Q.1 Attempt any TWO question of the following. [10]

Q.1(a) What is unfair competition? How to protect from it? [5]

(A) Unfair competition is a term applied to all dishonest or fraudulent rivalry in trade and commerce. This term is particularly applied to the practice of endeavoring to substitute one's own goods or products in the market for those of another for the purpose of deceiving the public. Acts of unfair competition are generally characterized by deception, bad faith, fraud or oppression, or as against public policy because of their tendency to unduly hinder competition.

Examples of unfair competition include:

- **Trademark infringement** - such as using the Coca-Cola® trademark on a soda container manufactured by a competing beverage maker.
- **False advertising** - such as making false claims about a drug's abilities to promote weight loss.
- **Unauthorized substitution of one brand of goods for another** – such as substituting a low-cost handbag for a designer handbag.
- **Misappropriation of trade secrets** - such as stealing a competitor's soft drink formula.
- **False representation of products or services** - such as exaggerating a software program's spellcheck capabilities.

Q.1(b) Explain the concept of Intellectual Property Rights. [5]

(A) **Intellectual property (IP)** refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

Intellectual property rights are like any other property right. They allow creators, or owners, of patents, trademarks or copyrighted works to benefit from their own work or investment in a creation. Tools of Intellectual Property rights are:

- **Patent:** A patent is an exclusive right granted for an invention – a product or process that provides a new way of doing something, or that offers a new technical solution to a problem. A patent provides patent owners with protection for their inventions.
- **Trademark:** A trademark is a distinctive sign that identifies certain goods or services produced or provided by an individual or a company. Trademarks may be one or combination of words, letters and numerals. They may consist of drawings, symbols or three dimensional signs such as shape and packaging of goods. In some countries, non-traditional marks may be registered for distinguishing features such as holograms, motion, color and non –visible signs (sound, smell or taste).
- **Copyright:** Copyright laws grant authors, artists and other creators protection for their literary and artistic creations, generally referred to as "works". Copyright covers literary works (such as novels, poems and plays), films, music, artistic works (e.g., drawings, paintings, photographs and sculptures) and architectural design.
- **Geographical Indication:** A geographical indication is a sign used on goods that have a specific geographical origin and possess qualities or a reputation due to that place of origin. Most commonly, a geographical indication consists of the name of the place of origin of the goods.
- **Industrial Design:** An industrial design refers to the ornamental or aesthetic aspects of an article. A design may consist of three-dimensional features, such as the shape or surface of an article, or two-dimensional features, such as patterns, lines or color.

Q.1(c) What is a copyright? What are its characteristics? [5]

(A) Copyright laws grant authors, artists and other creators protection for their literary and artistic creations, generally referred to as "works". A closely associated field is "related rights" or rights related to copyright that encompass rights similar or identical to those of copyright, although sometimes more limited and of shorter duration.

Works covered by copyright include, but are not limited to: novels, poems, plays, reference works, newspapers, advertisements, computer programs, databases, films, musical compositions, choreography, paintings, drawings, photographs, sculpture, architecture, maps and technical drawings.

The creators of works protected by copyright, and their heirs and successors (generally referred to as "right holders"), have certain basic rights under copyright law. They hold the exclusive right to use or authorize others to use the work on agreed terms. The right holder(s) of a work can authorize or prohibit: its reproduction in all forms, including print form and sound recording; its public performance and communication to the public; its broadcasting; its translation into other languages; and its adaptation, such as from a novel to a screenplay for a film. Similar rights of, among others, fixation (recording) and reproduction are granted under related rights. Many types of works protected under the laws of copyright and related rights require mass distribution, communication and financial investment for their successful dissemination (for example, publications, sound recordings and films). Hence, creators often transfer these rights to companies better able to develop and market the works, in return for compensation in the form of payments and/or royalties (compensation based on a percentage of revenues generated by the work).

Q.1(d) What is trademark? What are its functions? [5]

(A) Trademark

A trademark is a distinctive sign that identifies certain goods or services produced or provided by an individual or a company.

Trademarks may be one or combination of words, letters and numerals. They may consist of drawings, symbols or three dimensional signs such as shape and packaging of goods. In some countries, non-traditional marks may be registered for distinguishing features such as holograms, motion, color and non–visible signs (sound, smell or taste)

The Functions of a trade mark :

A trade mark serves the purpose of identifying the source of origin of goods. Trade mark performs the following four functions:

1. It identifies the product and its origin. For example, the trade mark 'Booke Bond' identifies tea originating from the Company manufacturing tea and marketing it under that mark.
2. It guarantees its quality. The quality of tea sold in the packs marked Brooke Bond Tea would be similar but different from tea labelled with mark Taj Mahal.
3. It advertise the product. The trade mark represents the product. The trade mark 'Sony' is associated with electronic items. The trade mark SONY rings bell of particular quality of particular class of goods. It thus advertise the product while distinguishing it from products of Sony's competitors.
4. It creates an image of the product in the minds of the public, particularly consumers or the prospective consumers of such goods. The mark 'M' which stands for the food items originating from the American fast food chain McDonalds creates an image and reputation for food items offered by it for sale in the market.

Q.2 Attempt any TWO question of the following. [10]

Q.2(a) Discuss Semiconductor Chip Protection Act. [5]

(A) Semiconductor Chip Protection Act, 1984

Prior to 1984, it was not necessarily illegal to produce a competing chip with an identical layout.

In 1984 the United States enacted the Semiconductor Chip Protection Act of 1984 (the SCPA) to protect the topography of semiconductor chips.

The Act extended legal protection to a new form of subject matter — semiconductor chip mask works — in order to address the problem of chip piracy.

The SCPA uses a modified copyright approach to protect the topography of integrated circuits against copying. Chip protection is acquired under the SCPA by filing with the U.S. Copyright Office an application for "mask work" registration under the SCPA, together with a filing fee. The application must be accompanied by identifying material, such as pictorial representations of the IC layers—so that, in the event of infringement litigation, it can be determined what the registration covers.

Protection continues for ten years from the date of registration.
The bundle of rights is also somewhat different from that granted under copyright law, and copies of the "mask work" made in the course of reverse engineering are not infringing, in spite of proof of unauthorized copying and striking similarity, so long as the resulting semiconductor chip product was the result of study and analysis and contained technological improvement.

Q.2(b) List out seven US safe labour principles. [5]

(A) US-EU Safe Harbor is a streamlined process for US companies to comply with the EU Directive 95/46/EC on the protection of personal data.

Intended for organizations within the EU or US that store customer data, the **Safe Harbor Principles** are designed to prevent accidental information disclosure or loss. US companies can opt into the program as long as they adhere to the 7 principles outlined in the Directive.
The process was developed by the US Department of Commerce in consultation with the EU.

Principles

These principles must provide:

- **Notice -** Individuals must be informed that their data is being collected and about how it will be used.
- **Choice -** Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer -** Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security -** Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity -** Data must be relevant and reliable for the purpose it was collected for.
- **Access -** Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- **Enforcement -** There must be effective means of enforcing these rules.

Q.2(c) Explain computer software as Intellectual Property and its protection. [5]

(A) "Computer software" also referred to as computer programs are the instructions executed by a computer. In other words, the explanations, instructions, commands and systems which have been developed in order to run the machine are called computer software. Software comprises of the following one or more components: the source code itself which contains the programmer's invaluable comments any literature that may be supplied with the package which could be in the form of manuals or explanatory material regarding the running of the programme. All these components require protection because the making of it involves the expenditure of skill, time and labour and therefore the resultant work should be protected from misappropriation.

Software has a market value. Computer software is subject to ferocious competition with a shorter life circle and is liable to be copied soon, as it is "read all on the face" technology.

Because of its nature the owner of computer program will have two problems (i) economic problem and (ii) competition. Economic problem means, others can access it without payment to the creator. Competition means the competitors will make competing products based on the creation either by reserve engineering or blatant copying.

Apart from protecting the economic interest of the owner the protection of software through appropriate IPR mechanism is considered necessary to encourage creativity, innovation and investment. As already mentioned software may be reproduced at no cost, some means of restricting the free copying and redistribution of software work is necessary to preserve an investment in a software product.

There is a divergence in views among various jurisdictions of the world as to what category of intellectual property may that is to be granted to protect computer software. Presently there are two principal modes of protection of software, copyright and patents. Copyright is most commonly used to protect computer program, because writing of a code is similar to any type of literary work. The copyright protection is extended to expression of ideas.

To establish intellectual property protection to computer software domestically and internationally the signatories of TRIPS Agreement, Berne convention, and WIPO Copyright Treaty (WCT) have agreed to protect copyright in a computer program until, at a minimum 50 years after the author (software writer) of the program dies.

For citizens of more than 162 members of Berne convention countries, once protection is grated to a work in one member country that work is automatically protected with in the borders of all other signatory countries.

However, It is the discretion of the states to given protection for computer program under copyright or patent laws.

Q.2(d) Write short note on TRIPS. **[5]**

(A) TRIPS

The Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) is an international agreement administered by the World Trade Organization (WTO) that sets down minimum standards for many forms of intellectual property (IP) regulation as applied to nationals of other WTO Members. It was negotiated at the end of the Uruguay Round of the General Agreement on Tariffs and Trade (GATT) in 1994.

The TRIPS agreement introduced intellectual property law into the international trading system for the first time and remains the most comprehensive international agreement on intellectual property to date. In 2001, developing countries, concerned that developed countries were insisting on an overly narrow reading of TRIPS, initiated a round of talks that resulted in the Doha Declaration. The Doha declaration is a WTO statement that clarifies the scope of TRIPS, stating for example that TRIPS can and should be interpreted in light of the goal "to promote access to medicines for all." Specifically, TRIPS requires WTO members to provide copyright rights, covering content producers including performers, producers of sound recordings and broadcasting organizations; geographical indications, including appellations of origin; industrial designs; integrated circuit layout-designs; patents; new plant varieties; trademarks; trade dress; and undisclosed or confidential information. TRIPS also specifies enforcement procedures, remedies, and dispute resolution procedures. Protection and enforcement of all intellectual property rights shall meet the objectives to contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.

Q.3 Attempt any TWO question of the following : **[10]**

Q.3(a) What are the rights awarded to Patentee? **[5]**

(A) Rights of Patentee

The right to exploit the patent : Section 48 confers the right to exploit the patent on the patent on the patentee or his licensee or his assignee or his agent when such a right is exercised within the condition imposed by section 47 of the Act.

Right to licence : Section 70 of the Act confers, inter.alia, the right on a grantee or proprietor of a patent to grant licence(s). for instance, a patentee of invention of new sound system has a right to license his right to another party to make and sell the system in a particular territory.

Right to assign : Section 70 also confers on the patentee the right to fully or partially assign his patent to another or others.

Such assignment and licensing should always be in writing in express agreements. Such agreement should be registered to avoid litigation later.

The right to surrender the patent : A patentee is not under an obligation to maintain his monopoly right on the patent for the entire term of the patent. He may surrender the patent any time.

Section 63 provides that a patentee may, at any time by giving notice to the Controller, offer to surrender his patent. The Controller, before accepting the offer of surrender, publishes the offer in India to give opportunity to the parties having any interest, for instance licensees, to oppose the offer of surrender.

Right to sue for infringement : The exclusive right conferred by a patent can be meaningful and lasting only when the statute confers a right on the patentee to take legal action for protection of his patent rights. Patentee, his assignee, licensee or agent has the right to institute a civil suit in a court not lower than the District Court in case of any infringement.

Q.3(b) Write a note on assignment of copyright. [5]

(A) Assignment of Copyright

Sections 18, 19 and 19A of the Copyright Act deal with the assignment of copyright. Assignment of copyright may be for the whole of the rights or for part of the rights only.
Assignment of copyrights may be general, i.e., without any limitation being placed on the assigned may be subject to certain limitations.

Assignment may be for the full term of the copyright or for a limited period of time.
Assignment may be on a territorial basis, i.e., for a particular territory or country.
An owner of a copyright can assign his right in the above combination of forms.
Illustration – An author assigns the right to serialise the work into a telelvision serial to a producer for a period of 20 years provided the serial is broadcast only within the territory of India. Here the author makes a limited assignment for a limited period of time placing territorial restrictions at the same time.

Mode of assignment

Section 19 elaborates the mode of assignment in the following manners:

1. Assignment is valid only when it is in writing signed by the assignor or by his duly authorized agent.
2. The assignment instrument shall identify the work and specify the rights assigned and the duration and territorial extent of such assignment.
3. The instrument of assignment of copyright shall also specify the amount of royalty payable, if any, to the author or his legal heirs during the subsistence of the assignment and the assignment shall be subject to revision, extension or termination on terms mutually agreed upon by the parties.
4. If the assignee does not exercise the rights assigned to him within one year from the date of assignment, the assignment in respect of such rights shall be deemed to have lapsed after the expiry of the said period unless otherwise specified in the assignment instrument.
5. When the period of assignment is not stated, the period shall be deemed to be five years from the data of assignment.
6. If the territorial extent of any assignment of the rights is not specified, it shall be presumed to extend within India.
7. When the assignment has been made before the coming into force of the Copyright (Amendment) Act, 1994, the above provisions of the above sub sections (2), (3), (4), (5), (6) shall not be applicable. However, even such an assignment has to be through a written instrument.

Q.3(c) What are the rights conferred by registration of Industrial Design? [5]

(A) Rights granted and the term of such rights

The exclusive right conferred on a design is termed as 'copyright in design' This should not be confused with exclusive right granted for literary and artistic work also termed a 'copyright' in the literary and artistic work. There may be certain designs which can qualify for registration both under the Designs Act and the Copyright Act. The industrial design and product design are covered by the Designs Act, 2000, if a design has been registered under this Act, it cannot be protected by the Copyright Act even though it may be an original artistic work.

If a design qualifies for registration under the Designs Act but has not been so registered under the Designs Act, the exclusive right will subsist under the Copyright Act. If such a design is of an article which is commercially produced, the copyright over the design under the Copyright Act will cease to exist when the article to which the design has been applied has been reproduced more than fifty times by an industrial process by the owner of the copyright.

There is an overlapping area of the applicability of the Designs Act and the Copyright Act but they cannot be applied co-terminously (at the same time) for protection of the same subject-matter.

Rights granted when a design is register

(i) The right to exclusive use of the design:

(1) When a design is registered, the registered proprietor of the design shall, subject to the provisions of the Act of 2000, have the copyright in the design during ten years from the date of registration.

(2) If, before the expiration of the said ten years applications for the extension of the period of copyright is made to the Controller in the prescribed manner, the Controller shall, on payment of the prescribed fee, extend the period of copyright for a second period of five years from the expiration of the original period of ten years.

(ii) Right to protect the design from piracy:

Infringement of a copyright in a design is termed as Piracy of Design. Any person responsible for infringing the monopoly of the proprietor of a registered design is guilty of piracy and is liable to a fine of a sum not exceeding twenty five thousand rupees. The registered proprietor is also granted the right to bring a suit for recovery of damages or for injunction against the reputation of such piracy provided that the total sum recoverable in respect of any one design shall not exceed fifty thousand rupees. The above right is laid down in section 22(2) of the Designs Act, 2000.

Q.3(d) What are the defences set up by defendant in case of infringement of trade mark? [5]

(A) The defences which may be set up by the defendant

The defendant may set up any of the following defences in an action for infringement against him depending upon the applicability of the relevant defence to his case:

(1) That the plaintiff in the suit has no title to sue-Questioning the proprietorship of the trade mark owner may do this.

(2) That the use of the mark by the defendant is not an infringement or is protected by the provisions of section 30 which lists out the acts the acts which do not constitute infringement.

(3) That the defendant's right to use the contested mark arises by virtue of concurrent registration.

(4) That the defendant is the prior-user of the disputed mark.

(5) That the defendant has been an honest concurrent user.

(6) That the use complained of is merely the defendant's bona fide use of his own name, address and description of goods which are protected by the Act.

(7) That the exclusive rights claimed by the plaintiff over the disputed trade mark have ceased to exist by virtue of the word claimed by the plaintiff becoming a common word, i.e. 'Publici Juris'. The words that are within the public domain cannot be claimed as exclusive proprietorship.

(8) That the defendant can attack the validity of registration of the plaintiff.

(9) That the plaintiff is debarred from suing or claiming the relief sought by his own conduct, e.g., by his own acquiescence, delay or latches or his having acquired his rights on the trade mark fraudulently.

Illustration

In the case of Electrolux v. Electrix, (1953) 70 RPC 127, it was held that the mark of the plaintiff was infringed but the relief was suspended in view of the long concurrent use to enable the defendants to apply for registration.

Defences which cannot be set up

(1) Honest adoption of the mark is not a defence. The defendant cannot plead that he had adopted the plaintiff's mark without the knowledge of existence of plaintiff's trade mark.
(2) Innocent infringement cannot be pleaded.

Q.4 Attempt any TWO question of the following : [10]

Q.4(a) What are general obligations for enforcement of Intellectual property rights? Explain. [5]

(A) Enforcement of Intellectual Property Rights

General obligations

1. Members shall ensure that enforcement procedures as specified in this Part are available under their law so as to permit effective action against any act of infringement of intellectual property rights covered by this Agreement; including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements. These procedures shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.
2. Procedures concerning the enforcement of intellectual property rights shall be fair and equitable. They shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.
3. Decisions on the merits of a case shall preferably be in writing and reasoned. They shall be made available at least to the parties to the proceeding without undue delay. Decisions on the merits of a case shall be based only on evidence in respect of which parties were offered the opportunity to be heard.
4. Parties to a proceeding shall have an opportunity for review by a judicial authority of final administrative decisions and, subject to jurisdictional provisions in a Member's law concerning the importance of a case, of at least the legal aspects of initial judicial decisions on the merits of a case. However, there shall be no obligation to provide an opportunity for review of acquittals in criminal cases.
5. It is understood that this Part does not create any obligation to put in place a judicial system for the enforcement of intellectual property rights distinct from that for the enforcement of law in general, nor does it affect the capacity of Members to enforce their law in general. Nothing in this Part creates any obligation with respect to the distribution of resources as between enforcement of intellectual property rights and the enforcement of law in general.

Q.4(b) Write a short note on Technology licensing. [5]

(A) Technology Licensing

By a technology licensing agreement the licensor authorizes the licensee to use the technology under certain agreed terms and conditions. It is, therefore, a contract freely entered into between two parties and contains terms and conditions so agreed.

Through Technology Licensing agreement, it is possible to

- Improving the quality of your product or manufacturing a new product by using the rights owned by others in the form of parent, utility model, or know-how protected by a trade secret, then acquiring such rights through a technology licensing agreement may be the right solution, or
- Entering a market or extending your existing market for a product for which your SME owns the rights to a patent, utility model or know-how protected by a trade secret, then authorizing another to use your process or product through a technology licensing agreement may be the right solution.

Q.4(c) Discuss civil remedies in enforcing intellectual property rights. [5]

(A) Injunction

An injunction is an order of a court prohibiting someone from doing some specified act or commanding someone to undo some wrong or injury. Generally it is a preventive and protective remedy aimed at preventing future wrongs. Injunctions are of two kinds:

Temporary / interlocutory injunctions

These are the Court orders which are in force for a specified time or until further orders of the Court.

An interlocutory injunction may be granted at any time during the proceedings of the suit.

Final injunction

Such injunction is granted at the termination of the trial. The time for which the final injunction is in force is the remaining term of the patent at the time of grant of the final injunction.

Damages

The damages are awarded to compensate for the loss or injury suffered by the plaintiff due to the action of the defendant.

The amount of damages awarded is proportionate to the injury suffered by the part and shall be such sum of money which will put the injured party in the same position as he would have been in, if he had not encountered the wrong.

Account of Profits

Section 108 provides that the Court may either award damages or account of profits but both of them cannot be claimed together. The plaintiff has to prefer either of the two.

The account of profits are determined on the basis of actual use of the patentee's invention by the infringers during the period of commission of the act of infringement. Account of profits is the part of profits which can be attributed to the use of the patentee's invention by the infringer.

Q.4(d) What are the advantages of IP licensing to licensor? [5]

(A) Advantages of Licensing for the Licensor

Many companies have a portfolio of patents, utility models, proprietary know-how, trademarks, and other IP assets that can be licensed. There are many reasons for a company to license out some or all of its IP rights in some or all of its IP assets in such a portfolio.

- A company that owns rights in a patent, know-how, or other IP assets, but cannot or does not want to be involved in the manufacturing of products, could benefit from licensing out of such IP assets by relying on the better manufacturing capacity, wider distribution outlets, greater local knowledge and management expertise of another company (the licensee).
- Licensing out could also help a company to commercialize its IP or expand its current operations into new markets more effectively and with greater ease than on its own. If the licensor's trademark is also licensed for use in the market along with other IP, then the licensee's marketing efforts essentially benefit the licensor's reputation and goodwill. In fact, a trademark license agreement is the heart of any merchandising program, because it delineates the relationship between the owner of a trademark (the licensor) and the producer of the goods or services to which the mark is to be affixed (the licensee). While the licensor is not involved in the manufacturing of the products, he must ensure that the licensee conforms to all conditions concerning maintenance of the quality of the product in relation to which the licensed trademark is used.
- Similarly, licensors with experience in the field of research and product development may find it more efficient to license out new products rather than take up production themselves. A company that owns IP rights in a technology that it cannot afford to manufacture could consider licensing out the IP rights over that technology for manufacturing and selling products embodying the technology in a specific manner for a specific time and region. Thus, the licensor continues to have the IP rights over the technology and has only given a defined right to the

use of that technology. An example of such a business model is a "fables semiconductor" company, where the company uses all its resources essentially for doing research, design and development work.

- Licensing out may be used to gain access to new markets, which are otherwise inaccessible. By granting the licensee the right to market and distribute the product, the licensor can penetrate markets it could not otherwise hope to serve.
  The licensee may agree to make all the adaptations required for entering a foreign market, such as translation of labels and instructions; modification of goods so as to conform with local laws and regulations; and adjustments in marketing.
  Normally, the licensee will be fully responsible for local manufacture, localization, logistics and distribution.

Q.5 Attempt any TWO question of the following : [10]

Q.5(a) What are the different roles of Certifying Authorities? Explain. [5]

(A) The Role and Function of Certifying Authorities

- Certificate Authority (CA) is a trusted entity that issues Digital Certificates and public-private key pairs. The role of the Certificate Authority (CA) is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.
- The Certificate Authority (CA) verifies that the owner of the certificate is who he says he is. A Certificate Authority (CA) can be a trusted third party which is responsible for physically verifying the legitimacy of the identity of an individual or organization before issuing a digital certificate.
- A Certificate Authority (CA) can be an external (public) Certificate Authority (CA) like verisign, thawte or comodo, or an internal (private) Certificate Authority (CA) configured inside our network.
- Certificate Authority (CA) is a critical security service in a network. A Certificate Authority (CA) performs the following functions.
- Certificate Authority (CA) Verifies the identity: The Certificate Authority (CA) must validate the identity of the entity who requested a digital certificate before issuing it.
- Certificate Authority (CA) issues digital certificates: Once the validation process is over, the Certificate Authority (CA) issues the digital certificate to the entity who requsted it. Digital certificates can be used for encryption (Example: Encrypting web traffic), code signing, authentication etc.
- Certificate Authority (CA) maintains Certificate Revocation List (CRL): The Certificate Authority (CA) maintains Certificate Revocation List (CRL). A certificate revocation list (CRL) is a list of digital certificates which are no longer valid and have been revoked and therefore should not be relied by anyone.

Q.5(b) What is cybercrime? Brief different cybercrimes. [5]

(A) Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.

Examples of Cybercrimes

- **Harassment via E-Mails :** It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.
- **Cyber-Stalking :** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Hacking :** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.

- **Cracking :** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing :** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **Cyber Squatting :** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.

Q.5(c) Explain the term Privacy. What are the privacy issues for data and software? [5]

(A) Amongst the personal rights which a Citizen in a Democracy enjoys, "Right to Privacy" and "Right to Freedom of Speech" are the very important. These rights are the foundation of democracy.
In the context of the Cyber Space, the civilized world expects that a similar right is available for the Netizens also.

Apart from the individual's sensitivity for some of his personal information, Privacy is also important to prevent unscrupulous persons from using the information to commit frauds or other crimes.

Privacy Issues

- **CYBER STALKING:** The Internet Technology provides an easy technical means of following an individual when he surfs different web sites. This tracking can provide very useful information to any intelligent marketing agency to understand the potential buyer's preferences. This could help them provide customized services to the buyer during his subsequent visits. Obviously, such personalization actually helps the buyer in his process of decision making and he may not therefore mind the tracking of their buying habits.

  But some consider this stalking an annoying intrusion of their privacy. For example, a person who is browsing through pornographic sites may not want to be embarrassed with a mail that sends a special offer in a related field. Similarly, an employee browsing through job sites may find it embarrassing if he knows that some body is watching his movements.

- **COOKIES:** Placing "Cookies" is a popular means by which website owners gather information about Netizens. Basically, Cookie is a "tag" which identifies the Computer from which a site is accessed. It doesn't alter any other functioning of the computer and is passive "Identifier Tag". The server hosting the web site keeps the data of how many times the site was accessed from the computer which had the cookie and what were the activities of the browser at the site during the session.

- **PRIVACY INVASION BY THE GOVERNMENT:** Apart from the issue of marketing agencies collecting consumer information for commercial exploitation, the other important issue in Privacy is the right of the Government in collecting information about its Citizens. Even in the Real world, Governments are the largest repositories of personal information.

- **PRIVACY INVASION BY THE EMPLOYER:** Another area of frequent dispute is the privacy of an employee as against his employers when he receives e-mails or surfs the web using his office computer. While the employer feels that since the employee is using the office resources, everything that is within it, should also be within his right to see and monitor.

Q.5(d) Discuss privacy issues for data and software. [5]

(A) Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.

1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.
3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
4. Cyberspace is absolutely open to participation by all. A tenyear- old in Bhutan can have a live chat session with an eightyear- old in Bali without any regard for the distance or the anonymity between them.
5. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.
6. Cyberspace offers never-seen-before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.
7. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.
8. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.
9. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the "original" information, so to say, remains in the "possession" of the "owner" and yet information gets stolen.

Q.6 Attempt any TWO question of the following : [10]

Q.6(a) What are the duties of the subscriber of Digital Signature certificate? [5]

(A) Duties of subscribers

Generating key pair

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate :
   (a) to one or more persons:
   (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that:
   (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
   (b) all representation made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true:
   (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.
Explanation: For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Q.6(b) What is Cyber Appellate Tribunal? What are its powers? [5]

(A) Cyber Appellate Tribunal has been established under the Information Technology Act under the aegis of Controller of Certifying Authorities (C.C.A.). The first and the only Cyber Appellate Tribunal in the country has been established by the Central Government in accordance with the provisions contained under Section 48(1) of the Information Technology Act, 2000.

The first Cyber Appellate Tribunal has been established by the central government under the Information Technology Act, 2000. The motive of Cyber Appellate Tribunal is to stop the cyber crimes and frauds over a period of time. These tribunal discharge their power as the same as Supreme Court under the code of civil procedure, 1908. The duties of Cyber Appellate Tribunal are discharged by one person, who is known as Presiding Officer. He acts and discharges his duties as Supreme Court judge.

Procedure and powers of the Cyber Appellate Tribunal

1. The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
2. The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:
   a. summoning and enforcing the attendance of any person and examining him on oath;
   b. requiring the discovery and production of documents or other electronic records;
   c. receiving evidence on affidavits;
   d. issuing commissions for the examination of witnesses or documents;
   e. reviewing its decisions;
   f. dismissing an application for default or deciding it ex parte;
   g. any other matter which may be prescribed.
3. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of section 193 and 228, and for the purposes of section 196 of the Indian Penal Code(45 of 1860) and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

Q.6(c) What does chapter 5 of IT act, 2000, "Secure Electronic records and secure digital signatures" specify? [5]

(A) Secure Electronic records and Secure Digital Signatures

Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time. then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Secure digital signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was
(a) unique to the subscriber affixing it.
(b) capable of identifying such subscriber.

(c) Created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

Security procedure.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including:

(a) the nature of the transaction:
(b) The level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;
(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications.

Q.6(d) What are the objectives of IT Act, 2000? [5]

(A) The following are its main objectives and scope:

1. It is objective of I.T. Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.
2. To give legal recognition to digital signature for accepting any agreement via computer.
3. To provide facility of filling document online relating to school admission or registration is employment exchange.
4. According to I.T. Act 2000, any company can store their data in electronic storage.
5. To stop computer crime and protect privacy of internet users.
6. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
7. To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

Q.7 Attempt any THREE question of the following : [15]

Q.7(a) Write short note on protection of Industrial Design.

(A) An industrial design refers to the ornamental or aesthetic aspects of an article. A design may consist of three-dimensional features, such as the shape or surface of an article, or two-dimensional features, such as patterns, lines or color.

Need for protection of industrial designs

Industrial designs are what make an article attractive and appealing; hence, they add to the commercial value of a product and increase its marketability. When an industrial design is protected, the owner – the person or entity that has registered the design – is assured an exclusive right and protection against unauthorized copying or imitation of the design by third parties.

This helps to ensure a fair return on investment. An effective system of protection also benefits consumers and the public at large, by promoting fair competition and honest trade practices, encouraging creativity and promoting more aesthetically pleasing products.

Protecting industrial designs helps to promote economic development by encouraging creativity in the industrial and manufacturing sectors, as well as in traditional arts and crafts. Designs contribute to the expansion of commercial activity and the export of national products.

Industrial designs can be relatively simple and inexpensive to develop and protect. They are reasonably accessible to small and medium-sized enterprises as well as to individual artists and craftsmakers, in both developed and developing countries.

Procedure for Protection of industrial designs

In most countries, an industrial design must be registered in order to be protected under industrial design law. As a rule, to be registrable, the design must be "new" or "original". Countries have varying definitions of such terms, as well as variations in the registration process itself.
Generally, "new" means that no identical or very similar design is known to have previously existed.
Once a design is registered, a registration certificate is issued.

Following that, the term of protection granted is generally five years, with the possibility of further renewal, in most cases for a period of up to 15 years.
Hardly any other subject matter within the realm of intellectual property is as difficult to categorize as industrial designs. And this has significant implications for the means and terms of its protection.

Depending on the particular national law and the kind of design, an industrial design may also be protected as a work of applied art under copyright law, with a much longer term of protection than the standard 10 or 15 years under registered design law. In some countries, industrial design and copyright protection can exist concurrently. In other countries, they are mutually exclusive: once owners choose one kind of protection, they can no longer invoke the other.

Q.7(b) What are Domain Name Disputes? [5]

(A) The disputes that arise over domain names are based on the second level domain name because they are what people remember most of all in a domain name address.

Cybersquatting: Cybersquatting is the practice of registering an Internet domain name that is likely to be wanted by another person, business, or organization in the hope that it can be sold to them for a profit. It involves the registration of trademarks and trade names as domain names by third parties, who do not possess rights in such names. Simply put, Cybersquatters (or bad faith imitators) register trade-marks, trade names, business names and so on, belonging to third parties with the common motive of trading on the reputation and goodwill of such third parties by either confusing customers or potential customers, and at times, to even sell the domain name to the rightful owner at a profit.

Example: In Satyam Infoway Ltd. v Sifynet Solutions 2004 (6) SCC 145, the Respondent had registered domain names www.siffynet.com and www.siffynet.net which were similar to the Plaintiff's domain name www.sifynet.com. Satyam (Plaintiff) had an image in the market and had registered the name Sifynet and various other names with ICANN and WIPO. The word Sify was first coined by the plaintiff using elements from its corporate name Satyam Infoway and had a very wide reputation and goodwill in the market. The Supreme Court held that "domain names are business identifiers, serving to identify and distinguish the business itself or its goods and services and to specify its corresponding online location." The court also observed that domain name has all the characteristics of a trademark and an action of Passing off can be found where domain names are involved. The decision was in favour of the plaintiff.

Q.7(c) What are essential factors for infringement of Trademark? [5]

(A)
1. The taking of any essential feature of the mark or taking the whole of the mark and then making a few additions and alterations would conaltute infringement.
2. The infringing mark must be used in the course of trade, i.e. in a regular trade wherein the proprietor of the mark is engaged.
3. The use of the infringing mark must be printed r usual representation of the mark in advertisements, invoices or bills. Any oral use of the trade mark is not infringement.
4. Any or all of the above acts would constitute infringement if the same is done in such manner as to sender the use of the mark likely to be taken as being used as a trade mark.

Q.7(d) Write a short note on "border security measures". [5]

(A) Border Security Measures

The recognition of the need to protect of intellectual property especially with regard to counterfeit trademark and pirated copyrighted goods, the enforcement of intellectual property rights at the borders has emerged as a significant issue in recent times.

Border Measures under TRIPS

India is a signatory to the WTO Treaty on Trade Related Aspects of Intellectual Property Rights (TRIPS), which was brought into force on 1st January, 1995. Articles 51 to 60 of TRIPS Agreement [Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization] relate to border measures (i.e. measures required to be taken for providing protection against infringement of IPRs at the border).

Under Articles 51 to 60 of the TRIPS Agreement, a WTO member country is obliged to enact laws to fulfill obligations relating to border measures by incorporating the following provisions, so far as enforcement of IPRs at Border is concerned:

- **Suspension of Release:** A provision, which allows a right holder to lodge an application with Customs to suspend release of suspected counterfeit goods.
- **Application:** Describes the conditions for making an application, Prima facie evidence of infringement and a sufficiently detailed description of the goods.
- **Security or Equivalent Assurance:** Security to prevent abuse of the system by person making the allegation of infringement.
- **Notice of Suspension:** Prompt notification by Customs to the rights holder of suspension.
- **Duration of Suspension:** 10 working days after the applicant has been served notice of the suspension; time period for Right Holder to commence legal proceedings.
- **Indemnification of the Importer and of the Owner of the Goods:** The applicant is liable to pay compensation to the importer, the consignee and owner, compensation in case of wrongful detention of goods.
- **Right of Inspection and Information:** The right holder is given sufficient information and the right to inspect detained goods, in order to substantiate the claim.
- **Ex Officio Action:** Optional provision, which allows Customs to act upon their own initiative, without an application being required, in order to suspend clearance of goods. {Ex Officio may have two distinct meanings: (1). Customs intercepting a shipment on their own information, after the right holder has already completed the recordal of their IPR. (2). Customs intercepting a shipment on their own information, even if the right holder has not completed recordal.
- **Remedies:** Order destruction of infringing goods. Re-exportation not allowed.
- **De Minimus Imports:** Small non-commercial consignments may be excluded.

While the mandatory obligations under Articles 51 to 60 of the TRIPS agreement dealing with border measures are restricted to Copyright and Trade Marks infringement only, the IPR (imported goods) enforcement Rules,2007 deal with Patents, Designs and Geographical Indications violations as well, in conformity with the practice prevailing in some other countries, notably EU countries.

Q.7(e) Explain the need of digital signature. [5]

(A) A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a nonsecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Q.7(f) What is CERT (Computer Emergency Response Team)? What are its functions? [5]

(A) Computer emergency response teams (CERT)

Computer emergency response teams (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT).

CERT–In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology Amendment Act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

❑ ❑ ❑ ❑ ❑