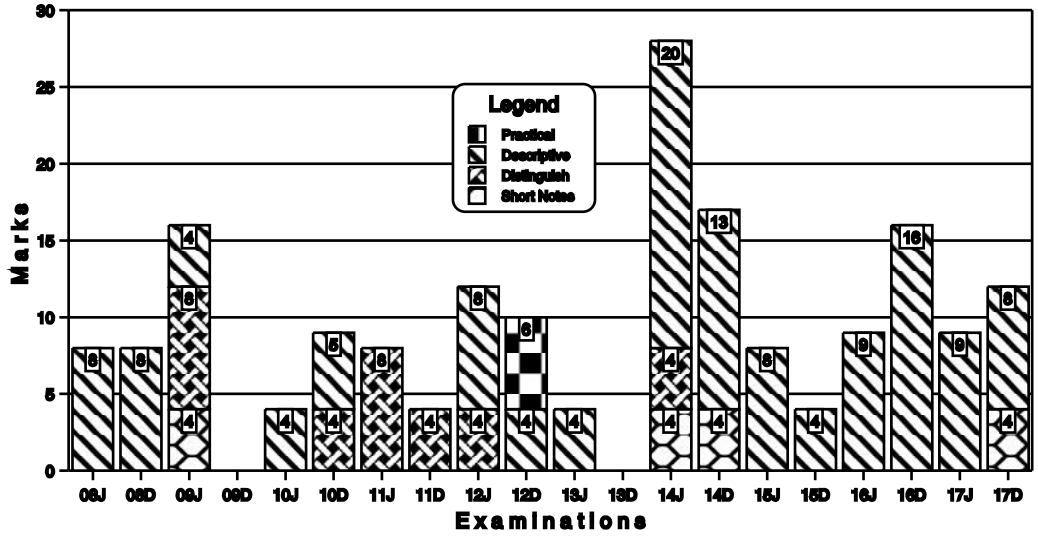
1 *INFORMATION TECHNOLOGY LAW*

THIS CHAPTER INCLUDES

- Information Technology Act– Definitions
- Important terms under Information Technology Legislation
- Digital Signatures
- Electronic Records
- Certifying Authority
- Electronic Signature Certificate
- Cyber Appellate Tribunal
- Offences and Penalties

Marks of Short Notes, Distinguish Between, Descriptive & Practical Questions



CHAPTER AT A GLANCE

Topic	Important Highlights
Objectives of IT Act	1. To give legal recognition to any transaction which is done electronically 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 in employment exchange. 4. To stop computer crime and protect privacy of internet users. 5. To give legal recognition for keeping books of accounts by bankers and other companies in electronic form. 6. To make more powerful to IPC (Indian Penal Code), RBI and Indian Evidence act for restricting electronic crime.
Non Applicability of the Act	**IT Act 2000** does not apply to: (a) A negotiable instrument as defined in **Section 13 of the Negotiable Instruments Act, 1881;** (b) A power-of-attorney as defined in **Section 1A of the Powers-of-Attorney Act, 1882;** (c) A trust as defined in **Section 3 of the Indian Trusts Act, 1882;** (d) A will as defined in Clause (h) of **Section 2 of the Indian Succession Act, 1925** including any other testamentary disposition by whatever name called;

	(e) Any contract for the sale or conveyance of immovable property or any interest in such property; (f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.
Digital Signature	● As per **Section 2(1) (p)** of information technology Act "Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of **Section 3;** ● A digital signature is issued by a Certification Authority (CA) and is signed with the CA's private key. ● A digital signature/electronic signature typically contains the: Owner's public key, the Owner's name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer. Digital signatures deploy the Public Key Infrastructure (PKI) technology.
Electronic Signature	Notwithstanding anything contained in **Section 3,** but subject to the provisions of **sub-section (2),** a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable; and may be specified in the Second Schedule.

Electronic Records	As per **Section 2(t) of Information Technology Act, 2000** as amended, "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
Authentication of electronic records	● As per **Section 3 of IT Act, 2000** any subscriber may authenticate an electronic record by affixing his digital signature. ● The authentication of the electronic record are effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.
Retention of Electronic Records	● **Section 7 of the IT Act, 2000** as amended provides for retention of records in electronic format. It provides that where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if: (a) the information contained therein remains accessible so as to be usable for a subsequent reference; (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; (c) the details which will facilitate the

	identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record. ● Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. These provisions will not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.
Time and place of dispatch and receipt of Electronic record	● **Section 13 of IT Act, 2000** as amended provides that unless otherwise agreed between the originator and the addressee, the dispatch of an Electronic record occurs when it enters a computer resource outside the control of the originator & the time of receipt of an Electronic record shall be at the time when the Electronic, record enters the designated computer resource and at the time when the Electronic record is retrieved by the addressee. ● If the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the Electronic record enters the computer resource of the addressee. ● Save as otherwise agreed to between the originator and the addressee, an Electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

Certifying Authority	A Certifying Authority is a trusted body whose central responsibility is to issue, revoke, renew and provide directories of Electronic Certificates. According to **Section 2(g) of Information Technology Act, 2000** as amended "Certifying Authority" means a person who has been granted a licence to issue Electronic Signature Certificates.
Recognition of Foreign Certifying Authorities	● The Controller of Certifying Authority may recognize the foreign certifying authority with the prior approval of the Central Government provided they fulfill the prescribed conditions and restrictions. ● Where any Certifying Authority is recognised, the electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
Electronic Signature Certificates	● Certifying Authority will issue Electronic Signature Certificate on an application by a person in the form prescribed by the Central Government. ● The application should be accompanied by a fee not exceeding ₹ 25,000/- and a certificate practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

Suspension of Digital Signature Certificate	● The provisions relating to Suspension of Digital Signature Certificate are contained in **Section 37 of IT Act, 2000** as amended. ● This provides that the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate: (a) on receipt of a request to that effect from: (i) the subscriber listed in to Digital Signature Certificate; or (ii) any person duly authorised to act on behalf of that subscriber, (b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.
Cyber Appellate Tribunal (CAT)	● Cyber Appellate Tribunal has been established under the Information Technology Act under the aegis of Controller of Certifying Authorities (C.C.A.). ● The **Information Technology Act, 2000** has empowered the Central Government to establish one or more Cyber Regulations Appellate Tribunal. ● The Act requires that a Cyber Appellate Tribunal shall consist of one person only to be referred as the Presiding Officer of the Cyber Appellate Tribunal who is to be appointed, by notification, by the Central Government. ● The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years. ● Subject to certain provisions, any person aggrieved by an order made by controller or an adjudicating officer under this Act may

	prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter. ● Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order.
Computer related offence [Section 66 read with Section 43]	**Section 66 of IT Act, 2000** as amended deals with computer related offences. Computer related offences have been defined in **Section 43 of IT Act, 2000** as amended. **Section 43** of IT Act provides that If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network: (a) accesses or secures access to such computer, computer system or computer network or computer resource; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer

	network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there- under; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or any other computer source code used for a computer resource with an intention to cause damage; If any person, dishonestly, or fraudulently, does any act referred to in **Section 43,** he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to 5 lakh rupees or with both. (**Section 66**)

SHORT NOTES

2009 - June [2] Write short note on the following :

(v) Adjudicating officer. **(4 marks)** ***[CSEM - I]***

Answer :

It is the officer who has a right to look into the case in hand, examine the evidence and the witnesses and to pass an order regarding the matter. An adjudicating officer has the powers of a Civil Court under most Indian acts, for example, under the **Information Technology Act, 2000**.

2014 - June [3A] (Or) Write a note on the following:

(ii) Computer viruses **(4 marks)**

Answer:

Computer Virus	• A computer program designed to carry out unwanted and often damaging operations. • It replicates itself by attaching to a host, which depending on the type of virus, may be a program, macro file or magnetic disc. In common with a human virus, the effects of a computer virus may not be detectable for a period of days or weeks during which time the virus will attempt to spread to other systems by infecting files and discs. • Eventually, the effects manifest themselves when a date or sequence of events triggers the virus.

2014 - Dec [3A] (Or) Write a note on the following:

(i) Powers of Cyber Appellate Tribunal. **(4 marks)**

Answer:

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**, 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 of documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex-parte;
(g) any other matter which may be prescribed.

2017 - Dec [6] Write short note on the following:
(c) Punishment for Cyber Terrorism as per IT Act, 2000. **(4 marks)**

DISTINGUISH BETWEEN

2009 - June [3] Distinguish between the following:
(i) 'Public key' and 'private key'.
(v) 'Computer' and 'computer network'. **(4 marks each)** ***[CSEM - I]***

Answer :

(i)
- 'Asymmetric crypto system', according to the definition of **Section 2(1)(f) of the Information Technology Act, 2000,** means a key pair that provides safety and authenticity to the electronic records being transmitted.
- The key pair consists of a public and a private key, both of which are needed to 'sign' an electronic document digitally.
- As per **Section 2(1) (zc) of the IT Act, 2000,** "Private Key" means the key of a key pair used to create a digital signature; while as per **Section 2 (1)** (zd) "Public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
- Digital signatures, a form of electronic signatures, are created and verified using Public Key Cryptography that is based on the concept of a key pair generated by a mathematical algorithm, the public and private keys.
- The private key, which is used to digitally attach a signature to a document, is securely held by the owner, while the public key is

made known to everyone for verifying the digital signature, together, they form the key pair.

(v) As per **Section 2(1) (i) of the IT Act, 2000**, "Computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network; while, as per **Section 2(1) (j)** "Computer network" means the interconnection of one or more computers through -

(i) The use of satellite, microwave, terrestrial line or other communication media; and

(ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

2010 - Dec [3] Distinguish between the following :

(v) Electronic form' and 'electronic record'. **(4 marks)** ***[CSEM - I]***

Answer :

- As per the Information Technology Act, 2000 electronic form with reference to information, means "any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device." **[Section 2(1)(r)]**
- Electronic record means "data, recorded or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro fiche". **[Section 2(1)(t)]**.

2011 - June [4] (b) Distinguish between the following :

(ii) 'Hacking' and 'passing off'.

(iii) 'Computer network' and 'computer system'.

(4 marks each) ***[CSEM - I]***

Answer :

(ii) Hacking and Passing Off:

Hacking	**Section 66** of the **Information Technology Act, 2000** deals with "hacking" with computer system. The term "hacking" with respect of computer terminology denotes the act of obtaining unauthorized access to a computer system. **Section 68** of the **Information Technology Act, 2000,** provides that: 1. Whoever with intent to cause or knowing that he is likely to cause, wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. 2. Whoever commits hacking, shall be punished with imprisonment upto three years or with fine which may extent upto five lakh rupees or with both. The Section imputes intention as per knowledge to the hacker. Modification of the contents of a computer will also be an offence. Modification includes addition. alteration and erasure. As is evident, the maximum punishment prescribed for hacking with computer system under **Section 66(2)** is imprisonment upto three years or with fine upto five lakh rupees or both.

Passing Off	• The Information Technology Act does not contain a specific provision, declaring illegal any fraudulent use, by one person, of other person's domain name. • However, even in the absence of specific legislation on the subject, such conduct can become actionable under the law of torts. • In fact, judicial decisions, both in India and elsewhere, amply demonstrate the potency of the law of torts in this context. • The tort of "passing off" is wide enough to afford legal redress (in damages) to a person who is the holder of a particular domain name and who suffers harm as a result of the fraudulent use of his domain name by another person. • Such conduct has been regarded as falling under the tort of "passing off". • The crux of the action of "passing off" lies in actual or possible or probable deception. • The principles relating to "passing off" were held to be applicable to domain names in **Rediff** ***Communication Ltd. v. Cyberbooth, (2000) 1 Recent Arbitration Judgements, 562 (Bombay High Court).*** • The domain name “Rediff” (of the plaintiff) and the domain name “Rediff” (of the defendant) were held to be deceptively similar and capable of causing deception, as the fields of business activity of both the parties were similar. • The grant of a temporary injunction, restraining the defendant from using the name in question, was held to be proper.

	• A similar view has been taken in ***Yahoo Inc. v. Akash Arora. (1999) 2 Recent Arbitration Judgements. 176 (Delhi)*.**

(iii) Please refer 2009 - June [3] (v) on page no. 31

2011 - Dec [3] Distinguish between the following:
(v) 'Computer' and 'computer system'.

(4 marks) ***[CSEM - I]***

Answer :

- As per **Section 2(1)(i)** of the **IT Act, 2000**, "Computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.
- As per **Section 2(1) (l)** "Computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

2012 - June [5] Distinguish between the following:
(v) 'Public key' and 'private key'

(4 marks) ***[CSEM - I]***

Answer :

Please refer 2009 - June [3] (i) on page no. 31

2014 - June [2A] (Or) Differentiate the following:
(i) 'Digital signature' and 'digital certificate'. **(4 marks)**

Answer:

Digital signature	• A data block appended to a file or message (or a complete encrypted file or message) such that the recipient can authenticate the file or message contents and/or prove that it could only have originated with the purported sender.
Digital certificate	• In cryptography, a message that guarantees the authenticity of the data contained within it. • In public key cryptography it is important that anyone using a public key can be sure about its authenticity. • Such a guarantee may be issued by a Certification Authority trusted by the users and based on assurances obtained from applicants for digital certificates. • A certificate generally contains the public key owner's identity, the public key itself and its expiry date. • A user supplies the certificate and the recipient decrypts it using the certification authority's public key (often performed automatically by the recipient's browser/e-mail software). • The recipient gains assurance that a trusted authority has signed the user identity and corresponding public key.

DESCRIPTIVE QUESTIONS

2008 - June [3] Explain of the following **:**

(iii) Digital signature. **(4 marks)** ***[CSIG - I]***

Answer :

- Digital signature' is defined in **Section 2(1)(p)**. This definition provides for electronic means of validating of electronic records by the procedure prescribed under the **Information Technology Act, 2000**.
- This is done with the help of a signature in electronic form, which is registered with the Certifying Authority under the Act.
- It is deemed to be secure when it is as per the requirements of **Section 15 of the Information Technology Act, 2000.** They are as under –
  (a) If the signature is unique and controlled by the person affixing it.
  (b) It distinguishes the subscriber, i.e. the person affixing or using it.
  (c) It is so linked with the electronic record to which it is attached that if the record was changed in any way, doing so would nullify the authenticity or veracity of the signature.

2008 - June [4] Attempt the following :

(iii) "The majority of the legal problems arising in the sphere of information technology relate to (a) the machine; (b) the medium; and (c) the message." Illustrate the statement. **(4 marks)** ***[CSIG - I]***

Answer :

- This is a true statement, as a big majority of the offences or rather, almost all of them occur because of the machine, the medium or the message, or even a combination of all these.
- For example, 'hacking' is an offence under the **Information Technology Act, 2000,** under **Section 11.**
- 'Hacking' means causing or attempting to cause loss or damage to anyone by removing or changing any information stored in a computer system or allied resources.
- This is done by unauthorized access of the information.
- The punishment for hacking is imprisonment upto three years, or fine upto rupees five lacs, or both. **(Section 66 of the Information Technology Act, 2000)**.
- For it to take place, the machine, i.e. the computer, if it is not safeguarded by strong passwords and physical checks, can be accessed by anyone.

- The medium might be a problem in case of non-secure websites, which can be easily hacked.
- The message, if the digital signature is accessed by someone, or if it is transferred through unsafe online sites, might be accessed and altered.

2008 - Dec [2] Attempt the following :

(v) Describe the offence of 'hacking' with computer system as provided under the Information Technology Act, 2000. **(4 marks)** ***[CSEM - I]***

Answer :

The offence of hacking

- 'Hacking' means unlawful access of a computer resource or system owned or controlled by another and altering, deleting or adding unauthorized information.
- Such a change might result in the lessening or loss of the value of the original information contained in the system.
- The punishment for this offence as per the Information Technology Act, 2000 is three years of imprisonment and/or fine upto rupees five lakhs. **(Section 66)**
- Hacking definitely affects the financial returns of a company, since the hacker takes a large slice of the profits.
- It might also cause loss of reputation to the company whose Id is hacked, or it may even cause company secrets to be brought out into the open if the confidential information of the company is accessed.

Section 43 of the IT Act defines hacking:

- If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,- accesses or secures access to such computer, computer system or computer network downloads, copies or extracts any data, computer data base information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

- damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;
- disrupts or causes disruption of any computer, computer system or computer network;
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network. He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

2008 - Dec [3] Explain the following :

(v) Digital signature. **(4 marks)** ***[CSEM - I]***

Answer :

Please refer 2008 - June [3] (iii) on page no. 36

2009 - June [4] Attempt the following :

(iv) What are the 'cyber offences' under the Information Technology Act, 2000? **(4 marks)** ***[CSEM - I]***

Answer :

- The cyber offences are described in **Section 43 of Chapter IX titled Penalties and Adjudication of the Information Technology Act, 2000.** Chapter XI **(Section 65-78)** mentions the offences related to cyber crimes, i.e. crimes related with computers.
- They are as under and are caused if anyone does the following acts with reference to a computer, computer system or computer network in an unauthorized manner, without permission of the relevant authority who controls the resource –
  - If someone hacks into a computer resource.
  - If the information contained in the resource is accessed without permission, and copied or altered in any way.

- If the resource is infected with a computer virus or bug.
- If the resource or its functioning is disordered in any way, or it is damaged in any way, either by altering the settings or programmes or in any other manner.
- If the regular and authorized users are denied entry into or access to the resource.
- If aid is provided to anyone for doing any of the above-mentioned acts.
- If someone pays or hires someone to do any of the above-mentioned works.

- All of these offences are punishable with a maximum penalty to pay damages upto rupees one crore.

2010 - June [2] Attempt the following :

(iii) What are 'cyber offences' under the Information Technology Act, 2000? **(4 marks)** ***[CSEM - I]***

Answer :

Please refer 2009 - June [4] (iv) on page no. 39

2010 - Dec [4] (c) What are 'cyber offences' under the Information Technology Act, 2000 ? **(5 marks)** ***[CSEM - I]***

Answer :

Please refer 2009 - June [4] (iv) on page no. 39

2012 - June [4] Explain the following:

(ii) 'Cyber Regulations Appellate Tribunal' under the Information Technology Act, 2000 **(4 marks)** ***[CSEM - I]***

(v) 'Digital signature' under the Information Technology Act, 2000. **(4 marks)** ***[CSEM - I]***

Answer :

(ii)
- 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 Tribunal was initially known as the Cyber Regulations Appellate Tribunal (C.R.A.T.).
- Anyone who is unable to accept the decision of the adjudicator can apply to the Cyber Appellate Tribunal.
- The Tribunal can be approached even against the decision of the Controller of Certifying Authorities, who regulates all Certifying Authorities.
- This appeal has to be filed within 45 days from the date of receipt of the order against which the appeal is being filed.
- The High Court has the power to hear appeals regarding any order of the Cyber Appellate Tribunal. The limitation period for this is 60 days.

  As per CHAPTER X of the Information Technology Act, 2000:

  "**THE CYBER REGULATIONS APPELLATE TRIBUNAL**"

  1. (a) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.
     (b) The Central Government shall also specify, in the notification referred to in **sub-section (1)**, the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.
  2. A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.
  3. A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he-
     (a) is, or has been, or is qualified to be, a Judge of a High Court; or
     (b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

(v) Please refer 2008 - June [3] (iii) on page no. 36

2012 - Dec [4] Attempt the following:

(ii) The majority of legal problems in the information technology relate to the machine, the medium and the message. Discuss.

(4 marks) ***[CSEM - I]***

Answer:

It is true that the majority of problems in information technology relate to the machine, the medium and the message.

- **The machine:** This includes the instruments used in IT; if these are not foolproof, the machine and consequently the data or information contained therein might be endangered. Additional safety measures like password locking, data encryption should be used.
- **The message:** There are copyright and hacking issues. Moreover, different countries address these issues differently, so there is no standardization and hence, very less chance of any dispute being properly addressed.
- **The medium:** Unless the information is encrypted, or saved in a format that cannot be tampered with, the information may be endangered.

All these problems are compounded by the information available on the internet, which can be freely copied and creates copyright issues and other problems.

2013 - June [4] (b) Describe the offence of 'hacking' the computer system as provided under the provisions of the Information Technology Act, 2000.

(4 marks) ***[CSEM - I]***

Answer:

Please refer 2008 - Dec [2] (v) on page no. 38

2014 - June [1] Answer the following:

(a) "The Cyber Appellate Tribunal enjoys the powers of a Civil Court under the Code of Civil Procedure, 1908." Comment. **(4 marks)**

Answer:

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**, 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 of documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex-parte;
(g) any other matter which may be prescribed.

2014 - June [2] Answer the following:
(a) What is 'encryption'? Discuss the role of public and private key in safeguarding sensitive organisational data. **(4 marks)**
(b) Explain the duties of the Certifying Authority under the Information Technology Act, 2000 in respect of digital certificates. **(4 marks)**

Answer: (a)

(a) Encryption	• It basically consists of transforming the information from an intelligible form to a non-intelligible form while sending.
(b) Role of Public and Private key	• While receiving, the received information is transformed back to the original form. Modern encryption uses a pair of keys, one called "public" which is downloaded by the sender on initiation of the session. • The sender's machine uses a mathematical algorithm to encrypt the information. • This encrypted information can only be decrypted with the "private" key, which the receiver has, on his/her machine. • Thus, even if a cracker traps the information, he/she cannot decrypt it. • It is no use trying to decrypt by permutation because not even the fastest of computers can crack the encryption in years of continuous working.

Answer:

(b) As per **Section 2(1)(g) of Information Technology Act, 2000** "Certifying Authority" means a person who has been granted a license to issue a Digital Signature Certificate under section 24;

Duties of a certifying authority are mentioned under **section 30 of the Information Technology Act, 2000**. These are:

(i) It shall make use of hardware, software and procedures that are secure from intrusion and misuse;

(ii) Provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(iii) Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured;

(iv) Observe such other standards as may be specified by regulations;

(v) It shall disclose in the manner specified by regulations:
   (a) Its Electronic Signature
   (b) Any certification practice statement relevant thereto;
   (c) Notice of the revocation or suspension of its Certifying Authority certificate, which that authority has issued or the authority's ability to perform it services.

(vi) Certifying authority shall also ensure that every person employed by him complies with the provisions of the Act or rules, regulations or orders made thereto;

(vii) It must display its license at conspicuous place of the premises in which it carries on its business;

(viii) Certifying authority whose license is suspended or revoked shall immediately surrender the license to the controller;

(ix) Certifying authority shall disclose its digital signature certificate, which contains the public key corresponding to the private key used by the certifying authority and other relevant facts.

2014 - June [4] Answer the following:

(b) What is an 'electronic record'? Discuss the details contained in relevant section of the Information Technology Act, 2000 about the authenticity of electronic records. **(4 marks)**

Answer:

Electronic Record has been defined under **Section 2(1)(t) of the Information Technology Act, 2000.** According to which **"Electronic record"** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

Section 3 of the Act deals with authentication of electronic records and it lays down that:

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

2014 - June [6] Answer the following:

(b) What are the functions of Controller of Certifying Authorities as per the Information Technology Act, 2000? **(4 marks)**

Answer:

The Controller may perform all or any of the following functions, namely:

(a) Exercising supervision over the activities of the Certifying Authorities;

(b) Certifying public keys of the Certifying Authorities;

(c) Laying down the standards to be maintained by the Certifying Authorities;

(d) Specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) Specifying the contents of written, printed or visual materials and Advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) Specifying the form and content of a Digital Signature Certificate and the Key,

(h) Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) Specifying the terms and conditions subject to which auditors may be Appointed and the remuneration to be paid to them;

(j) Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) Specifying the manner in which the Certifying Authorities shall conduct their Dealings with the subscribers;
(l) Resolving any conflict of interests between the Certifying Authorities and the Subscribers;
(m) Laying down the duties of the Certifying Authorities;
(n) Maintaining a database containing the disclosure record of every Certifying Authority;
(o) Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

2014 - Dec [1] (a) Describe the meaning and contents of digital signatures. Who issues digital signatures?
Under what conditions digital signatures may be revoked by the issuing authority? **(5 marks)**

Answer:

- Digital signatures are data block appended to a file or message (or a complete encrypted file or message) such that the recipient can authenticate the file or message contents and/or prove that it could only have originated with the purported sender.

- A digital signature is a technique used to validate the authenticity and integrity of a message, software or digital document. It is the equivalent to a handwritten signature or stamped seals in digital form, but offers far more inherent security.
- It is intended to solve the problem of tampering and impersonation in digital communications.
- Certifying Authority has been granted license to issue a Digital Signature Certificate under **section 24** of Information Technology Act.
- A Certifying Authority may revoke a Digital Signature Certificate issued by it:
  (a) where the subscriber or any other person authorized by him makes a request of that effect; or
  (b) upon the death of the subscriber, or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

- Certifying Authority may also revoke a Digital Signature Certificate which has been issued by it any time, if it is of opinion that:
  (a) a material facts represented in the Digital Signature Certificate is false or has been concealed;
  (b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
  (c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
  (d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

2014 - Dec [2] (a) (i) What does a 'computer network' mean in the Information Technoloy Act, 2000? **(2 marks)**

(ii) Which court has jurisdiction over matters pertaining to the Cyber Appellate Tribunal (CAT)? **(2 marks)**

Answer:

(i) **Section 2(1)(j)** defines 'Computer network' as the interconnection of one or more computers through -
- The use of satellite, microwave, terrestrial line or other communication media; and
- Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

Answer:

(ii)
- As per **Section 61 of the Information Technology Act, 2000**, no court shall have jurisdictions to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal (CAT) constituted under this Act is empowered by or under this Act.
- Further, no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

- As per **Section 62** of the Information Technology Act, any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him, on any question of fact or law arising out of such order.
- Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow the appeal to be filed within a further period not exceeding sixty days.

2014 - Dec [2] (b) (i) Mention briefly what does section 43A of the Information Technology Act, 2000 provide for. **(2 marks)**

(ii) Which section deals with the punishment for violation of privacy? What is the maximum punishment provided for violation of privacy? **(2 marks)**

Answer:

(i) Compensation for failure to protect data: As per **Section 43A of IT Act, 2000** as amended, where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Answer:

(ii) Punishment for Violation of privacy: As per **Section 66E of the IT Act, 2000** as amended whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding ₹ 2 lakh, or with both.

2015 - June [1] (a) Comment on the punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form as stated in section 67A of the Information Technology Act, 2000. **(4 marks)**

Answer:

As per **Section 67A of the IT Act, 2000,** whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

2015 - June [6] (a) What is the objective of establishing Cyber Appellate Tribunal under the Information Technology Act, 2000? **(4 marks)**

Answer:

The Cyber Appellate Tribunal (CAT) has been established with the objective to listen to the appeal of any person aggrieved by the order of controller or an adjudicating officer. Thus, CAT Act as a forum to seek redressal. However, the jurisdiction of this Tribunal cannot extend to hearing any other application or petition that is not an appeal from the order of the controller or an adjudicating officer.

2015 - Dec [3] (b) "The Information Technology Act, 2000 is not applicable over several other Acts." Explain. **(4 marks)**

Answer:

IT Act 2000 does not apply to:

(a) A negotiable instrument as defined in **Section 13 of the Negotiable Instruments Act, 1881**;
(b) A Power-of-Attorney as defined in **Section 1A of the Powers-of-Attorney Act, 1882;**
(c) A trust as defined in **Section 3 of the Indian Trusts Act, 1882;**
(d) A will as defined in clause (h) of **Section 2 of the Indian Succession Act, 1925** including any other testamentary disposition by whatever name called;

(e) Any contract for the sale or conveyance of immovable property or any interest in such property;
(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2016 - June [1] (a) Describe the 'digital signature certificate'. Under what conditions digital signature may be suspended by the certifying authority? Explain. **(5 marks)**

Answer:

Digital Signature Certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. It is a technique used to validate the authenticity and integrity of a message, software or digital document. Digital certificates can be presented electronically to prove ones identity, to access information or services on the Internet or to sign certain documents digitally and offer inherent security.

1. The provisions relating to Suspension of Digital Signature Certificate are contained in **Section 37 of IT Act, 2000** as amended. This provides that the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate:
   (a) on receipt of a request to that effect from:
      (i) the subscriber listed in the Digital Signature Certificate; or
      (ii) any person duly authorized to act on behalf of that subscriber.
   (b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.
2. A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.
3. On suspension of a Digital Signature Certificate under this Section, the Certifying Authority shall communicate the same to the subscriber.

2016 - June [2] (a) "The Information Technology Act, 2000 does not apply to certain documents or transactions." Explain. **(4 marks)**

Answer:

Information Technology Act, 2000 is not be applicable to:

(a) A negotiable instrument as defined in **Section 13** of the **Negotiable Instruments Act, 1881.**

(b) A power-of-attorney as defined in **Section 1A of the Powers-of-Attorney Act, 1882.**
(c) A trust as defined in **Section 3 of the Indian Trusts Act, 1882.**
(d) A will as defined in **clause (h) of Section 2** of the **Indian Succession Act, 1925** including any other testamentary disposition by whatever name called.
(e) Any contract for the sale or conveyance of immovable property or any interest in such property.
(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2016 - Dec [2] (b) Explain the retention of electronic records as per Section 7 of the Information Technology Act, 2000. **(4 marks)**

Answer :

Section 7 of Information Technology Act, 2000 provides for the retention of records in electronic format. It states that wherever any law provides that the documents, records or information shall be retained for any specific period, then that requirement shall be deemed to be have been satisfied if such documents, records or information are retained in electronic form, if:

1. The details which will facilitate their identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in electronic record.
2. The information contained therein remains accessible so as to be usable for a subsequent reference.
3. The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information digitally generated, sent or received.

Provided that this clause does not apply to any information, which is automatically generated solely for the purpose of enabling and electronic record to be dispatched or received. These provisions will not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

2016 - Dec [3A] (Or) (i) Define the following terms under Information Technology Act, 2000:

(a) Asymmetric crypto system
(b) Digital signature
(c) Private key
(d) Public key. **(1 mark each)**

Answer :

(a) **Asymmetric crypto system:** It means a system of a secure key pair consisting of a Private Key for creating a digital signature and a Public Key to verify the digital signature.

(b) **Digital Signature:** It means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of **Section 3 of Information Technology Act, 2000** as amended. Digital signatures are used to authenticate the contents of electronic documents. They can be used with PDF, e-mail messages, and word processing documents.

(c) **Private Key:** In cryptography, a private key (secret key) is a variable that is used with an algorithm to encrypt and decrypt code. Quality encryption always follows a fundamental rule: the algorithm doesn't need to be kept secret, but the key does. Private keys play important roles in both symmetric and asymmetric cryptography. It means the key of a key pair used to create a digital signature.

(d) **Public Key:** It means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

2016 - Dec [5] (b) A Certifying Authority certifies some parameters/conditions while issuing a digital signature certificate. Identify the section under which these parameters/conditions have been provided in the Information Technology Act, 2000 and explain the same in detail. **(8 marks)**

Answer :

A Certifying Authority certifies certain parameters/conditions while issuing a Digital Signature Certificate. These parameters/conditions are given **under section 36 of Information Technology Act, 2000** as amended, these are as under:

A Certifying Authority while issuing a Digital Signature Certificate shall certify that:

- It has complied with the provisions of this Act and the rules and regulations made there under,
- It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
- The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
  - ⇒ The subscriber holds a private key which is capable of creating a digital signature;
  - ⇒ The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber;
  - ⇒ The subscriber's public key and private key constitute a functioning key pair;
- The information contained in the Digital Signature Certificate is accurate; and
- It has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses above.

2017 - June [1] (a) What are the functions of Controller of Certifying Authority as per the Information Technology Act, 2000? **(5 marks)**

Answer:

Please refer 2014 - June [6] (b) on page no. 45

2017 - June [3] (a) Briefly explain the objectives of making Information Technology Act, 2000 of India. **(4 marks)**

Answer:

The Information Technology Act, 2000 was made applicable in India with following objectives:

1. To give legal recognition to any transaction which is done electronically 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 in employment exchange.

4. To provide legal recognition for storage in electronic format.
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 amend the Indian Penal Code, 1860, Indian Evidence Act, 1872, The **Bankers' Books Evidence Act, 1891** and the **Reserve Bank of India Act, 1934**.

2017 - Dec [4] (c) List out various powers of Cyber Appellate Tribunal. **(4 marks)**

(d) Explain computer related offences and related penalties as specified in IT Act. **(4 marks)**

PRACTICAL QUESTIONS

2012 - Dec [8] (a) One morning, scientists at an atomic research centre found a rude-nuclear message splashed across their computer screens. Someone had breached the atomic research centre's advanced security system and sensitive e-mail.

What offence has been committed in the atomic research centre? Decide with reference to the provisions of the relevant statute.

(6 marks) ***[CSEM - I]***

Answer:

- This is the offence of 'hacking' as per **Section 66 under the Information Technology Act, 2000.**
- This Section provides that if any person deliberately or knowingly causes destruction or deletion in information stored in a computer resource, or causes its value or importance to be reduced, or otherwise harms it, he is committing the offence of hacking.
- The punishment for which he might be liable to imprisonment upto three years or fine extending upto five lakhs rupees or with both.

TOPIC NOT YET ASKED BUT EQUALLY IMPORTANT FOR EXAMINATION

SHORT NOTES

Q.1 Write short note on Electronic Signature Certificate.

Answer:

- The provisions relating to Electronic Signature Certificate are contained in **Section 35-39 of IT Act, 2000** as amended.
- It provides that Certifying Authority will issue Electronic Signature Certificate on an application by a person in the form prescribed by the Central government.
- The application should be accompanied by a fee not exceeding ₹25,000/- and a certificate practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
- On receipt of an application, the Certifying Authority may, after consideration of the certification practice statement or the other prescribed statement and after making such enquiries as it may deem fit, grant the electronic Signature Certificate or for reasons to be recorded in writing, reject the application:
- Provided that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Repeatedly Asked Questions		
No.	**Question**	**Frequency**
1	Describe the offence of 'hacking' with computer system as provided under the Information Technology Act, 2000. 08 - Dec [2] (v), 13 - June [4] (b)	2 Times
2	What are 'cyber offences' under the Information Technology Act, 2000 ? 09 - June [4] (iv), 10 - June [2] (iii), 10 - Dec [4] (c)	3 Times
3	Distinguish between on 'Computer network' and 'computer system'. 09 - June [3] (v), 11 - June [4] (b) (iii)	2 Times
4	'Digital signature' under the Information Technology Act, 2000. 08 - June [3] (iii), 08 - Dec [3] (v), 12 - June [4] (v)	3 Times
5	'Public key' and 'private key' 09 - June [3] (i), 12 - June [5] (v)	2 Times
6	The majority of legal problems in the information technology relate to the machine, the medium and the message. Discuss. 08 - June [4] (iii), 12 - Dec [4](ii)	2 Times