CYBERSECURITY ISSUES AND CHALLENGES: COMPREHENSIVE THEORY NOTES

This material synthesises all key information from your notes (Source 19.pdf, 199.txt, and study notes) for maximum efficiency and detail, covering the syllabus topics for your engineering examination.

UNIT 1: CYBER SECURITY FUNDAMENTALS

1. Introduction to Cyber Security

Cyber security is the **protection of Internet-connected systems**, including hardware, software, and data, from malicious cyber attacks. It encompasses technologies, processes, and practices designed to safeguard networks, devices, programs, and data from theft, damage, modification, or unauthorized access. It is sometimes referred to as information technology security.

Components of Cyber Security: Cyber security can be broken down into security related to systems, networks, applications, and information.

2. Digital Security – The CIA Triad

Digital security is the protection of your computer, mobile devices, tablets, and any other Internet-connected devices from intruders like hackers or those using phishing techniques. It also protects personal data from being exploited or sold by companies.

The three core pillars (CIA Triad) of digital security are:

1. **Confidentiality:** The principle of keeping private information hidden from unauthorized persons. The core essence is sharing private information with the least amount of people to keep it secure. This is often achieved through **cryptography and encryption methods**.
2. **Integrity:** The ability to ensure that data is an **accurate and unchanged representation** of the original secure information. It ensures that information is not modified or corrupted.
3. **Availability:** Ensuring that information is **consistently and readily accessible** for authorized parties whenever needed. This involves managing hardware and technical infrastructure effectively.

Aspect	Pros (Advantages)	Cons (Disadvantages)

Digital Security	Protects personal data. Blocks suspicious/unauthorized access. Provides data confidentiality. Protects systems from crashing/slowing down. Fosters economy by cutting costs.	Tools/services can be costly. Compatibility issues with user devices. Configuration and updates can be difficult. May slow down device functioning.

UNIT 2: SECURITY BREACHES IN CYBERSPACE

1. Cyberspace Definition

Cyberspace is the virtual computer world, specifically an **electronic medium used for online communication**. It involves a large global computer network utilizing the **TCP/IP protocol** for data exchange.

2. Major Security Issues / Breaches

Cybersecurity challenges and breaches include threats from unauthorized access, various denial of service attacks, and malicious software.

- **Unauthorized Access:** Gaining access to a computer, network, system, or device without the permission of authorized personnel.
- **Distributed Denial of Service (DDoS) Attack:** When multiple systems (attackers) attempt to make a service unavailable or impossible to deliver by overwhelming servers, networks, applications, or specific transactions.
- **Malware (Malicious Software):** Any program or file harmful to a computer user.
    - **Types:** Viruses, worms, Trojan horses, spyware, and ransomware.
    - **Function:** Stealing, encrypting, or deleting sensitive data, altering core computing functions, or monitoring user activity.
- **Social Engineering Attacks:** Involve psychological manipulation to trick unsuspecting users or employees into revealing confidential data. Often involves communication designed to invoke urgency or fear.
- **Phishing:** Attacks attempting to steal sensitive information (usernames, passwords, credit card info, network credentials) via fake communication, typically email.
- **Crypto Jacking:** A cybercrime involving the unauthorized use of a person's device (computer, smartphone, server) to mine cryptocurrency.
- **Pharming:** An attacker redirects a user from a legitimate website to a fake, deceitful site where the system is infected with malware.
- **Exploiting Vulnerability:** Attacker finds and exploits a flaw (vulnerability) in existing security measures to gain access or harm the device.
- **Cyber-Physical Attacks:** Attacks that breach cyber security and consequently impact the physical environment, such as targeting cyber-controlled mechanisms like cameras or lights.

- **Drive-by Download:** Malicious programs installing onto devices without the user's consent, often by merely visiting a compromised website.
- **Man-in-the-Middle (MitM) Attack:** Occurs when criminals place themselves between a two-party communication, interpreting it to steal sensitive data and return modified responses.
- **Website Defacement:** A system cracker gains unauthorized access to a web server and replaces the site's homepage/content with their own message or destroys the contents.
- **Key Loggers:** Software intended to covertly monitor and log all keystrokes made by a user on the keyboard.

UNIT 3: CRYPTOGRAPHY MECHANISMS

1. Encryption and Algorithms

Data Encryption: Translates unencrypted data (**plaintext**) into code (**ciphertext**) so that only parties with the secret decryption key or password can read it.

A. DES (Data Encryption Standard)

- **Type: Symmetric Cryptosystem** (uses the same key for encryption and decryption).
- **Origin:** Developed by IBM and adopted as an NBS Standard in 1977.
- **Structure:** Operates on **64-bit blocks** of input, uses a **56-bit encryption key**, and is based on the **Feistel Structure**.
- **Process (16 rounds):** 64-bit plaintext $\rightarrow$ Initial Permutation (IP) $\rightarrow$ Split into Left Plain Text (LPT) and Right Plain Text (RPT) $\rightarrow$ 16 Rounds of encryption $\rightarrow$ Rejoin $\rightarrow$ Final Permutation (FP) $\rightarrow$ 64-bit ciphertext.
- **Triple DES (3DES):** A symmetric key-block cipher that applies the DES cipher three times (Encrypt with K1, Decrypt with K2, Encrypt with K3).

B. RSA Algorithm

- **Type: Asymmetric Cryptography Algorithm** (uses two different keys: a public key and a private key).
- **Origin:** Named after its inventors: Ron Rivest, Adi Shamir, and Leonard Adleman (1978).
- **Principle:** Based on modular mathematics of Number theory. The public key is shared, while the private key must be kept secret.
- **Encryption:** $C = P^e \text{ mod } n$ (P = plaintext, C = ciphertext).
- **Decryption:** $P = C^d \text{ mod } n$ (using the private key $(n,d)$).

C. Hybrid Encryption

This method combines the speed of symmetric encryption (best for large data encryption) with the strong identity verification features of asymmetric encryption (public/private key pairs).

2. Digital Signatures

A digital signature is a technique used to secure electronic information such that the **originator of the information** and its **integrity** can be verified. This process of guaranteeing origin and integrity is known as **Authentication**.

Feature	Electronic Signature	Digital Signature
Purpose	Used for verifying a document.	Used for securing a document.
Examples	Email signatures, web-based signatures, digitized images.	Signing tenders, e-filing for income tax or GST.
Technology	Authentication by electronic technique.	Uses hash function, private key, and public key (two-way protection).
Validity	Has no expiry or validity period.	Valid up to a maximum of three years.

3. Authentication and Authorization

- **Authentication:** The process of **identifying users** and validating who they claim to be, typically by checking credentials like a password against a stored user name. This process is done *prior* to authorization.
- **Authorization:** Occurs after successful authentication and involves **offering access rights** (full or partial access) to specific resources (like databases or funds), based on the user's privilege or security levels.

4. Hash Functions

A hash function is a mathematical function that converts an input value of **arbitrary length** into a compressed **numerical output of fixed length**. The output values are known as a **message digest** or simply a **hash value**.

- **Cryptographic Uses:**
  - **Digital Signatures:** A long message is hashed, and only the smaller hash value is signed, saving time and space.

    - **Data Integrity:** The hash value of data is computed and protected; later checks verify that the input data has not been altered.
- **Popular Functions:** Message Digest family (MD2, MD4, **MD5 -** 128-bit), **SHA family** (SHA-0, SHA-1, SHA-2, SHA-3), RIPEMD, and **Whirlpool** (512-bit).

5. Key Management and Infrastructure (PKI)

Key Management

- **Key Establishment:** The process by which a **shared secret key** becomes available to two or more parties for subsequent cryptographic use. This includes **key agreement** (both parties contribute) and **key transport** (one party sends the key).
- **Key Management (Maintenance):** The processes and mechanisms that support ongoing keying relationships, covering initialization, generation, distribution, installation, controlling use, updates, revocation, destruction, storage, and archival.
- **Symmetric-key systems** use the same secret key for both originator and recipient. **Asymmetric systems** use a public key (public transformation) and a related private key (private transformation).

Trusted Third Party (TTP)

A TTP is an entity in a domain trusted to perform a specific service, such as possessing secret decryption keys. A **Functionally Trusted** TTP is assumed to be honest and fair but does not have access to the secret or private keys of users.

Public Key Infrastructure (PKI)

PKI is a cryptography framework aimed at facilitating the **secure electronic transfer of information** for digital activities, primarily by providing assurance and distribution of public keys.

- **Components:** Public Key Certificate (digital certificate), Private Key tokens, Certification Authority (CA), Registration Authority, and a Certificate Management System.
- **Disadvantage:** The main vulnerability is that the public key is in the public domain and is vulnerable to misuse, emphasizing that cryptographic security largely depends on robust key management.
- **Indian CAs:** Five common Certified Authorities (CAs) in India include Safescrypt Ltd, TCS, IDRBT, MTNL, and NIC.

Pseudo Random Number Generator (PRNG)

An algorithm using mathematical formulas to generate sequences of random numbers. They are crucial for cryptographic applications, such as generating encryption keys in a manner unpredictable to an adversary. PRNG systems are efficient, easy to determine (for replaying sequences), and periodic.

UNIT 4: DATA SECURITY & MANAGEMENT

1. Data Security and Data Management

Data Security Management is the practice of collecting, keeping, and using data securely, efficiently, and cost-effectively, ensuring privacy, data integrity, and preventing access by unauthorized parties.

Database Security is necessary in cases of theft/fraud, and potential loss of confidentiality, privacy, integrity, or availability of data.

Five Components to Data Management (Responsible stewardship throughout its lifecycle):

1. Acquisition (Collecting data)
2. Utilization (Using data effectively)
3. Maintenance (Keeping data current)
4. Access (Controlling view/use)
5. Protection (Securing from threats)

2. Security Requirements (CIA Implementation)

Implementation practices ensure that the three pillars of data security (CIA) are met:

CIA Pillar	Key Implementation Practices
Confidentiality	Categorise data based on privacy requirements. Enforce data encryption and two-factor authentication. Regularly monitor and update access control lists (ACLs).
Integrity	Review data processing/transfer mechanisms. Run diagnostic tests to detect unauthorized access. Stay updated on compliance and regulatory requirements.
Availability	Build preventative measures into system design. Conduct routine security audits. Utilize auto-update systems, network monitoring software, and anti-virus solutions.

3. Key Security Threats (Recap & Details)

- **Man-in-the-Middle (MitM):** Attackers intercept two-party communications to steal data or return different responses.

- **State-Sponsored Attacks:** Hacking threats targeting governments and nations, not just private sectors or individuals.
- **Cyber-Physical Attacks:** Hacks targeting modernized and computerized critical infrastructure (e.g., electrical grids, transportation systems).

4. Devices and Internet Limitations

- **Computer:** The foundation of the virtual world; an information processor that stores, decrypts, and outputs data based on computer programs (like Microsoft Word or Excel).
- **Mobile Device:** A handheld computer or smartphone for communication on the move, featuring Wi-Fi/cellular access, a battery, a keyboard/touch-screen, and the ability to download data.
- **Internet:** A vast collection of interconnected computer networks where devices are differentiated by their assigned **Internet Protocol (IP) address**.
- **Limitations (Mobile/Internet):** Speed, accessibility, incompatibility, data leakage, use of unsecured Wi-Fi, and SMishing (phishing via SMS).

5. Security Measures and Solutions

1. **Access Control:** Restricting access to sensitive data only to users whose identity has been verified through an access control gateway.
2. **Data Encryption:** Encoding information (ciphertext) so it can only be accessed or decrypted by a user possessing the correct encryption key.
3. **Email Security:** Procedures like strong passwords and end-to-end encryption to protect email accounts and contents from hackers spreading malware, spam, or phishing attacks.
4. **Risk-Assessment Analysis:** Identifying internal and external risks pertaining to stored information to understand threats to security, confidentiality, and personal information.
5. **Strong Firewall:** Controls Internet traffic and protects a system from unauthorized network access or usage, distinguishing it from antivirus software which deals with files.
6. **Antivirus Protection:** Software designed to detect, avoid, and deal with cyber security threats, running background scans to restrict unauthorized access in the form of malware.
7. **Regular Backups:** Securing data helps prevent accidental modification, data theft, and breaches of confidentiality.

6. Security Management, Policy, and Audit

- **Security Management:** Minimizing business interruption and reducing vulnerability to attacks.
  - **6 Principles:** Availability, Integrity, Confidentiality (CIA), Accountability, Assurance, and Privacy.
- **Security Policy:** A formal written document outlining rules for authorized users regarding access to company technology and information assets, detailing how to protect the organization from threats and handle them when they occur.

- **Security Audit:** An overall assessment of an organization's security (physical configuration, software, practices).
    - **Goals:** Create a security benchmark, identify shortcomings, and prioritize high-risk exposures.
- **Usability:** The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction (encompassing the "user experience").

UNIT 5: REGULATION OF CYBERSPACE

1. Need and Methods for Regulation

Cyberspace is a global environment without a formal legal framework. Regulation is needed because anonymity allows misuse like viruses, rumor-mongering, and hate mail, undermining public safety and security.

Three-Fold Regulatory Strategy:

1. **Privatization:** Encouraging private sector involvement in regulation.
2. **Propertization:** Establishing property rights as a basis for control.
3. **Technological Controls:** Designing hardware and software systems to incorporate desired regulatory features (e.g., blocking software).

2. Filtering Devices and Rating Systems

- **Filters:** Software tools used to block unwanted material (e.g., spam filters, site blocking software).
- **PICS Protocol (Platform for Internet Content Selection):** Developed by the W3C for content labeling schemes, used by parents and schools for interoperability and classifying content.
- **RDF (Resource Description Framework):** A protocol for describing Internet content based on the "Dublin Core" (105 categories) used specifically to filter out obscene content.

3. Global Regulatory Frameworks

UNCITRAL Model Law (1996)

Adopted by the UN Commission on International Trade Law to eliminate legal and technical hindrances and boost legal certainty for electronic commerce.

- **Three Doctrines:** Non-discrimination principle, Technological neutrality principle, and the equivalence functional principle.
- **Structure:** Part 1 deals with general provisions regarding e-commerce; Part 2 deals with specific provisions for e-commerce in certain areas.

United States

Cyber regulation is composed of various laws, starting with the **Comprehensive Crime Control Act of 1984**.

- **Communication Decency Act (CDA, 1996):** Created a criminal offense for knowingly transmitting "obscene" or "indecent" messages to recipients under 18 years.
- **Children Internet Protection Act (CIPA, 2000):** Requires schools and libraries to install content filters on computers used by minors and adults.
- **Other Legislation:** Uniform Electronic Transaction Act (UETA, 1999), Health Insurance Portability and Accountability Act (HIPAA, 1996).

European Union (EU) and UK

EU strategy involves three main action lines: promoting a safer environment (hotlines, self-regulation), developing filtering/rating systems, and increasing awareness. The UK's mission is led by the **National Cyber Security Centre (NCSC)**, which is part of GCHQ, protecting critical services and managing major incidents.

India

The main cyber law is the **Information Technology Act (IT Act), 2000**.

- **Objective:** To provide legal recognition for transactions using electronic communication (e-commerce) and facilitate electronic filing of documents with government agencies.
- **Coverage:** Electronic signatures, e-governance, regulation of certifying authorities, digital certificates, penalties/adjudication, and offenses.

International Initiatives

- **Bonn Declaration (1997):** Focused on enforcing criminal law provisions for online crime using existing national frameworks, establishing industry self-regulation, and setting up national hotlines for online content complaints.
- **OECD:** Acknowledged the **primary role of the private sector** in regulating the Internet and recommended coordination between government and industry to combat global issues like spam.
- **UNESCO (1945):** Functions as a laboratory of ideas and a standard-setter for universal agreements on emerging ethical issues.
- **CYBERBRICS:** A project focused on cyber security governance for the BRICS nations (Brazil, Russia, India, China, South Africa), focusing on areas like data protection, cybercrime, and cyber defense.

UNIT 6: CYBER CRIMES

1. Definition and Classification

Cybercrime is defined as crimes committed on the internet using the computer as a tool to target the victim for the execution of the desired crime. Cyber crimes are typically harder to detect, investigate, and prosecute compared to traditional crimes.

Classification	Examples of Cyber Crimes
Against Individuals	Harassment, cyber-stalking, defamation, cheating, email spoofing, fraud.
Against Property	Transmitting viruses, net-trespass, unauthorized system control, internet thefts, infringement of intellectual property.
Against Organizations	Cyber terrorism within government/organization, possession of unauthorized information, distribution of pirate software.
Against Society	Child pornography, financial crimes, trafficking, forgery of records, gambling.

2. Penalties and Compensation (IT Act, 2000)

The IT Act differentiates between civil wrongs (liable for damages/compensation) and criminal offenses (liable for imprisonment/fines).

IT Act Section	Focus	Penalty / Compensation
Section 43 (Civil)	Unauthorized access, data damage, introducing viruses/contaminants, denying access, stealing source code (without permission).	Liable to pay **damages by way of compensation** to the affected party.
Section 43A	Body corporate's failure to protect sensitive personal data.	Liable for **compensation**.

Section 44	Failure to furnish information/return/records.	Penalties ranging from ₹5,000 to ₹1,50,000 for various failures.
Section 45	Residuary penalty for contravention of rules where no separate penalty is provided.	Maximum penalty of **₹25,000**.
Section 66 (Criminal)	Dishonestly or fraudulently committing any act referred to in Section 43 (e.g., hacking).	Imprisonment up to **3 years** or fine up to **₹5,00,000**, or both.

Definitions under Section 43 (Explanation):

- **Computer Contaminant:** Computer instructions designed to modify, destroy, transmit data, or usurp the normal operation of a computer resource.
- **Computer Virus:** Program that damages, destroys, or degrades the performance of a computer resource, operating when a program is executed.
- **Damage:** To destroy, alter, delete, add, modify, or rearrange any computer resource by any means.

3. Key Offences (IT Act, 2000)

IT Act Section	Offence	Penalty	Related IPC Section
Section 65	Tampering with computer source documents (intentionally concealing, destroying, or altering source code).	₹2,00,000 or 3 years imprisonment or both.	N/A
Section 66B	Dishonestly or fraudulently receiving or retaining any stolen computer resource.	₹1,00,000 or 3 years imprisonment or both.	**IPC 411** (Receiving stolen property).

Section 66C	Fraudulently using an Electronic Signature, Password, or Unique ID feature of another person.	₹1,00,000 or 3 years imprisonment or both.	N/A
Section 66D	Cheating by personation using a communication device or computer resource.	₹1,00,000 or 3 years imprisonment or both.	**IPC 419** (Cheating by personation); **IPC 420** (Cheating and inducing delivery of property).
Section 66E	Intentionally capturing, publishing, or transmitting an image of a person's private area without consent.	₹2,00,000 or 3 years imprisonment or both.	N/A

> **Note: Section 66A** was struck down by the Supreme Court in the *Shreya Singhal vs. Union of India* case (2015), as it violated the Constitutional guarantee of Freedom of Speech and Expression.

4. Adjudication, Appeal, and Jurisdiction

- **Adjudication (Section 46):** Disputes for awarding compensation where the claim does not exceed **₹5 crore** are handled by an adjudicating officer (who must possess IT, legal, or judicial experience). Claims exceeding ₹5 crore vest with the competent civil court.
- **Appellate Tribunal (Section 48):** Appeals from the Adjudicating Officer go to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT). Appeals must be filed within 45 days (Section 57). The Tribunal is guided by natural justice and has powers similar to a civil court.
- **Appeal to High Court (Section 62):** Any person aggrieved by the Appellate Tribunal's decision may appeal to the High Court within 60 days.
- **Jurisdiction (Section 75):** The IT Act applies to any offense or contravention committed **outside India** if the act involves a computer, computer system, or network located **in India**, regardless of the offender's nationality.

5. Liability of Network Service Providers (NSP)

An NSP provides access to electronic information services (e.g., ISPs, mobile service providers).

- **Exemption:** NSPs are exempt from liability if their function is limited to being an intermediary providing access to a communication system, and they neither initiate, select the receiver, nor modify the information, while observing due diligence.

- **No Exemption:** Liability applies if the NSP conspired/abetted the unlawful act, or if, after receiving actual knowledge or notification from the government regarding unlawful material, they fail to expeditiously remove or disable access to that material.

6. Cyber Forensics

Definition: The application of investigation and analysis techniques to gather and preserve evidence from computing systems (computers, networks, online domains, storage devices) in a manner appropriate for presentation in a court of law.

Process Phases (5 Steps of Digital Forensics):

1. Policy and Procedure Development
2. Assessment
3. Acquisition
4. Examination
5. Reporting

Techniques Used: Cross-driven analysis (correlating data from multiple drives), Live analysis (data acquisition before shutdown), Deleted file recovery, Stochastic Forensics (detecting data theft), and Steganography (concealing files within others). **Evidence Handling:** Digital evidence is fragile and easily damaged; therefore, the original evidence is often duplicated, and the analysis is carried out on the copy to prevent mishap.

UNIT 7: INTELLECTUAL PROPERTY RIGHTS (IPR)

1. IPR Basics

Definition: IPR refers to intangible property that constitutes the **creations of one's mind** (not merely an idea, but the expression of it). **Novelty** is considered the main ingredient for intellectual property. **Rationale:** To grant creators/inventors due recognition and monetary benefits for a certain period to encourage research, innovation, and economic growth.

Seven Forms of Intellectual Property:

1. Copyright and related rights
2. Patents
3. Trademarks
4. Industrial Designs
5. Geographical Indications (GI)
6. Trade Secrets
7. Plant Variety (Protection for new engineered plant species/strains)

2. Forms of IPR in Detail

IPR Type	Protection Scope & Key Requirements	Duration/Governing Act
Copyright	Literary, musical, dramatic, artistic works, films, sound recordings, web content, computer software. Grants exclusive economic (Sec 14) and moral rights (Sec 57).	**Duration:** 60 years after the author dies (literary/artistic) OR 60 years from publication (films/programs/recordings). **Act:** Copyright Act, 1957.
Patents	Exclusive right for a novel invention (product or process) having an **inventive step** (non-obvious) and capable of **industrial application**.	**Duration:** Limited period (territorial rights). Utility Models typically protect for 10 years and do not require an inventive step. **Act:** Patents Act, 1970. **Not Patentable:** Scientific theories, mathematical methods, bookkeeping, medical procedures, or inventions contrary to public order/morality.
Trademarks	Distinctive sign, word, symbol, or mark distinguishing goods or services (e.g., logo, slogan). **Requirement:** Must be distinctive in nature.	**Duration:** 10 years from application, renewable every 10 years. **Act:** Trade Marks Act (TMA), 1999.
Industrial Designs	Appearance of a product/logo; shape, pattern, lines, or color. **Requirement:** Must be new or original and aesthetic; requires **mandatory registration**.	N/A

Geographical Indication (GI)	Name/sign used on products corresponding to a specific geographical location or origin (e.g., Basmati rice, Tequila) with special quality or reputation.	**Registration:** Not required. **Act:** GI Act, 1999.
Trade Secrets	Confidential secret information providing an inherent economic advantage or competitive edge (e.g., formulae, recipes, practices).	**Registration:** Not required. Protection lasts as long as the secret is maintained (use NDAs and limit access).

3. IPR Infringements in Cyberspace

IPR protection is challenging in the digital world because works are easily replicated, transmitted, modified, and manipulated. This leads to piracy and counterfeited goods.

- **Deep Linking:** Links directly to subordinate pages of a website, **bypassing the homepage or advertisements**, thereby undermining the original site owner's potential revenue.
- **In-lining:** Displaying a graphic file (e.g., a photo or cartoon) hosted on a second website while the user remains viewing the first website.
- **Framing:** Allowing a user to view the contents of one website within a frame controlled by another site, creating a "picture-in-picture" effect. This may trigger disputes under trademark law as it can create a false impression of endorsement or association.
- **Search Engine Abuse:** Use of keywords or meta-tags to unfairly redirect users, often leading to trademark infringement issues.

4. Legal Protection in India (IPR Remedies)

The Indian framework for IPR protection relies on specific legislation:

Law	Infringement Remedies

Copyright Act, 1957	**Civil Remedies:** Injunctions, damages, rendition of accounts. **Criminal Remedies:** Imprisonment and fines (Section 63). **Fair Use Exceptions** allow making backup copies of computer programs, acts for inter-operability, observation/study, and non-commercial personal copies.
Trade Marks Act, 1999	**Civil Remedies:** Injunctions and damages (Section 135). **Criminal Remedies:** Penalties for applying false trademarks (Section 103: min 6 months to 3 years imprisonment); Penalties for selling goods with false marks (Section 104: min 6 months to 3 years imprisonment + fine ₹50,000-₹2 lakh).
Administrative Remedies	Import/export protection of IPR under the **Indian Customs Act, 1962**.
IT Act, 2000	Deals with electronic records.

5. International Scenario (IPR Treaties)

International treaties aim to create uniformity in dealing with IPR disputes, ensuring uniform protection across member countries.

Treaty	Year	Key Principles / Purpose
Berne Convention	1886	Protects literary and artistic works. **1. National Treatment:** Works originating in one Contracting State receive the same protection in others as domestic works. **2. Automatic Protection:** Protection is not conditional upon compliance with formalities. **3. Independence:** Protection is independent of protection existing in the country of origin.
Universal Copyright Convention (UCC)	1952	Established the Intergovernmental Copyright Committee.

TRIPS Agreement	1994	Agreement on Trade-Related Aspects of Intellectual Property Rights. Aims to create global uniformity in IPR disputes.

QUICK REVISION CHECKLIST & STUDY TIPS

Category	Must-Know Concepts	Key Acts & Dates
Fundamentals	**CIA Triad** (Confidentiality, Integrity, Availability). **Cyber Threats** (DDoS, Malware, Phishing, Social Engineering). Digital vs. Electronic signatures.	DES: 1977 (56-bit). RSA: 1978 (Asymmetric). IT Act (India): 2000.
Cryptography	**DES vs RSA** (Symmetric vs Asymmetric). Hash Functions (MD5, SHA, Whirlpool) & Uses. PKI components (CA, RA). Authentication vs. Authorization.	UNCITRAL Model Law: 1996.
Law & Crimes	**IT Act Sections** 43 (Compensation/Civil), 66 (Offense/Criminal), 66B-E. Cyber crime classifications (Individual, Property, Org, Society). Section 75 (Jurisdiction outside India).	CDA (USA): 1996. CIPA (USA): 2000.
IPR	**7 Forms of IPR**. Copyright duration (60 years). Trademark duration (10 years, renewable). Berne Convention Principles. Deep linking, in-lining, framing differences.	Berne Convention: 1886. Copyright Act: 1957. Patents Act: 1970. Trade Marks Act: 1999.
Forensics	Digital Forensic **5 Phases** (Policy, Assessment, Acquisition, Examination, Reporting). Cyber Forensic Techniques.	

Study Tips for Exam Success:

- Focus on **definitions and key differences** (e.g., Symmetric vs. Asymmetric encryption).
- Memorize acronyms: DES, RSA, PKI, PRNG, UNCITRAL, TRIPS, GI.
- Know the specific section numbers for IT Act penalties and offenses (e.g., Sec 43 vs. Sec 66).
- Understand the flow from **threat $\rightarrow$ protection $\rightarrow$ law $\rightarrow$ remedy**.
- Know the duration periods for key IPR types (Copyright 60 years, Trademark 10 years).