NETWORK SECURITY ON INTERNET

# CYBER CRIME:-

* **Crime means any illegal activities against law.**
* **Cyber crime is also called as computer crime.**
* **Cyber crime is defined as the crime committed through internet where computer is used as a tool or a target.**
* **Cyber crime committed on cyber space.**
* **Due to increase in the use of mobile phones, internet, computers, e-commerce, e-banking, etc. cyber crime is increasing day to day.**
* **Cyber crime does not obey or comes under any particular jurisdictional boundary.**
* **Example:- hacking, pornography, online fraud, cyber terrorism, software piracy, spamming, etc.**

# TYPES OF CYBER CRIME:-

* **Types of cyber crime where computer is used as target (using a computer to attack other computers):-**
	1. **Hacking**
	2. **Virus**
	3. **Worm**
	4. **Cookies**
	5. **Spam**
	6. **Denial of Service**
	7. **Snooping**
	8. **Spoofing**
	9. **Software piracy**
* **Types of cyber crime where computer is used as a tool (using a computer to commit real world crimes):-**
1. **Cyber terrorism**
2. **Intellectual Property Right violation**
3. **Cyber squatting**
4. **On-line fraud**
5. **Pornography**
6. **Phishing**
7. **Vishing**
8. **Cyber stalking**

# HACKING:-

* **It is a cyber crime where computer is used as a target.**
* **Hacking is a cyber crime where a computer is used to hack anybodies personal information like credit card information, bank account details, etc. and causes financial loss to the victim without his or her knowledge.**
* **A person who hacks is known as hacker.**
* **By hacking web server, taking control on another person’s website is called as web hijacking.**

# VIRUS:-

* **It stands for Vital Information and Resource Under Seize.**
* **Virus is a maliciously written code (destructive program) that replicates itself.**
* **It is a malicious code that may damage hardware, software, information files or other resources of a computer.**
* **Human interaction is necessary for a virus to spread to another user’s file.**
* **It enters to a computer through internet, file transferring, downloading, uploading, use of pen drives, memory card sharing, etc.**
* **Example:- Pakistani brother, love birds, I LOVE YOU(2000), etc.**
* **Types of virus:-**
1. **Boot infectors**
2. **System infectors**
3. **Executable program infectors**

## Boot infectors:-

* + **Some viruses that reside in the boot sector of the disk and not in the program file are known as boot infector virus.**
	+ **It gets loaded as soon as the system is switched on and takes the control of the system.**
	+ **It does not allow to access the disk of the system.**
	+ **These viruses can create Bad Sectors and stay in memory of the computer until the disk is formatted or system is shut off.**
	+ **These viruses corrupt the BIOS of a computer system.**

## System infectors:-

* + **Operating system is required to interact with the computer.**
	+ **The viruses that are attached themselves to memory resident files such as COMMAND.COM is called as system infector virus.**
	+ **These infectors take the control of the system and affects the hard disk after the system is booted.**
	+ **The system become hang after the system is switch on.**
	+ **These viruses corrupt the operating system, which is used as an interface between user and computer system.**

## Executable program infectors:-

* + **These are the most dangerous virus around.**
	+ **The viruses that are attached to the program files and can spread immediately to any of the executable files are called as executable program infector virus.**
	+ **When we start a program, the virus is executed first and then allows the original program to follow.**
	+ **It is memory resident and infects every executable program.**
	+ **It also increases the memory size of .EXE and .COM files.**
	+ **These viruses can be spread through memory card, pen drives, etc. which are used for data transfer.**

## Prevention of VIRUS attack:-

* **Following few tips can prevent our computer from VIRUS attack:-**
1. **Install Anti-virus/malware software in the system.**
2. **Keeping the Anti-virus Software Up to Date.**
3. **Scan the computer system regularly to detect and remove virus.**
4. **Keep the personal information safe by using privacy setting.**
5. **Avoid using open (free) Wi-Fi.**
6. **Do not click on unwanted software or link.**
7. **Always back up the files.**
8. **Use multiple strong passwords to avoid hacking.**

# WORM:-

* **It stands for Write Once Read Many.**
* **A worm is designed to replicate itself from one computer to another automatically.**
* **It enters into a computer without the knowledge of the user, through e-mail or file transfer.**
* **Worms replicate themselves like viruses, but do not alter files the way that viruses do.**
* **Worms reside in the memory and remain unnoticed until their effect become overwhelming.**
* **Worms replicate themselves in a large volume and spread very quickly, So that the system becomes slow and also internet cannot be operated to display a webpage, so that Denial of Service attack occurs.**

# TROJAN HORSE:-

* **A Trojan horse is a malicious program disguised as a normal application.**
* **Trojan horse programs do not replicate themselves like a virus, but they can be propagated as attachments to a virus.**
* **It breaks or damages the security of the computer system.**
* **When a system is running, Trojan horse programs run in the backdoor and access the computer files stored in the hard disk.**
* **Trojan horses can be included in software as an attachment that is downloaded for free.**

Never download software from a source that you don’t trust.

* **They slow down the speed of the internet and destroy the files stored in the hard disk of the computer system.**
* **They can be removed by using updated Anti-virus software.**

# COOKIES:-

* **Cookies are the browsing history of visited sites on a web browser.**
* **Cookies are messages that web servers pass to our web browser when we visit internet sites.**
* **Our browser stores each message in a small file (only up to 4kb in size), called ‘cookie.txt’.**
* **When we request another page from the server, our browser sends the cookie back to the server.**
* **Cookies files contain information about visited websites, web pages or links on a web browser.**

## Uses of cookies:-

* **It is used to track website activities on a web browser.**
* **It is also used in online shopping to store personal information we enter, as well as any items in our electronic shopping cart, so that we don’t need to re-enter this information each time we visit the site.**
* **Cookies provide customized webpage with selected preferences.**
* **Web servers can use only information that we provide or choices that we make while visiting the website as content in cookies.**
* **Many websites use cookies to log in their users automatically.**

## Cookie security:-

* **Cookies do not create any danger to the user or can’t damage the computer.**
* **It only allows to reads the website activities on our web browser.**
* **One major security problem with cookies is that, they can easily be read by anyone using the computer.**

# DENIAL OF SERVICE ATTACK:-

* **It is a cyber crime.**
* **In this type of cyber crime a computer is used as a target.**
* **When a computer resource is flooded with more request than it can handle, the resource crashes.**
* **Therefore it denies the service access to the authorized users.**
* **These requests are made intentionally to make one or more network resources unavailable to their valid users.**
* **These types of attempts are called as Denial of Service (DoS) attack.**
* **DoS attack denies individual user from accessing a service due to heavy request or system crash.**

# SPAM:-

* **It is a cyber crime.**
* **In this type of cyber crime computer is used as a target.**
* **Spam means unwanted or unsolicited message or e-mail.**
* **Spamming is an act of sending unsolicited messages (spam) to many users at a time for advertisement.**
* **Spamming creates irritation due to unwanted messages, which is sent thousands per second.**
* **Spamming is random and untargeted to an individual person, but it may be targeted to a group.**

# SNOOPING:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a target.**
* **The act of secretly checking one’s mail, writing or any such information without his/her**

knowledge is called as ‘snooping’.

* **In the world of computer network, snooping attacks involve an intruder listening to traffic between two machines on a network.**
* **If traffic includes passing of unencrypted passwords, then an unauthorized user can potentially access the network and read confidential data.**
* **Snooping may be done in a number of ways:-**
1. **By getting someone’s login information by casually watching what he/she is typing.**
2. **Reading the files on someone’s computer in an unauthorized manner.**
3. **Using some software which keeps track of the activities and data being sent or**

received on someone’s computer.

# EAVESDROPPING:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a target.**
* **Suppose two friends are talking to each other and a third person is secretly trying to listen to**

their talks. What that person is doing is called ‘eavesdropping’.

* **Eavesdropping refers to unauthorized access to another person’s or organization’s data while**

the data is on its way on the network.

* **This may be done in number of ways:-**
1. **By setting up parallel telephone lines.**
2. **By installing some software (spyware) in the target computer.**
3. **By installing some receiver which captures the data while on its way.**

# SPOOFING:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a target.**
* **It is a crime that refers to provide someone’s false or fake identity and misusing it.**
* **It refers to actively introducing network traffic pretending to be someone else.**
* **For example, let a message is sent by a user to X, but it is received by Y in the name of X is called spoofing.**
* **Various types of spoofing are:-**
1. **Caller ID spoofing:-**

It is a service that allows a caller to call a user as someone else.

1. **E-mail spoofing:-**

It is a practice of sending an e-mail pretending to be someone else.

1. **IP address spoofing:-**

It refers to the creation of fake IP address, with the purpose of hiding the identity of sender.

1. **Protocol spoofing:-**

It is used to improve the performance of communication when an existing protocol is insufficient.

# CYBER-STALKING:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a tool.**
* **It is a computer crime used to stalk someone through internet.**
* **It is an online harassment or online abuse.**
* **It involves threatening behavior repeatedly like following a person, appearing at a person’s**

home or place of business, making harassing phone calls, leaving written messages, etc.

* **It also includes solicitation for sex, false accusations, defamation, etc.**
* **It also includes expression of desire to control, intimidate, or manipulate a victim.**
* **A cyber stalker may be someone the victim is familiar with, or a complete stranger, or is a criminal offense.**
* **Key factors to identify cyber-stalking cases include:**
1. **False accusations**
2. **Gathering information about the victim**
3. **Monitoring victim’s activities**
4. **Encouraging others to harass the victim**
5. **False victimization**

# SOFTWARE PIRACY:-

* **It is a cyber crime.**
* **In this type of cyber crime computer is used as a target.**
* **It is a computer crime refers to illegal copying, distribution or use of software, that cause a great financial loss of revenue for its publisher.**
* **Software piracy generally applies to the full-function commercial software.**
* **There are two types of software:-**
1. **Shareware:-**

It is a time-limited commercial software, which is provided to the user by taking some fees.

1. **Freeware:-**

It is a copyrighted, but freely distributed software which is provided to the user at free of cost.

* **Software piracy violates IPR.**
* **Different types of software piracy are:-**
1. **Soft-lifting**
2. **Client-server overuse**
3. **Hard-disk loading**
4. **Counterfeiting**
5. **Online piracy**

# CYBER TERRORISM:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a tool.**
* **It is a computer crime used to target military installations, power plants, air traffic control, bank, trail traffic control, telecommunication networks, police stations, medical, fire & rescue systems, etc.**
* **It is suitable for modern terrorists due to cheaper and remotely handle.**
* **It damages a large area of a cyber space.**
* **It also affects to large number of people.**

# IPR VIOLATION:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a tool.**
* **IPR stands for Intellectual Property Right.**
* **IPR gives exclusive rights for a person’s any innovation, discoveries or writing of books.**
* **IPR allows the concerned person to distribute or sell of his/her intellectual properties.**
* **It includes copyright law, patent law, trademark law, etc.**
* **Any violation of these laws is known as IPR violation.**

# CYBER SQUATTING:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a tool.**
* **Domain names are also trademarks and protected by ICANN’s domain dispute resolution**

policy and also under trademark laws.

* **It is a computer crime where a cyber squatter registers in a domain name identical to a popular domain name and attracts others in the name of that domain and gets financial benefits.**
* **It violates trademark law.**

# ON-LINE FRAUD:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a tool.**
* **It is a cyber crime used to cheat a person while the victim is buying or selling through internet.**
* **Online fraud steals personal information and gain financial benefits by making fraudulent transaction.**
* **Online fraud or scam can also occur in chat rooms, social media, e-mail, or on websites.**
* **It includes non-delivery payment or goods do not receive as per order, bank-related scams, etc.**

# PHISHING:-

* **It is a cyber crime.**
* **In this type of cyber crime, computer is used as a tool.**
* **In this cyber crime computer is used to send message or e-mail in the name of lottery and trying to fool people.**
* **Phishing refers to receiving unwanted mail or message from financial institutions, that will ask for user ID, password, bank account details to access user’s personal information and transferred money from the accounts of the victim.**
* **It is a fraud over internet to fool people into parting with their money.**
* **A study found the banking industry as soft target for phishing scams in India.**

# VISHING:-

* **It is a cyber crime.**
* **In this type of cyber crime computer is used as a tool.**
* **Vishing is a combination of “voice” and phishing.**

Vishing = phishing + voice

* **Vishing uses VoIP (Voice over Internet Protocol).**
* **It uses VoIP protocol to gain access to private, personal and financial information from the people in the name of financial reward.**
* **It exploits people’s trust using landline telephone services where the victim is on the call and**

losses its identity.

# PORNOGRAPHY:-

* **It is a cyber crime.**
* **In this type of cyber crime computer is used as a tool.**
* **It is a cyber crime that shows sexual acts in order to cause sexual excitement through books or films.**
* **It includes pornography websites, materials, videos, photos through computer, mobile phone and internet.**
* **It also includes child pornography through mobile phone and internet.**
* **It is a severe cyber crime that may be a cause of someone’s death or damaging social image of**

someone, etc.

* **Several consequences like, insensitivity, lack of concentration, addiction, etc. are the results of the on-line pornography.**

# BOT NETWORKS:-

* **It is a cyber crime.**
* **In this type of cyber crime computer is used as a target.**
* **It is a crime where a group of persons remotely send malicious links to the user’s computer**

and takes the control of the computer without the knowledge of the user.

* **If a victim is knowingly or unknowingly click on that link, then the Bot Network attackers**

access the victim’s computer remotely.

* **Like Trojan horse, it provides backdoor (a method of bypassing normal authentication) to access computer remotely.**

# NETWORK SECURITY ARCHITECTURE:-

* **Network security can also be termed as Internet security.**
* **It is a mechanism used to protect data transfer over the Internet.**
* **Internet means network of networks or international network or internetworking.**
* **Internet is a global collection of small and individual networks to form a single large network by using wire or wireless medium, to share data, information and resources among each other.**
* **Internet is a universally accessible network.**
* **Security means protection of data from unauthorized access.**
* **Internet security refers to secrecy or privacy of information on internet.**
* **Some key components of internet security architecture:-**
1. **Authentication:**

It is the action of verifying information such as identity, ownership or authorization.

1. **Access control (Authorization):**

It is a security measure that defines who can access a computer, when they can access it, and what actions they can take while accessing the computer.

1. **Privacy:**

It is the state that refers to secrecy or confidentiality of information.

1. **Integrity:**

It refers to accuracy and validity of data, that does not allow any unauthorized modification of data.

* **Various types of mechanism (technique) used in internet security:-**
1. **Cryptography**
2. **Encryption**
3. **Decryption**
4. **Digital signature**
5. **VPN**
6. **Firewall**
7. **Proxy server**

# CRYPTOGRAPHY:-

* **The word cryptography comes from two Greek words ‘kryptos’ means secret and ‘graphia’**

means writing/coding. Hence cryptography means the science of secret coding.

* **Julius caesar the great roman emperor is called as father of modern cryptography.**
* **He used veni, vidi, vici which means I came, I saw, I conquered.**

## Terms used in cryptography:-

### Plain text:-

An original message is called as plain text.

### Cipher text:-

The secret message/disguised message is called as Cipher text.

### Encryption/Encoding:-

* **The method used to convert a plain text into cipher text is called as encryption.**
* **The general equation of encryption is given as:**

EK(P)=C (Encryption of P is equal to C by using a key K) Where, E=Encryption algorithm

P=Plain text C=Cipher text

K=Key

Encryption

Plain text

Cipher text

ABC BCD

**EK=shift by 1(ABC)=BCD**

### Decryption/Decoding:-

* **Decryption is the reverse of encryption.**
* **It is a method used to convert a cipher text into plain text.**
* **The general equation of decryption is given as:**

DK(C)=P (Decryption of C is equal to P by using a key K) Where, D=Decryption algorithm

P=Plain text C=Cipher text

K=Key

Decryption

Plain text

Cipher text

BCD ABC

**DK=Shift by 1(BCD)=ABC**

## Types of cryptography:-

* **There are two types of cryptography:-**
1. **Symmetric key (private/secret key) cryptography**
2. **Asymmetric key (public key) cryptography**

### Symmetric key cryptography:-

* + **A cryptography that uses same keys for both encryption and decryption is called symmetric key cryptography.**
	+ **The single key used for both encryption and decryption is called as private key or secret key.**
	+ **A private key is visible to only authorized users (sender and receiver).**
	+ **It is more secure than asymmetric key cryptography.**

P P

**EK1(P)=C**

N/W

**DK2(C)=P**

RECEIVER

SENDER

Where, K1=K2=K= private key E=Encryption algorithm D=Decryption algorithm P=Plain text

C=Cipher text

o Types of symmetric key cryptography:-

1. **Stream cipher:-**
	* **In stream cipher, an original message is converted into secret message character by character.**
	* **In stream cipher the message size get altered after encoding (encryption).**
	* **It is a slower technique than block cipher.**
2. **Block cipher:-**
	* **In block cipher, a message is converted into a fixed size block of 2byte, 4byte, 8byte, 16byte, etc.**
	* **In block cipher message size does not get altered after encoding.**
	* **It is a faster technique than stream cipher.**

### Asymmetric key cryptography:-

* + **A cryptography that uses two different keys for encryption and decryption is called as asymmetric key cryptography.**
	+ **A key that is used for encryption is called as public key.**
	+ **A public is visible to all.**
	+ **A key that is used for decryption is called as private key.**
	+ **A private is visible to only authorized users.**
	+ **A private key is more secure than public key.**

P P

**EK1(P)=C**

N/W

**DK2(C)=P**

RECEIVER

SENDER

Where, K1 ≠ K2

K1=Public key

K2=Private key E=Encryption algorithm D=Decryption algorithm P=Plain text

C=Cipher text

# DIGITAL SIGNATURE:-

* **A digital signature is an asymmetric key cryptography that uses two different keys for both encryption and decryption.**
* **When a person is identified by his/her signature which is verified electronically or digitally, then it is called as digital signature.**

P P

**EK1(P)=C**

N/W

**DK2(C)=P**

RECEIVER

SENDER

Where, K1 ≠ K2

K1=Private key K2=Public key E=Encryption algorithm D=Decryption algorithm P=Plain text

C=Cipher text

* **In digital signature, a key used for encryption is called as private key.**
* **A key used for decryption is called as public key.**
* **It authenticates electronic document or e-signature.**
* **It verifies the originality and authenticity of an e-document digitally.**
* **It uses an algorithm known as DSA (Digital Signature Algorithm).**
* **Digital signature uses a function called as hash function.**
* **This function is used to generate hash value by a process known as hashing. M(P)=H**

Where, M()=Hash function P=Plain text

H=Hash value

* **Hashing uses an algorithm known as SHA (Secured Hash Algorithm), to verify that the message received is the same as message sent.**
* **Using hashing a message is stored in a hash value and kept secret known as MD (Message Digest).**
* **There are several reasons to implement digital signature during important electronic communications. The reasons are:**

### Authenticity:-

* + **Authenticity refers to verification of identity.**
	+ **The sender and receiver must be identified to each other.**

### Integrity:-

* + **Integrity refers to accuracy and validity of information.**
	+ **Once the message is signed, any change in the message would invalidate the signature.**

### Confidentiality:-

* + **Confidentiality refers to secrecy or privacy of information.**
	+ **The information transferred between sender and receiver must be confidential to each other.**

### Non-repudiation:-

* + **Non-repudiation refers to denying of previous commitment.**
	+ **An entity that has signed some information cannot at a later time deny having signed it.**

**Digital Signature Certificate (DSC):-**

# VPN:-

* **A digital certificate is an e-document authenticated by a Certificate Authority (CA).**
* **It is an authenticated electronic document which is as valid as a certificate like e- Aadhaarcard.**
	+ **It stands for Virtual Private Network.**
	+ **A VPN is an organization or a company that uses a public network as its private network.**
	+ **By using this private network, it can transmit data over a VPN or tunnel connection from local site to remote site.**
	+ **The information sent by the local computer can only be seen by the remote computer, with which the VPN tunnel is connected.**
	+ **The process of sending message securely through a tunnel is called as tunneling.**
	+ **Here, the information sent through VPN tunnel is not able to known by any outsider.**



# FIREWALL:-

* + **A firewall is a hardware or a software which is used as a gatekeeper to an intranet and extranet.**
	+ **It is used to provide security to the intranet and extranet network from the unauthorized user or network.**
	+ **It is always wake up.**
	+ **The server of an intranet or extranet is present behind a firewall.**
	+ **When a packet reach to the server the firewall checks and verifies the IP address of the message or packet then allow or disallow into the network (intranet or extranet).**
	+ **A firewall is used as a barrier between internal network and external network.**



# INTRANET:-

* + **An intranet is a fully private network.**
	+ **It can allow only to individual person or user to access network, who are connected with that particular network.**
	+ **The server of an intranet is protected by a firewall.**
	+ **A firewall is a hardware or software that acts as a gatekeeper to an intranet.**
	+ **An intranet does not allow any outsider to enter into its network.**
	+ **It is a protected and secured network.**

INTRANE T SERVER

F I R E W A L L

# EXTRANET:-

**Not allowed**

EXTERNAL

* + **An extranet is also an intranet.**
	+ **It is also a privately owned network.**
	+ **It allows individual person or user and permissible outsider into the network, with which network they are connected.**

Extranet = Intranet + Permissible outsider

* + **It is also protected by a firewall that acts a gatekeeper.**

F

I **Allowed**

INTRANE T SERVER

R

E

W A

L Not allowed

L

Authorized user

Unauthorized user

# PROXY SERVER:-

* + **A proxy server is an alternative of main server.**
	+ **It is used in between clients and main server.**
	+ **It protects the main server from direct access of client.**
	+ **A client gives request to the proxy server, then it forwards the request to the main server.**
	+ **The main server processes the client request and gives response to the proxy server.**
	+ **Then the proxy server forwards that response to the requested client.**
	+ **There is one-to-one communication between main server and proxy server.**
	+ **There is one-to-many communication between proxy server and clients.**

Server response

M A I N S E R V E R

Client request

C1

forward response

C3

P R O X Y S E R V E R

C2

Forward request

C4

# CYBER LAW:-

* + **It is a law that governs cyber space.**
	+ **Cyber space includes networks, Software, data storage device, internet, mobile phones, ATM, etc.**
	+ **Cyber law has several rules and regulations to control the cyber crime.**
	+ **Any violation of the rules of cyber law leads to punishment in terms of imprisonment or fine or compensation pay.**
	+ **Cyber law includes copyright law, trademark law, patent law, etc.**
	+ **Indian government passed a law to provide legal recognition to electronic commerce on 17th October 2000, known as cyber law of India Act or IT Act 2000.**
	+ **It was amendment on 2008 by including several sections, known as IT Amendment Act 2008.**
	+ **It includes 13 chapters and several sections like section 43, section 66, etc.**

## Needs of Cyber law:-

There are various reasons which is extremely difficult to handle over cyberspace, that’s why

we need cyber law. Some of the reasons are:-

* + **Cyber space has complete disrespect for jurisdictional boundaries because it spreads to the whole world.**
	+ **It is difficult to handle gigantic volume of traffic in every second due to e-mail, online transaction, data transfer, etc.**
	+ **Cyber space is absolutely open to everyone from child to an old man.**
	+ **Cyber space offers hiding of information within an image or file for confidentiality.**
	+ **It offers economic efficiency for customers.**
	+ **A software source code consisting crores of rupees can be pirated within hour.**
	+ **Chance of hacking of electronic information in banks, ATM,E-commerce, etc.**

## Cyber law encompasses laws relating to:-

* + **Cyber law encompasses laws relating to:-**
1. **Cyber crime**
2. **Electronic and digital signature**
3. **IPR**
4. **Data protection and privacy**

### Cyber crime:-

* + **Cyber crime is defined as the crime committed through internet where computer is used as a tool or a target.**
	+ **Cyber crime committed on cyber space.**
	+ **Due to increase in the use of mobile phones, internet, computers, e-commerce, e- banking, etc. cyber crime is increasing day to day.**
	+ **Cyber crime does not obey or comes under any particular jurisdictional boundary.**
	+ **Example:- hacking, pornography, online fraud, cyber terrorism, software piracy, spamming, etc.**

### Electronic and digital signature:-

* + **Electronic signatures are used to authenticate electronic records.**
	+ **Digital signatures are one type of electronic signature.**
	+ **Digital signatures satisfy three major legal requirements:- signer authentication, message authentication and message integrity.**
	+ **When a person is identified by his/her signature which is verified electronically or digitally, then it is called as digital signature.**

### IPR:-

* + **IPR stands for Intellectual Property Right.**
	+ **IPR gives exclusive rights for a person’s any innovation, discoveries or writing of books.**
	+ **IPR allows the concerned person to distribute or sell of his/her intellectual properties.**
	+ **It includes copyright law, patent law, trademark law, semiconductor law, etc.**

### Data protection and privacy:-

* + **This law aims to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, e-mail service providers, etc.**

# OBJECTIVES OF IT ACT:-

* + **Grant legal recognition to all transactions made through e-commerce.**
	+ **Give legal recognition to digital signature.**
	+ **Give legal recognition to electronic document.**
	+ **Facilitates the electronic storage of data.**

# FEATURES OF IT ACT:-

* + **Some features of IT Act are:-**
1. **Focusing on data privacy**
2. **Focusing on Information Security**
3. **Reduce inclusion of some additional cyber crimes like child pornography and cyber terrorism.**
4. **Legal recognition to digital signature.**
5. **Legal recognition to e-document.**
6. **Legal recognition to all transaction made through internet.**
7. **Facilitates the electronic storage of data.**