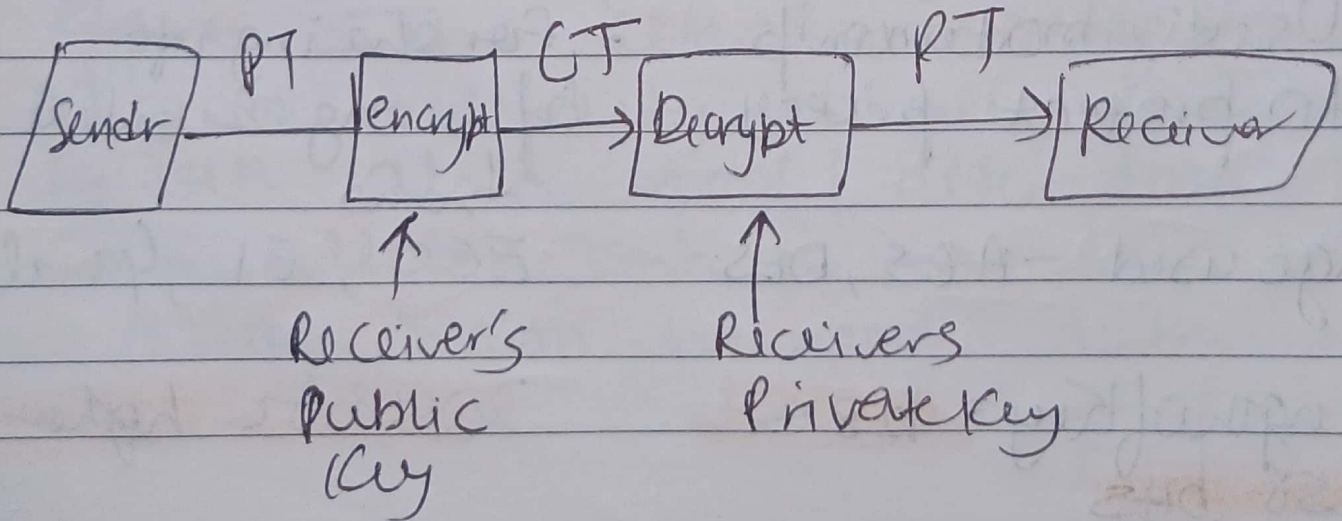
Cipher text - produced as output of encryption algo protected by secret key
decryption algo produces same as org text

Decryption Algo - Reverse of encryption algo

Symmetric V/S Assymtric



Symmetric



Aeroline
Date: / /
Page No: AS
visit us at www.aerolineproducts.com

S 3

- Single shared key	Two diff key for en & dec
- Size of cipher text could be same or smaller than plain text	- Size of ciper text could be same or larger than plain text
- Encryption process is faster as single key is used	- Slower as 2 diff key used, Keys compiled by mathematical process
- To transfer Bulk data	- To establish secure connection before actual transfer
- Old technique	- New technique
- less secure	- More secure
- low resource req	- More req
- Used in modern comp to protect privacy	- for sharing info b/w org & online trans.
- Algo used - AES, DES	ECC, EI, Gamal
- length of key = 128 or 256 bits	2048 or higher

types

Aeroline
Date: / /
Page No:
visit us at www.aerolineproducts.com

Active Attacks 3

Masquarade

takes place when one entity pretends to be other entity or authorized entity. type of active attack

A type of threat whereby unauthorized entity gain access to a system or perform a malicious act

It is performed using stolen pass & login credentials.

Modification of Msg

It means some portion of msg is altered or the msg is delayed or reordered to produce unauthorize effect. It is attack on integrity

Unauthorised party not only gain access to data also spoof / alter data.

Ex - allow John to read data to allow Smith to read data

done by either sender/Receiver
Sender ask host to transfer later
deny

Repudiation

This attack occurs when n/w is not completely secure or login has been tampered. Either done by sender or receiver. Sender of Receiver may deny that they have not send msg.

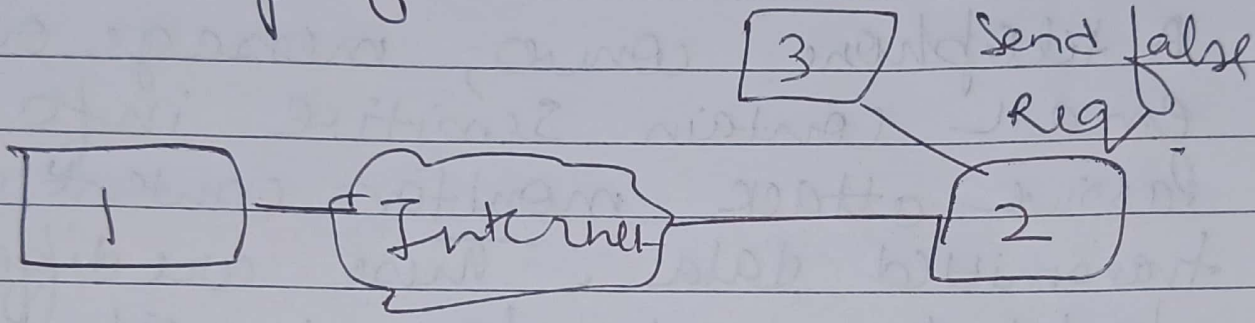
Replay

Involve passive capture of msg
Risk to data sent over n/w
Attacker capture traffic & send comm to org destination, acting as original sendr.
Main feature is that client receive message twice. one by sender, one by third party

DOS

Prevent normal use of communication facilities. This attack may have specific target. It causes

disruption of entire n/w either by disabling n/w or by overloading it with messages to degrade performance

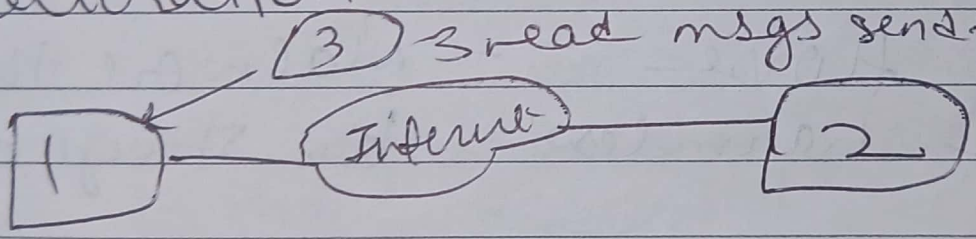


Trojan Horse - Malware that appear harmless & stays hidden, download unknowingly.

Passive

Release of Message Content

A telephone convo, message or email contain sensitive info. Passive attack monitor content of transmitted data. These are difficult to detect as it don't involve alteration



Traffic Analysis

In this the attacker observes the pattern, of length & frequency of message exchanged rather that actual data.