SURA'S

TNUSRB
SUB-INSPECTOR (TECHNICAL) EXAM

❖ **GENERAL KNOWLEDGE** ❖ **TECHNICAL**

Diploma Std.

V.V.K. Subburaj

SURA COLLEGE OF COMPETITION
Chennai

© PUBLISHERS

TNUSRB SUB-INSPECTORS (TECHNICAL) EXAM

V.V.K. Subburaj

ISBN: 978-93-6417-462-6
Code : B1189

[NO ONE IS PERMITTED TO COPY OR TRANSLATE IN ANY OTHER LANGUAGE THE CONTENTS OF THIS BOOK OR PART THEREOF IN ANY FORM WITHOUT THE WRITTEN PERMISSION OF THE PUBLISHERS]

SURA COLLEGE OF COMPETITION

Head Office: 1620, 'J' Block, 16th Main Road, Anna Nagar,
Chennai - 600 040. Phones: 044-48629977, 42043273

Printed at G.T. Krishna Press, Chennai - 600 102 and Published by
V.V.K.Subburaj for Sura College of Competition
1620, 'J' Block, 16th Main Road, Anna Nagar, Chennai - 600 040.
Phone : 044-48629977.
email: enquiry@surabooks.com; suracollege@gmail.com; website: www.surabooks.com

CONTENTS

Pages

TNUSRB SI Technical Solved Original Question Paper - 2018 with explanatory answers 1 - 20

❖ GENERAL AWARENESS 1 - 240

❖ **TECHNCIAL**

ELECTRONICS AND COMMUNICATION ENGINEERING (THEORY) 1 - 144

BASIC ELECTRICAL PRINCIPLES
BASIC PRINCIPLES OF ELECTRONICS
ELECTRONIC DEVICES AND CIRCUITS
POWER SUPPLY, AMPLIFIER AND OSCILLATORS
NUMBER SYSTEM, BOOLEAN ALGEBRA AND LOGIC GATES
ELECTROMAGNETIC FIELDS,
TRANSMISSION LINES & NETWORKS
MICROWAVE ENGINEERING
MICROPROCESSOR AND ITS APPLCIATIONS
ANTENNAS AND PROPAGATION
COMMUNICATION ENGINEERING & SYSTEM
COMMUNICATION DEVICES AND THEIR TECHNOLOGIES
PROGRAMMING AND APPLICATION OF COMPUTERS
PROGRAMMING IN "C"

ELECTRONICS AND COMMUNICATION ENGINEERING (MCQs) 1 - 16

✷ CURRENT EVENTS

TNUSRB
SUB-INSPECTORS (TECHNICAL) EXAM

ONLIINE COMPUTER BASED TEST OR WRITTEN EXAMINATION AND DISTRIBUTION OF MARKS :-

All the eligible candidates will be called for Online Computer Based Test or Written Examination

The distribution of marks are as follows:-

Sl.No	Tests	Marks
1.	Written Examination	80 Marks
	(a) General knowledge	30 Marks
	(b) Technical subjects	50 Marks
2.	Marks for additional educational qualification	5 Marks
3.	Special Marks for **open candidates** NCC, NSS & Sports / Games	5 Marks
	Departmental candidates National Police Duty Meet Gold, Silver and Bronze medals.	
4	Viva-voce	10 Marks
	TOTAL	100 Marks

ELECTRONICS AND COMMUNICATION ENGINEERING

- **Basic Electrical Principles**
- **Basic Principles of Electronics**
- **Electronic Devices and Circuits**
- **Power Supply, Amplifier and Oscillators**
- **Number System, Boolean Algebra and Logic Gates**
- **Electromagnetic fields, Transmission lines & Networks**
- **Microwave Engineering**
- **Microprocessor and Its Applciations**
- **Antennas and Propagation**
- **Communication Engineering & System**
- **Communication Devices and their Technologies**
- **Programming and Application of computers**
- **Programming in "C"**

ELECTRONICS AND COMMUNICATION ENGINEERING

1. BASIC ELECTRICAL PRINCIPLES

Introduction to Electricity

Electricity is the integral part of human lives like water, space, land, fire and air. The human life is dominated by electrical and electronic gadgets, hence, the learning and understanding of their working principle is well advised for proper handling, maintenance and troubleshooting of those devices. Hence, we will discuss the history and basic principles of electricity in this Chapter.

History of Electricity

In June 1752, American Scientist Benjamin Franklin, tried to prove that lightning is a phenomenon of electricity by flying a kite with conductive rods to attract lightning to a Leyden jar, which was an early form of a capacitor. When a kite was flying at a certain height, he observed an electric spark and felt electric shock slightly, which proved that lightning is electric in nature. In 1800, in Paris (France), Italian scientist Alessandro Volta proved that his invention, "Voltaic Pile" produced electricity.

Electricity

It is a kind of energy that one cannot see as like air. It's existence can only be known through the working of electrical appliances. Also its existence can be found using line tester and multimeter.

Generation of Electricity

In 1831-32, a British scientist Michael Faraday invented electromagnetic generator using Faraday's laws of electro magnetism which produced Alternating current. Nikola Tesla, Serbian-American inventor contributed the design of modern A.C supply system.

Types of Power Generation

Important types of power generation are

1. Hydroelectric power station
2. Thermal power station
3. Atomic power station
4. Wind Power station
5. Natural Gas power station
6. Solar power station (D.C)

Types of Electricity

Generally there are two types of Electricity. They are:

1. Alternating Current (AC)
2. Direct Current (DC)

Alternating Current

The direction of current varies with time is called as alternating current. It has two terminals viz., phase and Neutral. If the phase terminal acts as 'Positive', then neutral terminal acts as 'Negative' terminal. If phase terminal acts as 'Negative', then neutral terminal acts as 'Positive' terminal.

If you test the phase terminal with a line tester, you may see the light indication in the tester. Neutral shows no indication. Neutral is a common terminal used as a return path current flowing from phase to neutral through the connected device. It is neither 'Positive' nor 'Negative'.

Voltage and Frequency of Household AC Supply In our country, the voltage and frequency of single phase AC supply is maintained as 220V/50Hz. In Foreign Countries, particularly in U.S.A, it is maintained as 110V/60Hz AC. Figure 1.1 shows the waveform of the alternating current.

Amplitude

Amplitude is the distance from the X-axis to the vertex or peak of the any one half cycle of the AC waveform. Its unit is volt.

Polarities

The top half cycle is positive half cycle and the bottom half cycle is negative half cycle. Both half cycles combined together to form the one complete full cycle.

Wavelength

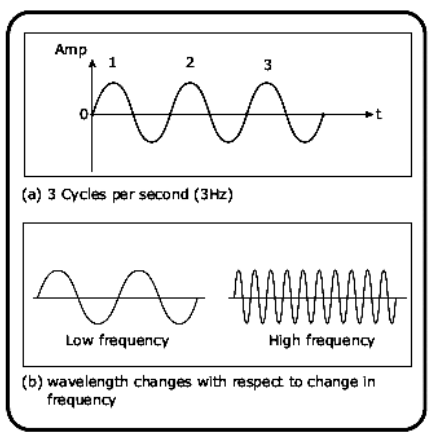
The length from starting point of the wave to the finishing point, which includes one positive half cycle and one negative half cycle, is called wavelength. Its unit is meter.

Peak to Peak Value

The distance between positive peak and negative peak is referred as peak to peak value. Its unit is volt.

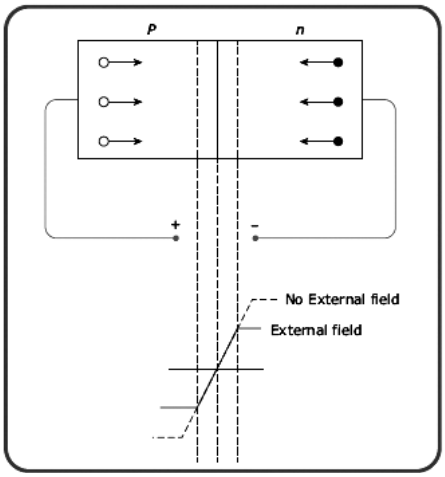
Frequency

The number of complete cycles per second is called Frequency. Its unit is Hertz (Hz). Higher value units are Kilo-Hertz (KHz), Mega-Hertz (MHz), Giga Hertz (GHz) and so on. If there are three full cycles occur in one second, then its frequency is 3 Hertz. Low frequency has long wavelength and high frequency has short wavelength.



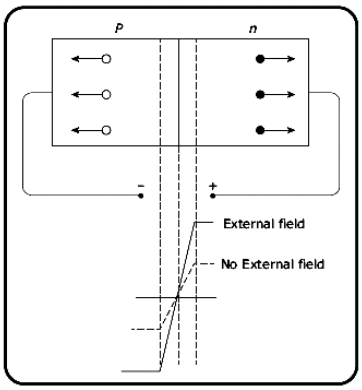
Frequency of the AC waveform

Forward Biasing



Forward bias

To apply forward bias, connect positive terminal of the battery to p-type and negative terminal to n-type as shown in Figure above. Due to this, barrier potential is very much reduced. Positive terminal of the battery repels holes in p-side and negative terminal of the battery repels electrons in n-side. Because of this, current flows in the circuit. This is called "forward current". The magnitude of current depends upon the applied forward voltage.



Reverse bias

Reverse Biasing

"When the external voltage applied to the junction is in such a direction that potential barriers is increased, it is called reverse biasing"

To apply reverse bias, connect negative terminal of the battery to p-type and positive terminal to n-type as shown in Figure below. Because of increase in barrier potential the width of the depletion layer is also increased. As a result, the increased potential barrier prevents the flow of charge carriers (majority carriers) across the junction and hence the current does not flow.

3. ELECTRONIC DEVICES AND CIRCUITS

We are experiencing many hoardings, advertising displays, high definition television in our daily routine life. Of course, these devices have very good features with long life and attractive characteristics. Most of these devices are built around a special type of semiconductor devices called LED, LDR, LCD, photodiode and photo transistor. They are optoelectronic devices. With these devices we study about the working of FET, MOSFET, SCR, DIAC, TRIAC, IGBT and their application.

Light Emitting Diode (LED)

LED is a PN junction device, which emits light when forward biased, by a phenomenon called electroluminescence. In all semiconductor PN junctions, some energy will be radiated as heat and some in the form of photons.

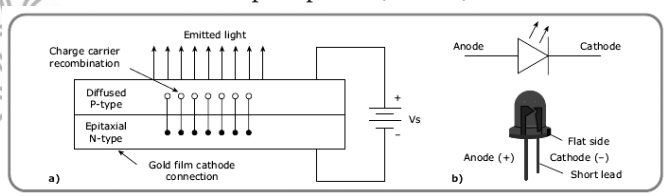
LEDs are widely used in indicators, smart phones, digital watches, solid state video displays, calculators, digital computers, electronic panels and optical communication system.

Construction

Figure below shows the construction of LED and its symbol. Here, an N type layer is grown on a substrate over which a P type layer is deposited by the process called diffusion.

The metal anode connection is made at the outer edges of the 'P' layer. It provides more central surface area for the light to escape. LEDs radiate different colours like red, green, yellow, orange, blue and white depend on material used. Some LEDs emit infrared (invisible) light also. The colour of the emitted light depends on the type of material used as given below.

- Gallium arsenide (GaAs)–Infrared Radiation (Invisible)
- Gallium phosphide (GaP) –Red or Green
- Gallium arsenide phosphide (GaAsP)- Red or Yellow



Construction and Symbol of LED

Working Principle

When an LED is forward biased, the electrons and holes move towards the junction and recombination takes place. This makes the electrons lying in the conduction band of N region fall into the holes lying in the valence band of P region.

The difference of energy between the conduction band and the valance band is radiated in the form of

the light energy. The brightness of the emitted light is directly proportional to the forward bias current.

Advantages

- LED can be switched ON and OFF at very fast speed (1 ns).
- Its operating voltage is from 1.5 V to 3.3 V with low current (some mA).
- It has a life time of 1,00,000 hours. LEDs are small in size and light in weight.
- They require no heating and warm up time.

Seven Segment LED

LEDs are often grouped to form seven segment displays. They are generally used as numerical indicators and consist of a number of LEDs arranged as seven segments.

The seven LEDs are labelled A through G. By forward biasing different LEDs, we can display the digits 0 to 9. For example, if LEDs A,B,C, D and G are lit (by forward biasing them), then the display will show the number 3.

There are two types of seven segment LED arrangement, they are

- Common Anode Type
- Common Cathode Type

Liquid Crystal Display (LCD)

Liquid Crystal Display (LCD) are used for displaying of numeric and alphanumeric character in dot matrix and segmental displays. There are two types of liquid crystal materials used, they are nematic and cholesteric. In the Nematic Liquid Crystal (NLC), all the molecules align themselves approximately parallel to a unique axis, while retaining the complete translational freedom.

The liquid is normally transparent, but if subjected to a strong electric field, disruption of the well-ordered crystal structure takes place causing the liquid to polarise and turn opaque. The removal of the disruption of the crystal structure regains its original form and the materials become transparent.

They are,

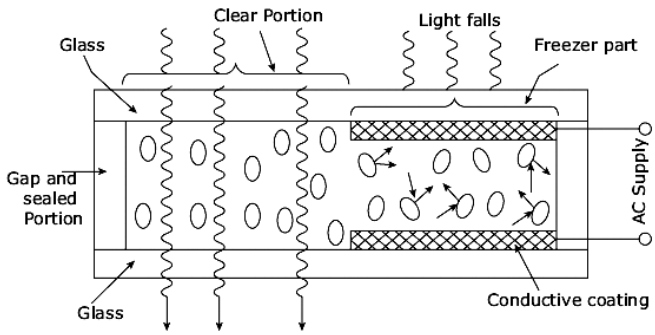
1. Dynamic scattering type
2. Field effect type

Dynamic Scattering LCD

Construction: Figure 5.3 shows the construction of dynamic scattering LCD.

The display consists of two glass plates, each coated with tin oxide (SnO_2) on the inside with transparent electrodes separated by a liquid crystal layer of 5 to 50 μm thick. The oxide coating on the front sheet is etched to produce a single or multi-segment pattern of characters with each segment properly insulated from each other.

Working Principle: When AC voltage is not applied to the plates of the molecules of liquid crystal, which align themselves in perpendicular (or parallel) direction and appear transparent. When a voltage is applied across the conductive coatings, the arrangement of molecular pattern gets disturbed. As a result, refractive index of the medium of the crystal changes. Therefore, the incident light is reflected in different directions. Now, the liquid appears dark in the white background. The area not enclosed by conducting surfaces remains translucent.



LCD Working

Advantages of LCD

1. The operating voltage required is small (3 to 20 V/AC).
2. They are economical.
3. They have low power consumption.

Disadvantages of LCD

1. LCD requires an external or internal light source. (poor visibility in darkness)
2. Its life time is limited due to chemical degeneration.
3. It operates slowly. Turn-On time is few ms.

When used on DC, the life-span is quite small and therefore, they are used with AC supplies having a frequency less than 50 Hz.

Application of LCD

1. It is used in solid state video displays.
2. It is used in laptop computers.
3. It is used in pocket calculators.
4. It is used in instrument displays and digital watches.
5. It can be used as numerical counter for counting items.

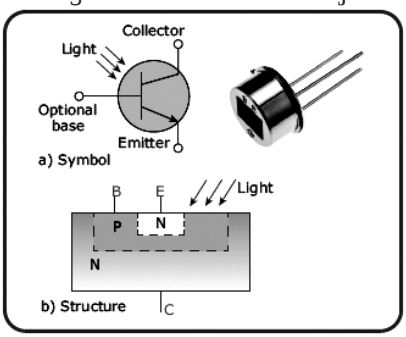
Photo Transistor

Photo transistor is a much more sensitive semiconductor photo device than the PN photodiode. The current produced by a photodiode is very low which cannot be directly used in control applications.

Therefore, this current should be amplified before applying to the control circuits. The photo transistor is a light detector which combines a photodiode and a transistor amplifier. When the photo transistor is illuminated, it permits the flow of current. Figure below shows the NPN phototransistor.

It is usually connected in common emitter (CE) configuration with base open. A lens focuses the light on the base-collector junction. The modern photo transistor uses efficient light effective materials instead of making a hole and fixing a lens on it. Photo transistor has three

terminals, but only two terminals are generally used. Here the base current is supplied by the current created by the light falling on the base-collector junction.



NPN Photo Transistor

The voltage (VCE) applied to the transistor makes emitter-base junction forward biased and collector-base junction reverse biased. When the transistor is kept in darkness, there will be a very few minority charge carrier flow. This makes negligible collector current. When the light is turned 'ON', and focused at the collector-base junction, the transistor starts conducting and the amplified current starts flowing through the reverse-biased junction. The amount of current flow depends upon the intensity of focused light.

Application

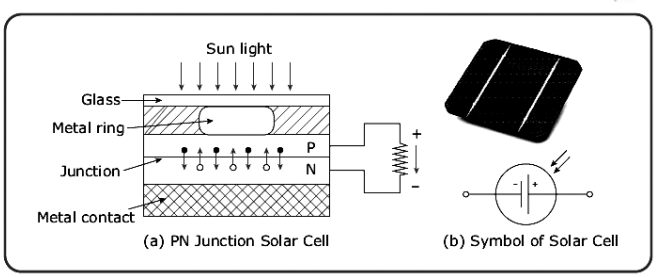
1. They are used in light detection system.
2. They are widely used in high speed reading of computer punching cards.
3. They also used in light operating switches.

SOLAR CELL

It is widely used in satellites to provide electrical power, when sunlight is incident on a photovoltaic cell. It is converted into electric energy and the energy converter is called solar cell or solar battery. Basically, solar cell is large PN junction diode. It is made up of Silicon and Selenium.

Construction: Figure below shows the basic construction of PN junction solar cell.

It consists of single semiconductor crystals, which has been doped with both P and N type impurities, thereby forming a PN junction. A glass window is provided at the top of the P type layer. The thickness of the P layer is small, so that the incident light can easily reach the junction of the diode.



Basic Construction of PN Junction Solar Cell

A nickel plated ring is provided around the P layer, which acts as a positive terminal. A metal contact provided at the bottom of the N-layer, acts as negative terminal.

Working Principle

The sunlight incident on the glass plate passes through and reaches the junction. An incident light photon at the junction may collide with a valence electron and impart sufficient energy to make a transition to the conduction band. As a result, an electron-hole pair is formed. The newly formed electrons are minority carriers in the P region. They move freely across the junction. Similarly, holes formed in the N-region cross the junction in the opposite direction. The flow of these electrons and holes across the junction is in a direction opposite to the conventional forward current in a PN junction. Further, it leads to the accumulation of majority carriers on both sides of the junction.

In bright sunlight, 0.6 V is developed by a single solar cell. The amount of power the cell can deliver depends on the extent of its active surface. An average cell will produce about 30 mW per square inch of surface, operating in a load of 4 Ω. To increase the power output, large banks of cells are used in series and parallel combinations.

Application

1. It is used to provide electrical power to satellites and space vehicles
2. It is used to energize these storage cells
3. It is also used in home for electrical requirements.

FIELD EFFECT TRANSISTOR (FET)

In the previous Chapters, we have discussed about the Bipolar Junction Transistor (BJT). They are controlled by both electrons and holes and called current operated devices. BJT has two main disadvantages; first, it has low input impedance because of forward biased emitter junction. Secondly, it has considerable noise level.

To overcome the above problems, FET can be developed and become important electronic device in the integrated circuit (IC) technology. The FET is a device in which the flow of current through the conducting region is controlled by an electric field (voltage). There are two types of field effect transistor,

1. Junction Field Effect Transistor (JFET)
2. Metal Oxide Semiconductor Field Effect Transistor(MOSFET)

Junction Field Effect Transistor (JFET)

JFET is a three terminal semiconductor device in which current conduction is by one type of carrier (i.e.) electrons or holes.

It is a unipolar device. It has high input impedance and low noise level. There are two types of JFET. They are

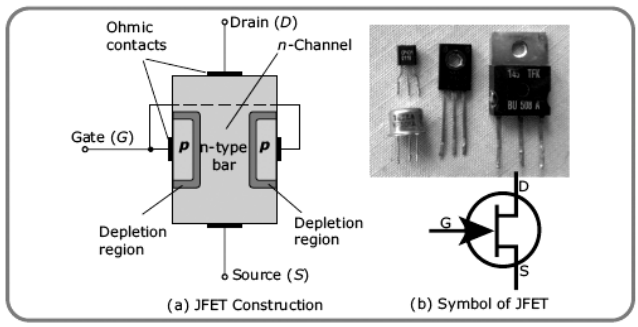
1. N-Channel JFET
2. P-Channel JFET

N-Channel JFET

Construction: Figure below shows the construction of n-channel JFET and its symbol. It consists of a uniformly doped N-type semiconductor bar made of silicon.

On both sides of this N-type semiconductor bar, two heavily doped P-type regions are formed by diffusion. The two P-regions are internally connected and a single lead is taken out, which is called Gate (G). Ohmic contacts are made at the two N-type semi-conductor bar. One lead is called as Source(S) and the other as Drain (D). These two terminals may be interchanged. The source(S) is a terminal through which the majority carriers (electrons in the N type bar) enter the bar. The drain (D) is a terminal through which the majority carriers leave the bar.

Since the two P-regions are heavily doped and N-type bar is lightly doped, two depletion layers are formed in the N-type bar as shown in Figure below. The region between the two layers is called channel. The majority carriers move from source to drain through this channel. The gate terminal controls the flow of majority carriers from source to drain.



Construction of N-Channel JFET and its Symbol

Comparison of BJT and JFET	
BJT	**JEET**
Bipolar device (current conduction by both type of carriers i.e. majority and minority -electrons and holes)	Unipolar device (current conduction is only due to one type of majority carrier either electron or hole)
Current driven device	Voltage driven device
Low Input impedance	High Input impedance
High noise level	Low noise level
Low Power gain	High Power gain
Low switching speed	High switching speed
Less thermal stability	Better thermal stability
Emitter and collector terminals are not interchangeable	Source and drain terminals are interchangeable

Advantages

1. The JFET has higher input impedance.
2. It is a low power consumption device.
3. It can be fabricated in small size area.

Disadvantages

1. The JFET is relatively low gain bandwidth product.
2. Its voltage gain is low

Application

1. The JFET is used as a constant current source.
2. It is used as buffer amplifier.
3. It is used as electronic switch.

METAL OXIDE SEMICONDUCTOR FIELD EFFECT TRANSISTOR (MOSFET)

The MOSFET is an abbreviation of Metal Oxide Semiconductor Field Effect Transistor.

In MOSFET, the gate is insulated from the channel by using SiO_2 layer. The input impedance of MOSFET is high, because the gate current is extremely small. It is also called as Insulated Gate FET (IGFET).

History: MOSFET, largely superseded the JFET and has profound effect on digital electronic development, which was invented by Dawankahng and Martin Atalla in 1959. There are two types of MOSFET. They are

1. Enhancement MOSFET (E-MOSFET).
2. Depletion MOSFET (DE-MOSFET).

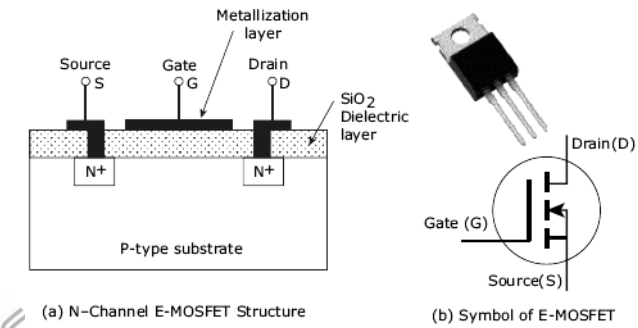
Enhancement MOSFET (E-MOSFET)

The enhancement MOSFET works only in enhancement mode. It does not conduct when gate to source voltage (VGS) is equal to zero, therefore it is called as 'normally OFF MOSFET'. It is widely used in digital circuits. There are two types of enhancement

MOSFET. They are

1. N-channel E-MOSFET 2. P-channel E-MOSFET

N-Channel E-MOSFET



Construction of N-Channel E-MOSFET and Its Symbol

Figure above shows the construction and symbol of n-channel E-MOSFET. It consists of lightly doped P type substrate into which two highly doped N-type regions are diffused. These two N regions act as Source (S) and Drain (D). A thin layer of SiO2 is grown over its surface then a metal contact is provided at the top of the SiO2layer, which acts as a Gate (G). The oxide layer provides high input impedance (1010 Ω to 1015 Ω) to the MOSFET.

Application

1. MOSFET is widely used for switching and amplifying the signals.
2. It is used in FM radio and TV receivers (for mixer operation).
3. It is used in computer memories.

decimal number is divided by 8, and writes down the remainder after each division. The remainders are taken in reverse order to form the octal number.

Example: Conversion of the decimal number 408 to its equivalent octal number.

8 | 408
8 | 51 - 0
8 | 6 - 3

Hence, $408_{10} = 630_8$

Octal to Decimal Conversion

To convert an octal number to its equivalent decimal number, multiply each octal digit by its weight and then add the resulting products.

Example: Conversion of an octal number 375 into its equivalent decimal number.

The weight of 5 is 8°, 7 is 8° and 3 is 8°.

Hence, the equivalent decimal number is

$= (3 \times 8^2)+(7 \times 8^1)+(5 \times 8^0)$

$= (3 \times 64)+(7 \times 8)+(5 \times 1)$

$= 192+56+5= 253$

Hence, $375_8 = 253_{10}$

Decimal to Hexadecimal Conversion

To convert Decimal to Hexadecimal, "Repeated division by 16 method" can be used. The decimal number is divided by 16 and write down the remainder after each division. The remainders are taken in reverse order to form the hexadecimal number.

Example: Conversion of a decimal number 4538 to its equivalent hexadecimal number.

16 | 4538
16 | 283 - 10
16 | 17 - 11
1 - 1

Hence, $4538_{10} = 11BA_{16}$

Hexadecimal to Decimal Conversion

To convert the hexadecimal to its equivalent decimal number, multiply each hexadecimal digit by its weight and then add the resulting products.

Example: Conversion of a hexadecimal number of B35 to its equivalent decimal number.

The weight of B is 16^2, 3 is 16^1 and 5 is 160

Hence its equivalent Decimal number is

$= (B \times 16^2)+(3 \times 16^1)+(5 \times 16^0)$

$= (11 \times 256)+(3 \times 16)+(5 \times 1)$

$= 2816+48+5$

$= 2869$

Hence, $B35_{16} = 2869_{10}$

Octal to Binary Conversion

In this conversion, each octal digit is converted into its equivalent three digit binary form. The octal number and its equivalent three digit binary numbers are shown in the Table.

Conversion of Octal into Equivalent Binary Number	
Octal number	**Equivalent Binary number**
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Example: Conversion of an octal number 43 to its equivalent binary number.

4 3
100 011
$43_8 = 100011_2$

Binary to Octal Conversion

The binary numbers are grouped as 3-bit from left to right. If there is any binary digit left with one or two bits then sufficient numbers of zero are added to the left most side of the binary number.

Then, grouped 3-bit number is converted into an equivalent octal number.

Example: Conversion of a binary number of 010111011 to its equivalent octal number.

010 111 011
2 7 3

Hence, $010111011_2 = 273_8$

Hexadecimal to Binary Conversion

In this conversion, each hexadecimal digit is converted into its equivalent four digit binary form.

The hexadecimal number and its equivalent 4 digit binary numbers are shown in the Table.

Conversion of Hexadecimal into Equivalent Binary Number.	
Hexadecimal Number	Equivalent Binary Number
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010

Hexadecimal Number	Equivalent Binary Number
B	1011
C	1100
D	1101
E	1110
F	1111

Example: Conversion of a hexadecimal number 7B3 into its equivalent binary number.

7 B 3

0111 1011 0011

Hence, $7B3_{16} = 011110110011_2$

Note: Delete the left most zeros.

Binary to Hexadecimal Conversion

In this conversion, the binary number is arranged in group of 4 bits. Suppose the binary number grouping is not completed with the 4 digits, sufficient numbers of zero are added to the left most side of the binary number.

Example: Conversion of a binary number 110110101011100 into its equivalent hexadecimal number.

0110 1101 0101 1100

6 D 5 C

Hence, $110110101011100_2 = 6D5C_{16}$

Fractional Decimal to Binary Conversion

The method of "Repeated multiplication by 2" has to used to convert the decimal fractions.

$0.2 \times 2 = 0.4$ 0 (Step-1)

$0.4 \times 2 = 0.8$ 0 (Step-2)

$0.8 \times 2 = 1.6$ 1 (Step-3)

$0.6 \times 2 = 1.2$ 1 (Step-4)

$0.2 \times 2 = 0.4$ 0 (last integer part obtained)

Note: Fraction repeats, the product is the same as in the first step.

Write the integer parts from top to bottom to obtain the equivalent fractional binary number.

Hence $(0.2)_{10} = (0.00110011\ldots)_2$

Decimal to BCD Conversion

In this Conversion, each decimal digit is converted into its equivalent 4 digits binary form (BCD).

Example: Conversion of a decimal number 892 to its equivalent BCD number.

8 9 2

1000 1001 0010

Hence, $892_{10} = 100010010010_{BCD}$

BCD to Decimal Conversion

In this method, each BCD number grouped in the form of 4 digit binary pattern is converted into its equivalent decimal number.

Example: Convert a BCD number 100100111000 to its equivalent decimal number.

1001 0011 1000

9 3 8

Hence, $100100111000_{BCD} = 938_{10}$

BINARY ADDITION AND SUBTRACTION

A logic circuit can be used to perform arithmetic functions like addition, subtraction, multiplication, division etc. For performing these operations, compliment method of number patterns are used. First, we will see the complement methods in order to understand the basic arithmetic operations.

One's Complement Method

In one's complement method, each binary bit of the number is changed from 0 to 1 or 1 to 0 depending on the existing bit value.

For instance, the binary number is $A_3\ A_2\ A_1\ A_0 = 0010$, its corresponding one's complement number is $\overline{A_3}\ \overline{A_2}\ \overline{A_1}\ \overline{A_0} = 1101$

The same principle will apply for number having any bit length and its corresponding one's complement number can be obtained by complement each bit.

Two's Complement Method

The two's complement of a binary number is the number that results when we add '1' to the one's complement number. The formula for two's complement of a binary number is given below.

Two's complement number = one's complement +1

For instance, to find the two's complement number of 0101, the following procedure is employed.

0101 $\Rightarrow$ 1010 (1's complement)

1010 +1 $\Rightarrow$ 1011 (2's complement)

Binary Addition

For binary addition, the arithmetic rules used are given below.

1. 0+0=0
2. 0+1=1, No carry is formed
3. 1+0=1, i.e. carry = 0
4. 1+1=0,with a carry of 1, and sum = 0
   i.e. $1+1 = 10_2$.

This is a binary number 10 and not the decimal number ten. Here, the first digit 0 is called sum and next digit 1 is called carry.

Examples:

1. Add the binary numbers 1011 and 1100

1011
1100
10111

Sum = 0111, and Carry = 1

2. Add the binary number 11101 with 11011001.

The first number = 00011101 +
The second number = 11011001
Result = 11110110

Binary Subtraction

The general rules for carrying out the binary subtraction are given below.

1. 0 - 0=0
2. 1 - 0=1
3. 1 - 1=0
4. 0 - 1=1, with a borrow of 1 from the next higher bit.
5. 10-1=1

Example: Subtract 0111 from 1011

$1011 \Rightarrow 11_{10}$
$0111 \Rightarrow 7_{10}$
$0100 \Rightarrow 4_{10}$

First column $\Rightarrow 1 - 1 = 0$
Second column $\Rightarrow 1 - 1 = 0$
Third column $\Rightarrow 0 - 1 = 10 - 1 = 1$
Forth column $\Rightarrow$ After borrowing, the fourth column becomes 0

Hence, $0 - 0 = 0$

$1011_2 - 0111_2 = 0100_2$

BINARY CODES

All digital circuits operate with only two states namely, High and Low or ON and OFF or 1 and 0. In binary number system, the number of bits required goes on increasing as the numbers become larger and larger.

So, some special binary codes are required to represent alphabets and special characters. Based on these points, different types of binary code have been developed.

They are,

1. BCD codes
2. Gray codes
3. Excess 3 code
4. ASCII code

BCD - 8421 Code Conversion

A group of bits (usually four) which are used to represent decimal numbers 0 to 9 are called BCD(Binary Coded Decimal) codes. The most popular BCD code is 8421 code. The 8421 indicates the binary weights of the four bits (2_3, 2_2, 2_1, 2_0). Using the four bits with weights 8,4,2,1, we can easily represent the decimal numbers 0 to 9 as given in the Table below.

Conversion of Decimal Number into BCD Code	
Decimal Numbers	**BCD Code**
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	0001 0000
56	0101 0110
963	1001 0110 0011

Gray Code

The gray code is not a weighted code. Therefore it is not suitable for arithmetic operations, but finds applications in input/output devices and in some types of analog to digital converters.

Gray code conversion		
Decimal numbers	**Binary code**	**Gray code**
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

The gray code is a minimum change code in which only one bit in the code group changes when moving from one step to the next. The gray code is also called as reflected binary code, which has a special property of

containing two adjacent code numbers that differ by only one bit. The gray code representation for the decimal numbers 0 to 15, together with the binary code is given in the Table above.

Excess-3 Code

The excess-3 code is another BCD code used in earlier computers. The excess-3 code is not a weighted code. It is a self-complementing code and helps in performing subtraction operations in digital computers. The excess–3 code is also a reflection code.

An excess–3 code is obtained by adding 3 to each digit of a decimal number. For example, to encode the decimal number 6 into an excess–3 code, we must first add 3, in order to obtain 9. The 9 is then encoded into its equivalent 4 bit binary code 1001.

Example: Conversion of the decimal number 548 to its equivalent excess-3 code.

Decimal number		5	4	8
Add to each bit	+	3	+3	+3
Sum	=	8	7	11

Hence, the equivalent excess-3code 1000 0111 1011

The representation of Excess-3 code for the decimal numbers is given in the Table below.

Excess - 3 Code of Decimal Number	
Decimal Number	**Excess-3 Code**
0	0011
1	0100
2	0101
3	0110
4	0111
5	1000
6	1001
7	1010
8	1011
9	1100

Binary to Gray Conversion

To convert a given binary number to its equivalent gray code, the following rules are applied.

1. The MSB of the gray code is same as the MSB of the binary.

2. Coding starts from left to right, add each adjacent pair of bits to get the next bit of the gray code. Omit the carry, if occurs.

Example: Conversion of the binary number 1011 to gray code.

Step 1: The MSB in gray code is same as the MSB of the binary

1 0 1 1 Binary
↓
1 1 Gray

Step 2: Add the left most bit to the adjacent one.

1 + 0 1 1 Binary
↓
1 1 Gray

Step 3: Add the next adjacent pair.

1 0 + 1 1 Binary
↓
1 1 1 1 Gray

Step 4: Add the next adjacent pair and omit the carry.

1 0 1 + 1 Binary
1 1 1 0 Gray

Hence, $(1011)_2 = (1110)_G$

Suffix 'G' is used to represent the Gray code.

Gray to Binary Conversion

To convert a given Gray code number into equivalent binary, the following rules are applied.

1. The MSB of the binary is same as the MSB of the Gray.
2. Coding from left to right, add the binary digit generated to the adjacent gray bit to get the next bit of the binary. Omit the carry if occurs.

Example: convert the gray code 1110 to its equivalent binary.

Step 1: The MSB in binary is same as the MSB of the gray

1 1 1 0 Gray
↓
1 Binary

Step 2: Add the binary digit generated to the adjacent bit of the Gray code.

1 1 1 0 Gray
↗ + ↓
1 0 Binary

Step 3: Add the binary digit generated to the adjacent bit of Gray codes.

1 1 1 0 Gray
↗ + ↓
1 0 1 Binary

Step 4: Add the binary digit generated to the adjacent bit of gray code.

1 1 1 0
↗ + ↓
1 0 1 1

Hence, $(1110)_G = (1011)_2$

ADVANTAGES AND DISADVANTAGES OF DIGITAL ELECTRONICS

Advantage

1. Very simple logic the lead to identify the faults very easily

Attenuation Measurement

Attenuation α in dB is defined as

$$\alpha = 10\log_{10}\left(\frac{P_i}{P_O}\right)$$

where, P_i = Input power to the device

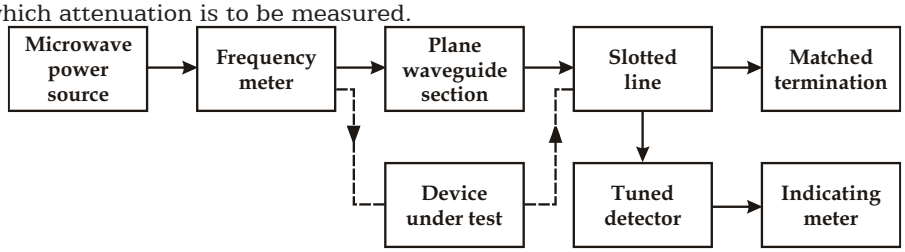
P_O = Output power from the device

Attenuation measurement can be performed by two methods

i) Direct or power ratio measuring method. ii) RF substitution method.

Power Ratio Measurement Method

The direct method involves measuring power at two desired points i.e. input power and output power with and without device of which attenuation is to be measured.



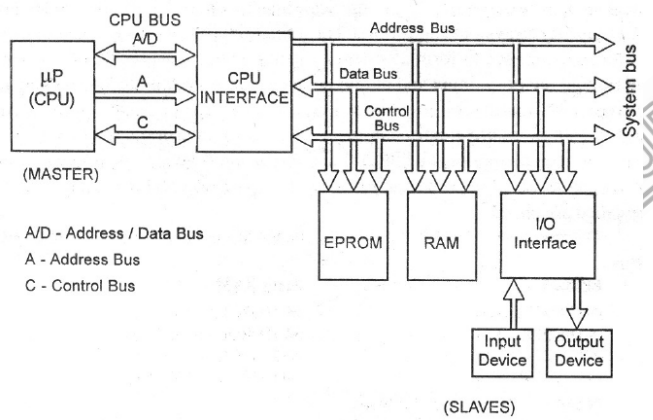
It is measured under matched conditions, otherwise it is not possible to calculate accurately how much is the power reduction is due to the mismatch, and how much is due to attenuation of the network.

Power delivered to the load (DUT) is measured and then the power is measured without load (DUT), the ratio of the second to the first power gives attenuation.

MICROPROCESSOR AND ITS APPLICATIONS

Introduction to Microcomputer

The Microprocessor based system (single board microcomputer) consists of microprocessor as CPU, semiconductor memories like EPROM and RAM, input device, output device and interfacing devices. The memories, input device, output device and interfacing devices are called peripherals. The popular input devices are keyboard and floppy disk and the output devices are printer, LED/LCD displays, CRT monitor, etc.



Microprocessor Based System (organization of microcomputer)

The above block diagram shows the organization of a microprocessor based system. In this system, the microprocessor is the master and all other peripherals are slaves. The master controls all the peripherals and initiates all operations.

The work done by the processor can be classified into the following three groups.

1. Work done internal to the processor
2. Work done external to the processor
3. Operations initiated by the slaves or peripherals.

The work done internal to the processors are addition, subtraction, logical operations, data transfer operations, etc. The work done external to the processor are reading/writing the memory and reading/writing the I/O devices or the peripherals. If the peripheral requires the attention of the master then it can interrupt the master and initiate an operation.

The microprocessor is the master, which controls all the activities of the system. To perform a specific job or task, the microprocessor has to execute a program stored in memory. The program consists of a set of instructions. It issues address and control signals and fetches the instruction and data from memory. The instruction is executed one by one internal to the processor and based on the result it takes appropriate action.

Input

The input section transfers data and instructions in binary from the outside world to the microprocessor.

It includes devices such as keyboards, teletypes, and analog-to-digital converters. Typically, a microcomputer includes a keyboard as an input device. The key board has sixteen data keys (0 to 9 and A to F) and some additional function keys to perform operations such as storing data and executing programs.

Output

The output section transfers data from the microprocessor to output devices such as light emitting diodes (LEDs), cathode-ray-tubes (CRTs), printers, magnetic tape, or another computer. Typically, single-board computers include LEDs and seven-segment LEDs as output devices.

Memory

Memory stores binary information such as instructions and data, and provides that information to the microprocessor whenever necessary. To execute programs, the microprocessor reads instructions and data from memory and performs the computing operations in its ALU section. Result are either transferred to the output section for display or stored in memory for later use. The memory block has two sections : Read - Only Memory (ROM) and Read / Write Memory (R/WM), popularly known as Random Access Memory (RAM).

The ROM is used to store programs that do not need alterations. The monitor program of a single - board microcomputer is generally stored in the ROM. Program stored in the ROM can only be read; they cannot be altered.

The Read / Write memory (R/WM) is also known as user memory. It is used to store user programs and data. The information stored in this memory can be read and altered easily.

System Bus

The system bus is a communication path between the microprocessor and the peripherals; it is nothing but a group of wires that carries bits. The microcomputer bus is in many ways similar to a one-track, express subway, the microcomputer bus carries bits between the microprocessor and only one peripheral at a time. The same bus is time - shared to communicate with various peripherals, with the timing provided by the control section of the microprocessor.

Address Bus

This is a unidirectional bus, because information flows over it in only one direction, from the CPU to the memory or I/O elements. The CPU alone can place logic levels on the lines of the address bus, thereby generating 216 = 65,536 different possible addresses. Each of these addresses corresponds to one memory location or one I/O element.

When the CPU wants to communicate (read or write) with a certain memory location or I/O device, it places the appropriate 16-bit address code on its 16 address pin outputs, A0 through A15, and onto the address bus. These address bits are then decoded to select the desired memory location or I/O device.

Data Bus

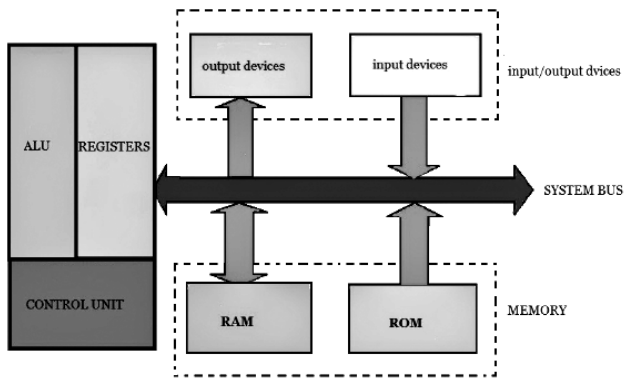
This is a bi-directional bus, because data can flow to or from the CPU. The CPU's eight data pins, D0 through D7,can be either inputs or outputs, depending on whether the CPU is performing a read or a write operation. During data bus by the memory or I/O element. During a write operation the CPU's data pins act as outputs and place data on the data bus, which are then sent to the selected memory or I/O element.

Control Bus

This is the set of signals that is used to synchronize the activities of the separate microcomputer elements. Some of these control signals, such as RD and WR are sent by the CPU to the other elements to tell them what type of operation is currently in progress. The I/O elements can send control signals to the CPU. An example is the rest input (RES) of the CPU which, when driven LOW, causes the CPU to reset to a particular starting stare.

Microprocessor

The microprocessor is a semiconductor device consisting of electronic logic circuits manufactured by using either a large-scale (LSI) or very large-scale integration (VLSI) technique. The microprocessor is capable of performing computing functions and making decisions to change the sequence of program execution. The microprocessor can be divided into three segments, arithmetic/logic unit (ALU), register unit, and control unit.



Block Diagram of Microprocessor

Arithmetic and Logic Unit : In this area of the microprocessor, computing functions are performed on data. The CPU performs arithmetic operations such as addition and subtraction, and logic operations such as AND, OR, and exclusive OR. Results are stored either in register or in memory or sent to output devices.

Register Unit : This area of the microprocessor consists of various registers. The register are used primarily to store data temporarily during the executing of a program. Some of the registers are accessible to the user through instructions.

Control Unit : The control unit provides the necessary timing and control signals to all the operations in the microcomputer. It controls the flow of data between the microprocessor and peripherals (including memory).

Microprocessor Architecture and its Operations

The MPU performs primarily four operations.

1. Memory Read: Reads data from memory.
2. Memory Write: Writes data into memory.
3. I/O read: Accepts data from input devices.
4. I/O Write: Sends data to output devices.

All these operations are part of the communication process between the MPU and peripheral devices (including memory). To communicate with a peripheral (or a memory location), the Microprocessor needs to perform the following steps:

Step 1 : Identify the peripheral or the memory location (with its address).

Step 2 : Transfer data

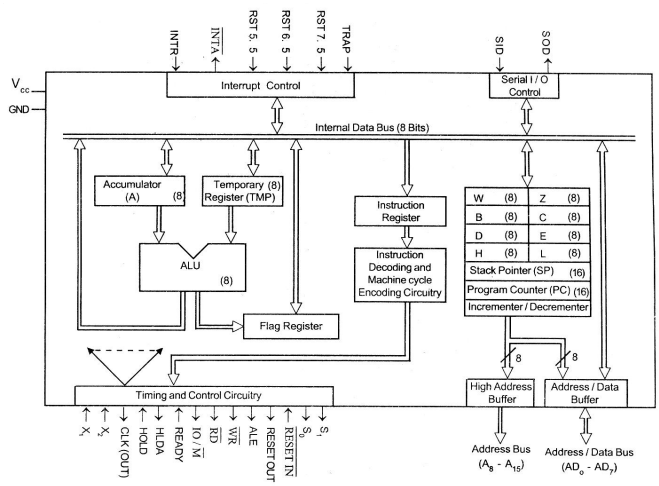
Step 3 : Provide timing or synchronization signals.

The internal operations can be performed by the microprocessor are

1. Store 8-bits data.
2. Perform arithmetic and logical operations.
3. Test for conditions.
4. Sequence the execution of instructions.
5. Store data temporarily during execution in the defined R/W memory locations called the stack.

To perform these operations, the microprocessor requires registers, an arithmetic logic unit (ALU) and control logic, and internal buses (path for information flow).

INTEL 8085 ARCHITECTURE



The architecture of.8085 is shown in figure given below. The internal architecture of 8085 includes the ALU, timing and control unit, instruction register and decoder, register array, interrupt control and serial I/O control.

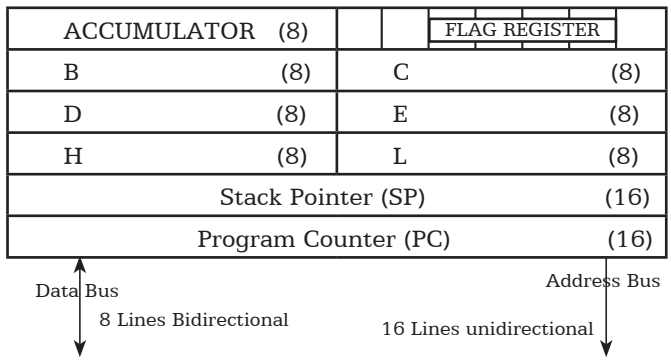
Operations performed by 8085

The ALU performs the arithmetic and logical operations.

The operations performed by ALU of 8085 are addition, subtraction, increment, decrement, logical AND, OR, EXCLUIVE -OR, compare, complement and left / right shift. The accumulator and temporary register are used to hold the data during an arithmetic / logical operation. After an operation the result is stored in the accumulator and the flags are set or reset according to the result of the operation.

Registers

The 8085 has six general - purpose registers to perform the first operation listed above, that is, to store 8-bit data during a program execution. These registers are identified as B, C, E, H, and L. They can be combined as register pairs - BC, DE, and HL - to perform some 16-bit operation.



Register Organisation

These registers are programmable, meaning that a programmer can use them to load or transfer data from the registers by using instructions.

Accumulator

The accumulator is an 8-bit register that is part of the arithmetic logic unit (ALU). This register is used to store 8-bit data and to perform arithmetic and logical operations. The result of an operation is stored in the accumulator. The accumulator is also identified as register A.

Flags

The ALU includes five flip-flops that are set or reset according to data conditions in the accumulator and other registers. The microprocessor uses them to perform the third operation; namely testing for data conditions.

The bit position of the flip flop in flag register is:

D7	D6	D5	D4	D3	D2	D1	D0
S	Z		AC		P		CY

All of the three flip flop set and reset according to the stored result in the accumulator.

For example, after an addition of two numbers, if the result in the accumulator is larger than 8-bit, the flip-flop uses to indicate a carry by setting CY flag to 1. When an

arithmetic operation results in zero, Z flag is set to 1. The S flag is just a copy of the bit D7 of the accumulator. A negative number has a 1 in bit D7 and a positive number has a 0 in 2's complement representation. The AC flag is set to 1, when a carry result from bit D3 and passes to bit D4. The P flag is set to 1, when the result in accumulator contains even number of 1s.

Stack Pointer (SP)

The stack pointer SP, holds the address of the stack top. The stack is a sequence of RAM memory locations defined by the programmer. The stack is used to save the content of registers during the execution of a program.

Program Counter (PC):

The program counter (PC) keeps track of program execution. To execute a program the starting address of the program is loaded in program counter. The PC sends out an address to fetch a byte of instruction from memory and increment its content automatically. Hence, when a byte of instruction is fetched, the PC holds the address of the next byte of the instruction or next instruction.

Timing and Control Unit

It provides timing and control signal to the microprocessor to perform the various operation. It has three control signal. It controls all external and internal circuits. It operates with reference to clock signal. It synchronizes all the data transfers.

There are three control signal:

1.ALE-Address Latch Enable, It provides control signal to synchronize the components of microprocessor.

2.RD- This is active low used for reading operation.

3.WR-This is active low used for writing operation.

There are three status signal used in microprocessor S0, S1 and IO/M. It changes its status according the provided input to these pins.

Serial Input Output Control

There are two pins in this unit. This unit is used for serial data communication.

Interrupt Unit

There are 6 interrupt pins in this unit. Generally an external hardware is connected to these pins. These pins provide interrupt signal sent by external hardware to microprocessor and microprocessor sends acknowledgement for receiving the interrupt signal. Generally INTA is used for acknowledgement.

A8 – A15 (Output 3 State): Address Bus

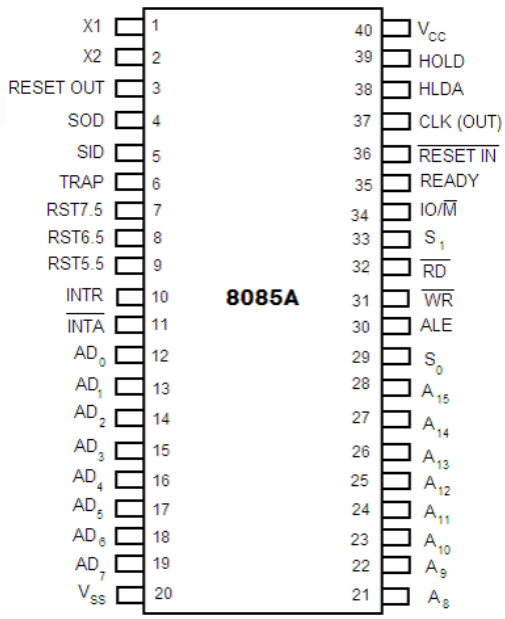
The most significant 8 bits of the memory address or the 8 bits of the I/0 addresses, 3 stated during Hold and Halt modes.

AD0 - AD7 (Input/ Output 3 state): Multiplexed Address/ Data Bus

Lower 8 bits of the memory address (or I/0 address) appear on the bus during the first clock cycle of a machine state. It then becomes the data bus during the second and third clock cycles. 3 stated during Hold and Halt modes.

The 8085 microprocessor is available on a 40-pin Dual-in-Line package (DIP). The following describes the function of each pin:

Pin Diagram and Pin description of 8085



ALE (Output): Address Latch Enable

It occurs during the first clock cycle of a machine state and enables the address to get latched into the on chip latch of peripherals. The falling edge of ALE is set to guarantee setup and hold times for the address information. ALE can also be used to strobe the status information.

SO, S1 (Output): Data Bus Status

Encoded status of the bus cycle:

Encoded status of the bus cycle:

S1	S0	status
0	0	HALT
0	1	WRITE
1	0	READ
1	1	FETCH

RD (Output 3state): READ

Indicates the selected memory or 1/0 device is to be read and that the Data Bus is available or the data transfer.

WR (Output 3state): WRITE

Indicates the data on the Data Bus is to be written into the selected memory or 1/0 location.

READY (Input):

If Ready is high during a read or write cycle, it indicates that the memory or peripheral is ready to send or receive data. If Ready is low, the CPU will wait for Ready to go high before completing the read or write cycle.

$$dE_\theta = jZ_0 \frac{kI(z)e^{-jkr}}{4\pi r} e^{jkz\cos\theta} \sin\theta dL$$

$$dE_r = 0 ; dH_r = 0 ; dH_\theta = 0 \quad \text{..... (27)}$$

$$dH_\phi = j \frac{kI(z)e^{-jkr}}{4\pi r} e^{jkz\cos\theta} \sin\theta dL$$

where the $e^{jkz\cos\theta}$ phase term accounts for the extra path length associated with an element at z compared with one at the origin. The total E_θ field is therefore

$$E\theta = \int_{-L/2}^{L/2} dE_\theta = jZ_0 \frac{ke^{-jkr}}{4\pi r} \sin\theta \int_{-L/2}^{L/2} I(z) e^{jkz\cos\theta} dz \quad \text{..... (28)}$$

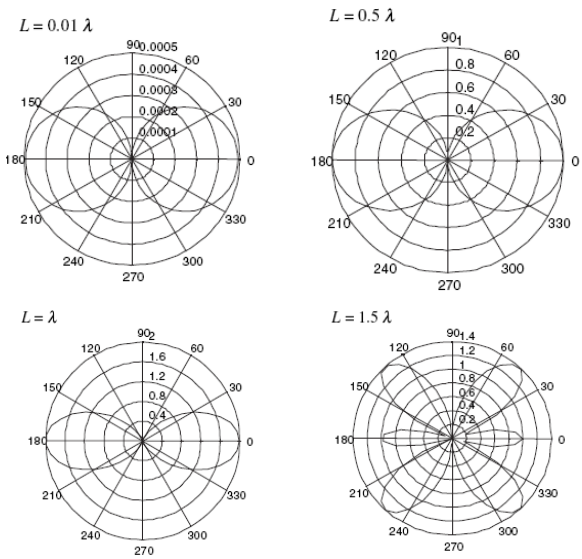
The result of these calculations is

$$E_\theta = \frac{jZ_0 I(0) e^{-jkr}}{2\pi r} \left[\frac{\cos\left(\frac{kL}{2}\cos\theta\right) - \cos\left(\frac{kL}{\lambda}\right)}{\sin\theta} \right] \quad \text{..... (29)}$$

This pattern is omnidirectional with nulls along the z-axis, just as for the Hertzian dipole. A similar calculation can be performed for H, but it is simpler to use the relation established in Section before.

$$\frac{E_\theta}{H_\phi} = Z_0 \quad \text{..... (30)}$$

Equation (29) is plotted in Figure below for the same dipole lengths as Figure above. In the case of L =0·01λ the radiation pattern is essentially identical to the Hertzian dipole: despite the current distribution being non-uniform, the radiation contributions are so closely located that they sum as if the current was indeed constant along the dipole length. As the length increases through 0:5λ to λ, the HPBW increases through 78° to 47°. Above around L =1·2λ, however, the pattern becomes multilobed, which is rarely useful in practice. Note also that the magnitude of the field is itself strongly dependent upon the



Pattern factors for dipoles of various lengths

antenna length. The most common length is the half-wave dipole (L = 0·5λ), which has significant directivity, high efficiency and relatively compact size. The directivity of the half-wave dipole is 1.64 or 2.15 dBi. As the half-wave dipole is an easily controlled, realisable antenna, whereas the isotropic antenna is not, it is common for antenna manufacturers to measure and quote antenna gains and directivities referenced to the half-wave dipole, in which case a suffix 'd' is used. Thus

0 dBd = 2:15 dBi. ....(31)

The above analysis of the dipole illustrates one general means of analysing antennas: first the current distribution is determined, and then contributions from infinitesimal elements are summed to find the radiation pattern. The first step is usually the most complicated, as simple approximations like the transmission line analogy above cannot always be used.

Input Impedance

A thin, lossless dipole, exactly half a wavelength long, has an input impedance Za = 73+j42.5Ω. It is desirable to make it exactly resonant, which is usually achieved in practice by reducing its length to around 0:481, depending slightly on the exact conductor radius and on the size of the feed gap. This also reduces the radiation resistance.

ANTENNA ARRAYS

Introduction

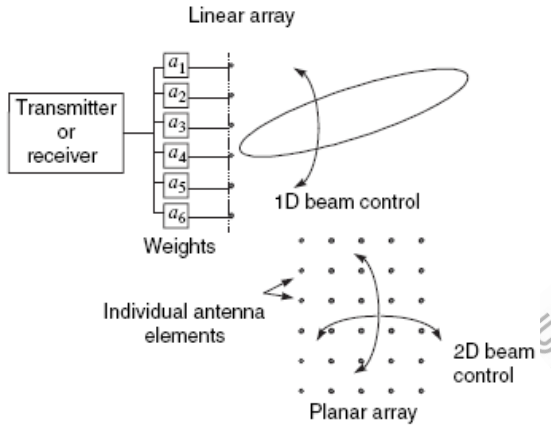
The maximum directivity available from a single dipole was shown in Figure above to be limited to that which can be achieved with a dipole a little over one wavelength. In some applications this may not be sufficient. One approach to improving on this is to combine arrays of dipoles, or of other antenna elements, where the amplitude and phase with which each element is fed may be different. The fields produced by the elements then combine with different phases in the far field, and the radiation pattern is changed. This also allows the radiation pattern to be tailored according to the particular application, or varied to allow beam scanning without any physical antenna motion. If the amplitude and phase weights are controlled electronically, then the beam can be scanned very rapidly to track changes in the communication channel.

Linear and Planar Arrays

Arrays may be linear or planar, as shown in Figure below. A linear array allows beam steering in one dimension, permitting directivity to be obtained in a single plane, hence an omnidirectional pattern can be synthesised. A planar array has two dimensions of control, permitting a narrow pencil beam to be produced.

The Uniform Linear Array

The simplest array type is the uniform linear array, which is a linear array with equal interelement spacing and a progressive phase shift across the array. In this case the field



Array types: Each array element transmits a signal which is a version of the same signal, apart from a weighting coefficient a_i

pattern of the total array is equivalent to the pattern of the individual elements multiplied by an array factor, whose normalised value is

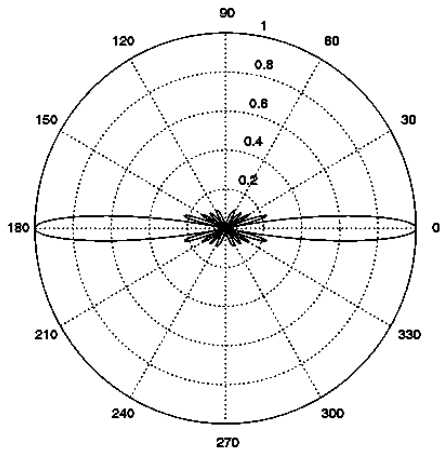
$$F_a \frac{\sin(n\psi/2)}{(n\psi/2)} where\, \psi = \frac{2\pi d}{\lambda}\cos\phi + \beta$$

Here n is the number of elements, d is the interelement spacing and α is the phase shift between adjacent elements. The weight applied to the ith element is then $a_i = e^{j(i-1)\alpha}$ The peak gain is 20 log n dB greater than that for a single element, so in principle the gain may be increased to any desired level. The weights may be created by splitting the signal through a phasing network, consisting of lengths of transmission line of increasing length for each element. Figure below shows the radiation pattern which can be obtained from a 10-element uniform linear array.

Parasitic Elements: Uda–Yagi Antennas

Another array-based approach to enhancing the directivity of dipole antennas is to use parasitic elements. *Parasitic elements* are mounted close to the driven dipole and are not connected directly to the source. Instead, the radiation field of the driven element induces currents in the parasitics, causing them to radiate in turn. If the length and position of the parasitic elements are chosen appropriately, then the radiation from the parasitics and the driven element add constructively in one direction, producing an increase in directivity. The classic form of such an antenna is the *Uda–Yagi*, or simply *Yagi antenna*, illustrated and widely used as a television reception antenna.

Typically, the driven element is made a little shorter than $\lambda/2$, to permit a good match to 50Ω. Elements in the radiation direction, called *directors*, are made a little shorter than the driver element, and an element very close to $\lambda/2$ is placed behind and called the *reflector* . Increasing the number of directors increases the gain, although the improvement diminishes

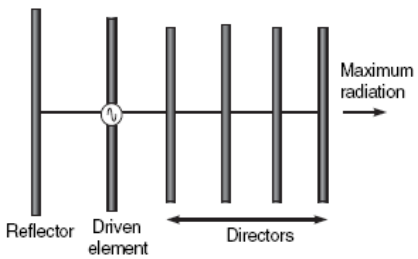


Array factor for a 10 - element uniform linear array: α = 0 and d = λ / 2

according to how far the director is from the driven element. A 4-director Yagi can have a gain of up to around 12 dBi.

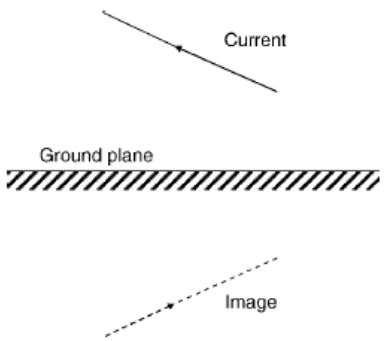
Reflector Antennas

Reflector antennas rely on the application of *image theory*, which may be described as follows. If an antenna carrying a current is placed adjacent to a perfectly conducting plane, the *ground plane*, then the combined system has the same fields above the plane as if an image



The Uda–Yagi antenna

of the antenna were present below the plane. The image carries a current of equal magnitude to the real antenna but in the opposite direction and is located an equal distance from the plane as the real antenna but on the other side, as shown in Figure below. This statement is a consequence of Snell's law of reflection, given the Fresnel reflection coefficients for a perfect conductor.



Illustrating image theory

Monopole Antennas

The monopole antenna results from applying image theory to the dipole. If a conducting plane is placed below a single element of length L/2 carrying a current, then the combined system acts essentially identically to a dipole of length L except that the radiation takes place only in the space above the plane, so the directivity is doubled and the radiation resistance is halved. The quarter-wave monopole (L/2 = λ/4) thus approximates the half-wave dipole and is a very useful configuration in practice for mobile antennas, where the conducting plane is the car body or handset case.

Corner Reflectors

The monopole principle can be extended by using two reflectors. This results in multiple images and a correspondingly increased gain. This is known as the corner reflector antenna.

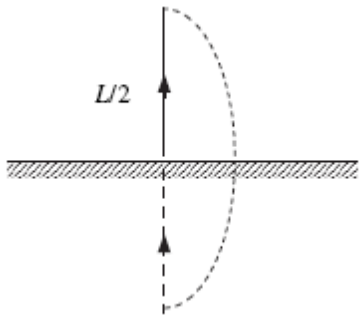
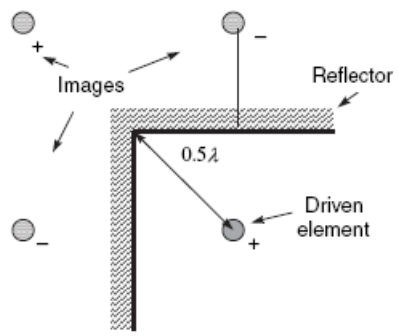
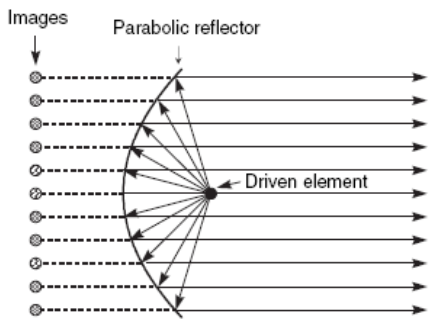


Image theory applied to the monopole antenna

In Figure below the gain is up to 12 dBi. Variations on this type of antenna are often used in cellular base station sites.



The corner reflector antenna



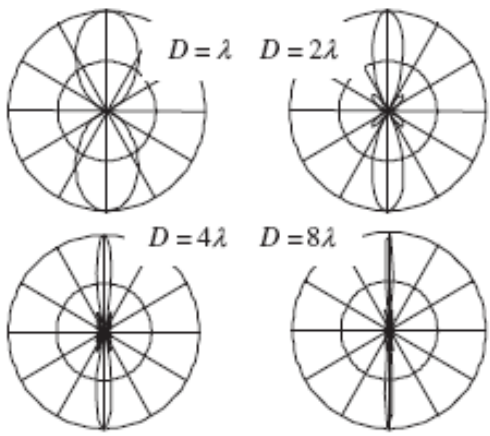
A parabolic reflector (dish) antenna

Parabolic Reflector Antennas

The parabolic (dish) antenna extends the reflector antenna concept to curved reflectors. In this case the number of images is effectively infinite and the locations of the images are such as to produce a parallel beam from the reflector, provided that the driven element is placed at the focus of the parabola. The antenna then acts like an infinite uniform array and the array factor can therefore be found from Eq. (32) by setting $\alpha = 0$, $nd = D$, where D is the diameter of the dish, and letting $n \to \infty$. This yields

$$P = \sin\left(\frac{\pi D \cos\phi}{\lambda}\right) / \left(\frac{\pi D \cos\phi}{\lambda}\right) \qquad \text{..... (33)}$$

The result is shown in Figure below for various values of D. The gain can be increased essentially arbitrarily by enlarging the size of the dish; this makes it appropriate for longrange communications applications, such as satellite systems.



Array factors for parabolic dish antennas of various diameters

In general, the gain of a parabolic dish antenna is given by

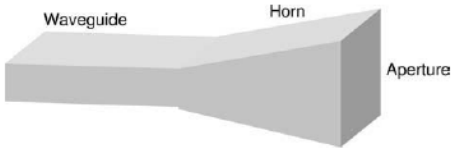
$$G = \eta\left(\frac{\pi D}{\lambda}\right)^2 \qquad \text{..... (34)}$$

where η is the antenna efficiency as a fraction, D is the diameter of the dish [m] and λ is the wavelength [m]. The efficiency is dependent on the material and accuracy of the dish construction and the details of the feed system.

HORN ANTENNAS

The horn antenna is a natural evolution of the idea that any antenna represents a region of transition between guided and propagating waves. Horn antennas are highly suitable for frequencies (typically several gigahertz and above) where waveguides are the standard feed method, as they consist essentially of a waveguide whose end walls are flared outwards to form a megaphone-like structure. In the case illustrated, the aperture is maintained as a rectangle, but circular and elliptical versions are also possible. The dimensions

of the aperture are chosen to select an appropriate resonant mode, giving rise to a controlled field distribution over the aperture. The best patterns (narrow main lobe, low side lobes) are produced by making the length of the horn large compared to the aperture



The rectangular horn antenna

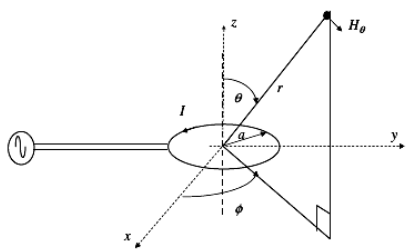
width, but this must be chosen as a compromise with the overall volume occupied. A common application of horn antennas is as the feed element for parabolic dish antennas in satellite systems.

LOOP ANTENNAS

The loop antenna is a simple loop of wire of radius a; it is small enough in comparison to a wavelength that the current I can be assumed constant around its circumference. The resulting radiation pattern is

$$H_\theta = -\frac{I}{r}\left(\frac{ka}{2}\right)^2 e^{-jkr}\sin\theta \qquad \text{..... (35)}$$

Note that this has exactly the shape of the Hertzian dipole pattern in Eq. (4.3), except that the electric and magnetic fields are reversed in their roles. As with the Hertzian dipole, the loop is relatively inefficient. In practice, loops are usually applied as compact receiving antennas, e.g. in pagers. The loop need not be circular, with approximately the same fields being produced provided the area enclosed by the loop is held constant.

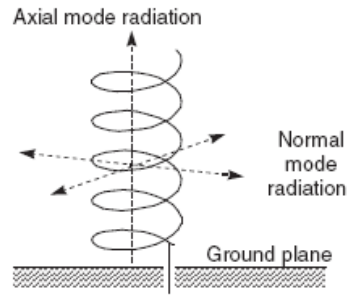


The loop antenna

HELICAL ANTENNAS

The helical antenna can be considered as a vertical array of loops, at least for the case when the diameter of the helix is small compared to a wavelength. The result is normal mode radiation with higher gain than a single loop, providing an omnidirectional antenna with compact size and reasonable efficiency, but rather narrow bandwidth. It is commonly used for hand-portable mobile applications where it is more desirable to reduce the length of the antenna below that of a quarter-wave monopole.

In the case where the diameter is around one wavelength or greater, the mode of radiation changes completely to the axial mode, where the operation of the antenna is similar to that of a



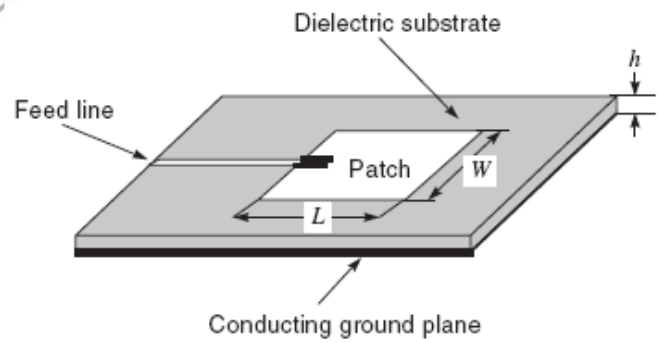
The helical antenna

Yagi, but with circular polarisation. This mode is commonly used for satellite communications, particularly at lower frequencies where a dish would be impractically large.

PATCH ANTENNAS

Patch antennas, as seen in Figure below, are based upon printed circuit technology to create flat radiating structures on top of dielectric, ground-plane-backed substrates. The appeal of such structures is in allowing compact antennas with low manufacturing cost and high reliability. It is in practice difficult to achieve this at the same time as acceptably high bandwidth and efficiency. Nevertheless, improvements in the properties of the dielectric materials and in design techniques have led to enormous growth in their popularity and there are now a large number of commercial applications. Many shapes of patch are possible, with varying applications, but the most popular are rectangular (pictured), circular and thin strips (i.e. printed dipoles).

In the rectangular patch, the length L is typically up to half of the free space wavelength. The incident wave fed into the feed line sets up a strong resonance within the patch, leading to a specific distribution of fields in the region of the dielectric immediately beneath the patch, in which the electric fields are approximately perpendicular to the patch surface and the magnetic fields are parallel to it. The fields around the edges of the patch create the radiation, with contributions from the edges adding as if they constituted a four-element array. The resultant radiation pattern can thus be varied over a wide range by altering the length L and



Microstrip patch antenna

4	Menu Select Buttons	Marked with plus (+) and minus (-) symbols
5	Menu Button	Used for changing functions and settings. There is a provision to lock the keypad to prevent the channel or other settings from changing accidentally while the radio is in the user's pocket.
6	Loud Speaker	For making the audible sound.
7	Push-To-Talk Button (PTT)	Users press and hold the button to talk, then let go to listen.
8	ON/OFF Switch and Volume Control.	Users can press the Switch to Power ON and OFF the walkietalkie
9	LED Indicator	Light shows when channels are busy
10.	Microphone	Unlike some models, Walkie-talkie has separate Loudspeaker
11.	Transmit Call Tone	This sends a tone signal to other radios on the same channel alerting them that the user wants to talk.



Parts of Walkie - Talkie

Applications

1. Military and Police organizations use the handheld radios for variety of purposes.

2. Now a days it is widely used in shopping malls, factories and even in apartments.

Advantages

1. These are robust, easy-to-use and simple.

2. Lots of people can listen and only one needs to talk at once.

Disadvantages

1. The Analog units are much expensive.

2. They are not designed for communication over longer ranges.

3. Users are hearing additional noises on the two-way radios or other conversations (interference with radios)

Full Duplex

In a Full-duplex transmission mode shown in figure below the communication between the sender and the receiver occurs, simultaneously. The duplex transmission mode is like a two-way road in which traffic can flow in both the direction at the same time. Here, the entire capacity of the channel is shared by both the transmitted signals, travelling in opposite directions by sharing the channel capacity in two different ways. In this mode of communication, the user physically separates the link in two parts, viz. one for sending and other for receiving.

Then, the user lets the capacity of a channel to be shared by the two signals travelling in opposite directions. Full Duplex can be understood with an example of a Mobile phone. When two people communicate over a mobile phone, both are free to speak and listen at the same time.



Full Duplex Transmission Mode

Mobile Phone

A mobile phone is a portable device that access to Cellular radio system. It has many names like, Cell phone, smart phone or telephone. This device is classified into two categories.

1. Simple device 2. Smart device

In simple devices, the user can access to make and receive the calls and send/ receive the messages. While smart devices have the facility to access the internet along with the above said two facilities.



Parts of a Mobile phone

Basic Principle of Mobile Phones

A mobile phone is a two-way radio, consisting of a radio transmitter and a receiver as shown in Figure above The mobile phone converts the received voice into an electrical signal, which is then transmitted as radio waves to the nearest mobile tower. Then, the network of mobile towers relays the radio wave to the dialled mobile phone, which converts back the radio wave to an electrical signal and then to sound waves. In the basic form, a mobile phone works just like a Walkie-talkie.

In additional to the basic function of the voice calls, most modern mobile phones come with additional

features such as web surfing, camera, games, messaging and music. Smart phones can perform similar functions of a portable computer.

A cellular Network, also known as a mobile network is a network of mobile base stations that provide coverage for the user to establish phone calls, text messages and data services (Mobile internets).

Radio Waves

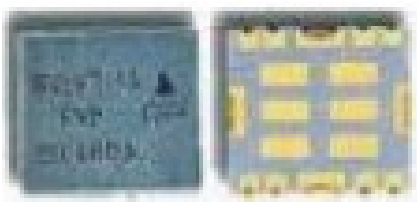
Mobile phones use radio waves for communication purposes as shown in Figure below. Radio waves transmit digitized voice or data in the form of oscillating electric and magnetic fields, called the Electro - Magnetic Field (EMF). The rate of oscillation is called frequency of radio waves, which carry the information and travel in air at the speed of light. Mobile phones transmit radio waves in all directions. The waves can be absorbed and reflected by surrounding objects before they reach the nearest mobile tower. For example, when the mobile phone is placed near to users head during a call, a portion of the emitted energy is observed into users head (ear) and body. In this event, much of the mobile phones EMF energy is wasted and no longer available for communication. In the following sections, let we see the various components of the mobile phone communication.



Radio waves (EMF)

Antenna

An antenna converts an electrical signal in to the transmitting radio wave and vice versa. Mobile phones use single antenna as transmitter and the receiver, others have multiple transmitting or receiving antennas. Figure below shows a Mobile phone antenna switch.



Mobile Phone Antenna Switch

An antenna is a metallic element (such as copper) having particular size and shape for transmitting and receiving specific frequencies of the radio waves. Older generation mobile phones have external or extractable antennas, while modern mobile phones contain more compact antenna, which is built inside the device. It is important to understand that any metallic component in the device (such as the circuit board and the metal frame) can interact with the transmission antenna(s) and contribute to the pattern of the transmitted signal.

Many modern smart phones also contain more than one type of antenna. In addition to the Cellular antenna, they may also have Wi-Fi, Bluetooth and/or GPS antennas.

Specific Absorption Rate (SAR) is the guidelines created for measuring the rate at which the body tissue absorbs radiation during cell phone operation. It is set at a maximum of 1.6 watts/kilogram of radiation energy absorbed by the body. Over exposure of cell phone radiation might cause cancer.

Connectivity

The magnitude of the received signal from the mobile tower is called the "signal strength" which is commonly indicated by "bars" on the mobile phone as shown in Figure below. The connectivity between a mobile phone and its cellular network depends on both signals and is affected by many factors, such as the distance between the phone and the nearest mobile tower, the number of obstacles/hindrance between them and the type of wireless technology (e.g. GSM or CDMA).



Mobile phone Signal Strength Image

A poor reception (fewer bars) normally indicates a long distance and/ or much signal interruption between the mobile phone and the mobile tower.

Hardware parts of a GSM Mobile Phone

The block diagram below shows the Hardware parts of a GSM mobile phone. The components which include display (LCD, Touch screen), keypad, microphone, speaker, SIM card, battery, USB port, antenna, memory unit (RAM, ROM), camera, CODEC, RF part, DAC/ ADC, baseband part (L1/Layer 1/physical layer) running on DSP, Application/ protocol layers on CPU, ON/OFF switch and Bluetooth/GPS features

1. Mobile Phone RF Transceiver

Generally all the mobile phone will have RF part which consists of RF frequency up converter and RF frequency down converter. For GSM system, up converter converts modulated baseband signal (I and Q) either at zero IF (Intermediate frequency) or some IF to RF frequency (890 to 915 MHz). RF down converter converts RF signal (935 to 960 MHz) to baseband signal (I and Q). For GSM, GMSK (Gaussian Minimum Shift Keying) modulation is used.

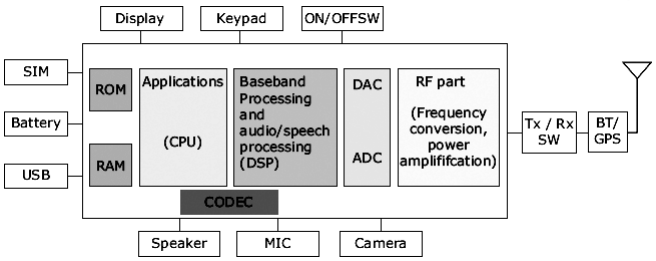
2. Mobile phone Antenna

Antenna is the metallic object which converts electro-magnetic signal to electric signal and vice versa. Commonly used antennas in the mobile phone are helix type, planar inverted F type, whip or patch type. Microstrip

based patch type of antennas are popular among mobile phones due to its size, easy integration on the PCB and multi frequency band of operation.

3. Tx/Rx Switch

As there is only one antenna used for both transmission and reception at different times, Tx/Rx switch is used to connect both Tx path and Rx path with antenna. Tx/Rx switch is controlled automatically by DSP based on GSM frame structure with respect to the physical slot allocated for that particular GSM mobile phone in both downlink and uplink. For FDD systems diplexer is used in place of switch which acts as filter to separate various frequency bands.



Hardware parts of a GSM mobile Phone

4. Mobile phone Baseband part

This part basically converts voice/data to be carried over GSM air interface to I/Q baseband signal. This is the core part which changes modem to modem for various air interface standards viz. CDMA, Wimax, LTE, HSPA and more. It is often named as physical layer or Layer 1 or L1. It is ported usually on DSP (Digital Signal Processor) to meet latency and power requirements of mobile phone. For speech/audio, codec is used to compress and decompress the signal to match the data rate to the frame it has to fit in. CODEC converts speech at 8 kHz sampling rate to 13 kbps rate for full rate speech traffic channel. To do this RELP (Residually Excited Linear Predictive Coder) speech coder is used which packs 260 bits in 20 ms duration to achieve 13 kbps rate. The baseband or physical layer will add redundant bits to enable error detection as well as error correction. Error detection is obtained with CRC and error correction with forward error correction techniques such as convolution encoder (used at transmit part) and decoder (used at receive part).

5. ADC and DAC

ADC (Analog to Digital Converter) and DAC (Digital to Analog Converter) are used to convert analog speech signal to digital signal and vice versa in the mobile handset. At Transmit path, ADC converted digital signal is given to speech coder. There are various ADCs available, among them popular one is sigma delta type. AGC (Automatic Gain Control) and AFC (Automatic Frequency Control) are used in the receiver path to control gain and frequency. AGC helps to maintain working of DAC satisfactorily, as it keeps signal within the dynamic range of DAC. AFC keeps frequency error within limit to achieve better receiver performance.

6. Mobile phone OS (Operating System)

Various OS supported in mobile phone are Symbian, Java, Android, RT-Linux, Palm, etc. It runs on CPU of different manufacturers. For time critical applications RTOS (Real-Time Operating System) is used.

7. Battery

It is the only major source of power to make / to keep mobile phone functional. There are various types of batteries made of Nickel Cadmium (NiCd), Nickel Metal Hydride(NiMH), based on lithium, Li-ion and so on. The major factors for designers is to reduce battery size, last for more talk time and increased battery life. Battery comes usually from 3.7 to 4.2 voltages and from 600 mAh to 7000 mAh ratings.

Battery charger is usually provided with mobile phone to charge the battery. It is an AC to DC converter.

8. Microphone:

Microphone or Mic converts air pressure variations (result of our speech) to electrical signal to couple on the PCB for further processing. Usually, in mobile phone has mic of types condenser, dynamic, carbon or ribbon are used.

9. Speaker

It converts electrical signal to audible signal (pressure vibrations) for human being to hear. This is often coupled with audio amplifier to get required amplification of audio signal. It also tied with volume control circuit to change (increase or decrease) the amplitude of the audio signal.

10. Camera

Now-a-days almost all the mobile phones are having the camera feature for one to click pictures at various occasions. It is the major specification in increasing the cost of mobile phone. Latest mobile phones are fitted with various mega pixel cameras such as 12 mega pixels, 14 mega pixels, even 108 and 200 mega pixels. This has become evident because of advancement in sensor technology. If one wants to buy low cost mobile phone, they usually go for non camera mobile phone.

11. Display

There are various display devices used in mobile phone such as LCD (Liquid Crystal Display), TFT (Thin-film transistor) screen, OLED (Organic Light Emitting Diode), TFD (Thin Film Diode), touch screen of capacitive and resistive type etc., (Capacitive touch is familiar and sensitive).

12. Keypad

Earlier days keypad was simple matrix type keypad which contains numeric digits (0 to 9), alphabets (a to z), special characters and specific function keys. These have been designed for various applications such as accepting call, rejecting call, cursor movement (left, right, top, down) dialling number, typing name/sms/mms and so on. Now-a-days keypad has been removed from the phone and it has become part of mobile phone software. It pops

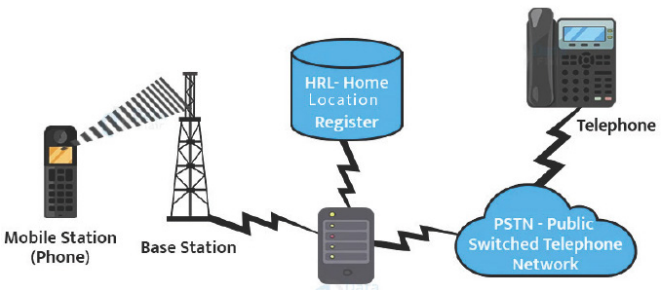
on the display screen itself which can be operated by user using touch of a finger tip.

MOBILE PHONE TECHNOLOGIES

Cellular technology is one of the mobile technologies that gave mobile phones the name "mobile phone". Cellular technology basically refers to having many small interconnected transmitters. The other main concept of Cellular technology was that it has "multiple access", meaning it places multiple voice or data connection into a single radio channel.

Types of Mobile phone Technologies

Many people use mobile phones, but do not know about the technology variances. In India, many mobile phones runs based on GSM and CDMA networks only. Nowa- days 5G is extremely growing in India, which operates mainly based on VoLTE Network technology. An overview of the important and widely used mobile network technologies in India and across the world is presented in the following sections.



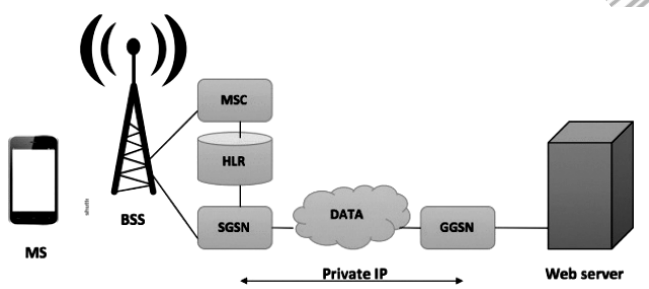
MSC - Mobile-Services Switching Center

GSM protocal

GSM (Global System for Mobile Communication)

GSM is the original 2G standard launched in 1991. It was the first major mobile technology. GSM protocol shown in Figure above was initially based on time division, meaning calls take turns using the radio signal.

GSM is the global technology authenticates SIM cards and performs simultaneously voice and data transmission. 3G GSM is better for world travellers, which covered most of the countries but, weak in rural locations. GSM traditionally work on 900, 1800 and 1900 MHz and was initially designed, only for circuit switched voice service, which is a combination of FDD (Frequency Division Duplex) and TDD (Time Division Duplex).



Public IP

GPRS (General Packet Radio Service)

GPRS is the service provided by the GSM network as shown in Figure above. This is a packet data transport-based service, which provides mobile internet over a mobile device. This uses same radio interface of the mobile used to make calls.

GPRS support Nodes are devised in to two

1. SGSN: Serving GPRS Support Node in VPLMN (Visited Public Land Mobile Network) for GPRS functionality in GSM network.

2. GGSN: Gateway GPRS Support Node between Mobile and Internet.

Global Positioning System (GPS)

GPS is a space-based satellite Navigation system that provides location and time information in all weather conditions, anywhere on or near the earth where there is an unobstructed Line-of-Sight to four or more GPS Satellites. The system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States of America Government and is freely accessible to anyone with a GPS receiver. Figure below shows the representation of GPS.



Space based satellite Navigation System

The GPS is made up of a network of 24 satellites placed into orbit by US Department of Defences. GPS was originally intended for military applications but, in the 1980s, the US Government made the system available for civilian use. GPS works in any weather conditional, anywhere in the world and 24 hours a day. There are no subscription fees or setup charges to use GPS.

Major Differences between GPS and GPRS

1. GPS (Global Positioning System) will give you location in terms of Latitude and Longitude.

2. GPRS will allow user to transfer data over cellular networks.

MULTIPLE ACCESS TECHNIQUES

Multiple access techniques are used to allow a large number of mobile users to share the allocated spectrum in the most efficient manner.

In wireless communication system, it is often desirable to allow the subscriber to send information to the base station while receiving information from the base station simultaneously.

A cellular system divides any given area into mobiles where a mobile unit in each communicates with a base station. The main aim in the cellular system design is to be able to increase the capacity of the channel i.e. to handle as many calls as possible in a given bandwidth.

There are several different ways to allow access to the channel. Some of them are as follows.

Cyber Security

Cyber security is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. It can be classified into three categories:

1) **Information Security:** Information security aims to protect the users' private information from unauthorized access and identity theft. It protects the privacy of data and hardware that handle, store and transmit that data. Examples of Information security include User Authentication and Cryptography.
2) **Network Security:** Network security aims to protect the usability, integrity, and safety of a network, associated components, and data shared over the network. When a network is secured, potential threats gets blocked from entering or spreading on that network. Examples of Network Security includes Antivirus and Antispyware programs, Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.
3) **Application Security:** Application security aims to protect software applications from vulnerabilities that occur due to the flaws in application design, development, installation, and upgrade or maintenance phases.

Just to have basic understanding of the cyber world, one should have fundamental acquaintance with the basic terms of cyber space, some of the most important cyber security terminologies that one should know are as follows:

1. **Cloud:** A technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it is a collection of computers with large storage capabilities that remotely serve requests.
2. **Software:** A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.
3. **Domain:** A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace.
4. **Virtual Private Network (VPN):** A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.
5. **IP Address:** An internet version of a home address for your computer, which is identified when it communicates over a network; For example, connecting to the internet (a network of networks).
6. **Exploit:** A malicious application or script that can be used to take advantage of a computer's vulnerability.
7. **Breach:** The moment a hacker successfully exploits vulnerability in a computer or device, and gains access to its files and network.
8. **Firewall:** A defensive technology designed to keep the bad guys (cyber threats) out. Firewalls can be hardware or software-based.
9. **Malware:** An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include; viruses, trojans, worms and ransomware as covered in a following heads.
   i. **Virus:** A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.
   ii. **Ransom ware:** A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered. For example, WannaCry Ransom ware. For more information on Ransomware, check out our free Ransomware Guide.
   iii. **Trojan horse:** A piece of malware that often allows a hacker to gain remote access to a computer through a "back door".
   iv. **Worm:** A piece of malware that can replicate itself in order to spread the infection to other connected computers.
   v. **Bot/Botnet:** A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a "botnet" and is controlled by the hacker or "bot-herder".
   vi. **DDoS:** An acronym that stands for distributed denial of service – a form of cyber-attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
   vii. **Phishing or Spear Phishing:** A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

NEED AND CONCEPT BEHIND SECURITY

To help and explain "why security knowledge is so important?" let's first establish the baseline of how daily life operates for most of us. "There aren't many careers left that aren't based on technology, nowadays even teachers in classrooms are using Smart boards, and many a times someone who comes to your home to do contract work will

whip out a smart phone or tablet and add information to an app on the spot, something as small as clicking attachments in emails without knowing if they are safe or there are many more incidences where we need to understand that how such things can affect our security.

We need to understand that "how basic security knowledge can help any career?" Aside from simply not clicking suspicious email attachments, there are things nearly all employees can do to enhance company security and make themselves more valuable workers. Within any role in the organization, learning about security can help an individual understand the risks and make informed decisions for their key stakeholders, here are a few examples:

- ✦ In sales, reassure customers of an organization's security posture.
- ✦ In corporate communications, you should assess in the context of business reputation and brand trust.
- ✦ The legal team should ensure that the right security clauses are built into supplier and customer contracts.
- ✦ Regarding HR and/or security, know what's needed for better security awareness and training.
- ✦ Product managers should advise on good security features.
- ✦ In engineering development, make sure you develop secure code.
- ✦ Security professionals should perform reviews and quality assurance tests for functional and security verification.
- ✦ Corporate management should ensure that a good security incident response plan is in place to address any vulnerability.

Type of Cyber Threats

Below mentioned are the few examples of online cyber security threats.

1. **Computer Viruses:** A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to the computer in the process. It is perhaps the most well-known computer security threat. Carefully evaluating free software downloads from peer-to-peer file sharing sites, and emails from unknown senders are crucial to avoiding viruses. Most web browsers today have security settings which can be ramped up for optimum defense against online threats. But, single most-effective way offending off viruses is up-to-date antivirus software from a reputable provider.
2. **Spyware Threats:** A serious computer security threat, spyware is any program that monitors your online activities or installs programs without the consent for profit or to capture personal information. While many users won't want to hear it, reading terms and conditions is a good way to build an understanding of how your activity is tracked online. And of course, if a company don't recognize is advertising for a deal that seems too good to be true, be sure that we have an internet security solution in place and click with caution.
3. **Hackers and Predators:** Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change, or destroy information as a form of cyber-terrorism. These online predators can compromise credit card information, lock you out of your data, and steal your identity. As we may have guessed, online security tools with identity theft protection are one of the most effective ways to protect yourself from this brand of cybercriminal.
4. **Phishing:** Phishing attacks are some of the most successful methods for cybercriminals looking to pull off a data breach. Masquerading as a trustworthy person or business, phishes attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Antivirus solutions with identity theft protection can be used to recognize phishing threats in fractions of a second.

CYBER CRIME AND LAW

A commonly accepted definition of cybercrime is a "crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs". While there are many different definitions of cybercrime, they all have a few key concepts throughout. These key concepts are criminal activity and the use or abuse of computers. With these concepts in mind cybercrime can be easily defined as using a computer to commit a criminal act.

Cybercrimes create an overwhelming task for law enforcement bureaus since they are extremely technological crimes. Law enforcement organizations must have individuals trained in computer disciplines and computer forensics in order to accurately investigate computer crimes or cybercrimes that have been committed. Additionally, many states must modernize and generate legislation, which disallows cybercrimes and outlines suitable penalties for those crimes. Cybercrimes will likely become more frequent with the arrival of advance technologies. It is important that civilians, law officials, and other associates of the justice system are well-informed about cybercrimes in order to diminish the threat that they cause.

Understanding the threat of cybercrimes is a very pertinent issue because technology holds a great impact on our society as a whole. Cybercrime is growing every day because since technological advancing in computers makes it very easy for anyone to steal without physically harming anyone because of the lack of knowledge to the general public of how cybercrimes are committed and how they can protect themselves against such threats that

cybercrimes poses. There are many ways or means where cybercrimes can occur. Here are a few causes and methods of how cybercrimes can be committed on a daily basis.

1. **Hacking:** In other words, can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.
2. **Theft of information contained in electronic form:** This type of method occur when information stored in computer systems are infiltrated and are altered or physically being seized via hard disks; removable storage media or another virtual medium.
3. **Email bombing:** This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.
4. **Data diddling:** It is the changing of data before or during an intrusion into the computer system. This kind of an occurrence involves moving raw data just before a computer can processes it and then altering it back after the processing is completed.
5. **Salami attacks:** This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack. This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace an example is the "Ziegler case "wherein a logic bomb penetrated the bank's system, which deducted only 10 cents from every account and deposited it in one particular account which is known as the "penny shaving".
6. **Denial of Service attack:** It is basically where a computer system becomes unavailable to its authorize end user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more requests than it can handle which in turn causing the pc to crash. E.g., Amazon, Yahoo. Another incident occurs in the past whistle blower site wikileaks.org got a DDoS attack.
7. **Virus / worm attacks:** Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by changing or erasing it. However, worms are not like viruses, they do not need the host to attach themselves to but make useful copies of them and do this constantly till they consume up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers around the world.
8. **Logic bombs:** They are basically a set of instructions where can be secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects. This suggests that these programs are produced to do something only when a specific event (known as a trigger event) occurs. E.g. Chernobyl virus.
9. **Trojan attacks:** The term suggests where a program or programs mask themselves as valuable tools but accomplish damaging tasks to the computer. These programs are unlawful which flaccidly gains control over another's system by assuming the role as an authorised program. The most common form of a Trojan is through e-mail. E.g. lady film director in the U.S.
10. **Internet time thefts:** This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.
11. **Web jacking:** This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means. An example of such method was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers whereas another was the 'gold fish' case, site was hacked and the information relating to gold fish was altered and the sum of $ 1 million was demanded.

Cyber terrorism may be defined to be where the deliberate use of disrupting activities, or the risk thereof, via virtual machine, with the purpose to further public, political, spiritual, radical or to threaten any person in continuance of such purposes. Theft crimes include the following:

1. **Credit/Debit Card Fraud:** It is the unlawful use of a credit/debit card to falsely attain money or belongings. Credit/debit card numbers can be stolen from leaky web sites, or can be obtained in an identity theft scheme.
2. **Identity theft:** Identity theft occurs when someone seizes another's individual information without his or her awareness to commit theft or fraudulency. Typically, the victim is led to believe

they are revealing sensitive private data to a genuine business, occasionally as a response to an e-mail to modernize billing or membership information etc.

3. **Non-delivery of Goods and Services:** Goods or services that were acquired by individuals online those were never sent.
4. **Phony Escrow Services:** This is where auction participants were persuading by the fraudster where he or she will recommend the use of a third-party escrow service to help the exchange of money and merchandise. The victim is unmindful the impostor has deceived a legitimate escrow service the victim sends payment or products to the phony escrow and obtains nothing in return.
5. **Ponzi/Pyramid method:** This is where investors are lured to capitalize in this falsified arrangement by the promises of irregularly or abnormally high profits but none of the funds are actually made by the so called "investment firm".

Cyber Crime is regulated by Cyber Laws or Internet Laws, in India it is addressed by the Information Technology Act, 2008.

Snapshot of Important Cyber law Provisions in India

OFFENCE	SECTION UNDER IT ACT
Tampering with Computer source documents	Sec.65 (IT Act)
Hacking with Computer systems, Data alteration	Sec.66 (IT Act)
Publishing obscene information	Sec.67 (IT Act)
Un-authorized access to protected system	Sec.70 (IT Act)
Breach of Confidentiality and Privacy	Sec.72 (IT Act)
Publishing false digital signature certificates	Sec.73 (IT Act)
Sending threatening messages by email	Sec 351 (BNS)
Sending defamatory messages by email	Sec 356 (BNS)
Forgery of electronic records	Sec 336 (BNS)
Bogus websites, cyber frauds	Sec 318 (BNS)
Email spoofing	Sec 336 (BNS)
Web-Jacking	Sec 308 (BNS)
E-Mail Abuse	Sec 356 (BNS)
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

E-BANKING

- Electronic banking is a form of banking in which funds are transferred through an exchange of electronic signals rather than through an exchange of cash, checks, or other types of paper documents. It is also known as electronic funds transfer (EFT) and basically uses electronic means to transfer funds directly from one account to another. Internet banking is a financial institution with no physical branches; everything is completed online. There is no ability to cash a check, deposit cash and or coinage and such. Online banking is the ability to access account information, make transfers, set up automatic payments and such via the Internet. Internet banking typically is an electronic payment system, that allows the bank account holder to execute the monetary transaction, such as bill payments, fund transfer, stop payment, balance enquiries, etc. anytime and anywhere using the bank's website. Online banking is part and parcel of the core banking system handled by the bank.
- Automated Clearing House (ACH) is a computer-based electronic network that coordinates electronic payments and automated money transfers i.e processes transactions, usually domestic low value payments, between participating financial institutions. ACH is a way to move money between banks without using paper checks, wire transfers, credit card networks, or cash. ACH and EFT payments are similar in that they are both forms of electronic payments. However, EFT refers to all digital payments, whereas an ACH is a specific type of EFT. An ACH payment occurs when money moves from one bank to another bank. This money moves electronically, through the Automated Clearing House Network. In India National Automated Clearing House, or NACH, introduced by National Payments Corporation of India, is a centralized clearing service that aims at providing interbank high volume, low value transactions that are repetitive and periodic in nature. Most people already use ACH payments, although they might not be familiar with the technical jargon. When employers pay wages through direct deposit or consumers pay bills electronically out of checking accounts, the ACH network is often responsible for those payments.

UPI

Unified Payments Interface is an instant real-time payment system developed by National Payments Corporation of India facilitating inter-bank transactions. The interface is regulated by the Reserve Bank of India and works by instantly transferring funds between two bank accounts on a mobile platform. Unified Payments Interface is a real time payment system that allows sending or requesting money from one bank account to another. Any UPI client app may be used and multiple bank accounts may be linked to single app. Money can be sent or requested with the following methods:

- **Virtual Payment Address (VPA) or UPI ID:** Send or request money from/to bank account mapped using VPA.

```
while(test condition)
{
        ...
        if(condition1)
        {
        ...
        break
    }
    ...
}
...
```

If the 'condition1' is true then computer encounter break statement and terminate the loop.

```
void main( )
{
    int n, a[100], i;
    // Read 100 array elements
    ...
    printf("Enter your number to be search : ");
    scanf("%d",&n);
    for( i = 0 ; i< 100 ; i++ )
    {
        if(a[i] = = n)
        {
            printf("Your number is on position %d\n",i
            + 1); break;
        }
    }
    getch( ) ;
}
```

Here when computer encounter your desired number then computer print the position of number and terminate the loop and go to next immediate statement getch( ).

continue statement

During loop operations, it may be necessary to skip the part of the body of the loop during certain condition. We are using continue statement to skip the portion of loop. For example we are determining the square root of any number and print it. But our condition is that if number is negative then we don't want to determine square root. At that time we can use continue statement to skip the body of loop for negative number.

```
while(test condition)
{
    ...
    if(condition1)
    {
        ...
        continue;
    }
    ...
}
```

Let's see the example of skipping negative number printing using 'continue'. Here we are reading the number until number is not greater than 1000. If the number is negative then we have to not print it otherwise print it.

```
void main ( )
  {
    int n=1;
     while(n<=1000)
     {
            printf("Enter your number : ");
            scanf("%d", &n);
            if(n<0)
                continue;
            printf("Your number is %d\n", n);
     }
}
```

Method of Structured Programming

Large program are difficult to understand. Hence the large programs are written using three logic structures:

1. Sequence 2. Selection 3. Iteration

A **sequence** construct is a set of instructions serially performed without any looping. The normal flow of control is from top to bottom and from left to right unless there is an iteration construct. Thus the first instruction in the program is executed first, then control passes to the next instruction that sequence.

A **selection** construct involves branching but the branches join before the exit point. The selection is required and the flow of control depends on the selection. For example, if statement, if…else statement and switch statement in C language.

An **iteration** construct contains loops in it but has only one exit point. This construct allows repeated execution of a set of codes without repeating codes in the program. It saves the trouble of writing the same codes again and again in the program. For example, while loop, do..while loop and for loop in C language.

★★★

Shortcuts to select text using mouse and Keyboard

Press	To extend a selection
Shift +RightArrow	One character to the right
Shift + Left Arrow	One character to the left
Ctrl+Shift+Right Arrow	To the end of a word
Ctrl+Shift+Left Arrow	To the beginning of a word
Shift+End	To the end of line
Shift+Home	To the beginning of line
Shift+Down Arrow	One line down
Shift+Up Arrow	One line up
Ctrl+Shift+Down Arrow	To the end of a paragraph
Ctrl+Shift+Up Arrow	To the beginning of a paragraph
Shift+Page Down	One screen down
Shift+Up Down	One screen up
Ctrl+Shift+Home	To the beginning of a document
Ctrl+Shift+End	To the end of a document
Alt+Ctrl+Shift+Page Down	To the end of a windo
Ctrl+A	To select the entire document
Ctrl+Shift+F8 (use the arrow keys)	To a vertical block of Text
F8+arrow keys; press Esc to cancel	To a specific location in a document
For deleting the text and graphics	
Backspace	Delete one character to the left
Ctrl+Backspace	Delete one WORD to the left
Delete Key	Delete one character to the Right
Ctrl+Delete	Delete one word to the left right
Ctrl+X	Cut selected text to the Clipboard
Ctrl+Z	Undo the last action

Keys and their functions in a worksheet

Press	To
Arrow Keys	Move one cell up,left or right
Ctrl+Arrow keys	Move to edge of current data region
Home	Move to the beginning of the row
Ctrl+Home	Move to the beginning of the worksheet
Ctrl+End	Move to the last cell on the worksheet, which is the cell at the intersection of the rightmost used column and the bottom-most used row
Page Down	Move down one screen
Page Up	Move up one screen
Alt+Page Down	Move one screen to the right
Alt+Page Up	Move one screen to the left
Ctrl+Page Down	Move to the next sheet in the workbook
Ctrl+Page Up	Move to the previous sheet in the workbook
Alt+F6 or Ctrl+Tab	Move to the next workbook or window
Ctrl+Shift+F6 or Ctrl+Shift+Tab	Move to the previous workbook or window
F6	Move to the next pane in a workbook that has been split
Shift+F6	Move to the previous pane in a workbook that has been split
Ctrl+Backspace	Scroll to display the active cell
F5	Display the Go To dialog box
Shift+F5	Display the Find dialog box
Shif+F4	Repeat the last Find Action
Tab	Move between unlocked cells on a protected worksheet