UNIVERSITY CORE CURATED FRAMEWORK

MODULE 4: CYBER LAW & INTELLECTUAL PROPERTY RIGHTS

Calicut University • B.Com Semester III • Business Regulations Infrastructure

15. INTRODUCTION TO INDIAN CYBER LAW

The Evolution and Need for Cyber Regulations

Traditional mercantile laws (like the Indian Penal Code, 1860 or the Indian Evidence Act, 1872) were constructed entirely around tangible objects, physical handshakes, and geographic boundaries. The rapid rise of the internet exploded those concepts, creating a completely borderless digital ecosystem known as cyberspace. Because physical laws cannot easily govern virtual data, a specialized branch of jurisprudence was required: **Cyber Law**. In India, this system is anchored by **The Information Technology (IT) Act, 2000**, which was enacted on **17 October 2000** as the primary legislative pillar for digital oversight.

Primary Objectives of the IT Act, 2000

The act was introduced with specific operational objectives designed to validate and safeguard digital trade:

- **Legal Recognition of E-Commerce:** Replaces the mandatory paper-based filing rules with explicit validation for electronic data storage and communication transactions.
- **Filing and Digital Interfacing:** Authorizes government agencies to legally accept digital document submissions, applications, payments, and statutory receipts.
- **Banking and Record Upkeep:** Provides a regulatory framework to validate electronic fund transfers (EFTs) and electronic books of accounts for commercial banks under the Bankers' Books Evidence Act.

🌐 International Alignment The IT Act, 2000 is directly modeled after the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996, aligning Indian digital infrastructure with international trade rules.

16. E-COMMERCE, DIGITAL SIGNATURES & ELECTRONIC CONTRACTS

Legal Recognition of Electronic Contracts

Under **Section 10A** of the IT Act, electronic contracts are granted full legal validity and parity with traditional paper contracts. A contract cannot be denied enforceability or validity simply because electronic communications (such as emails, digital forms, or click-wrap agreements) were used to convey the offer, acceptance, or modifications.

The Cryptographic Matrix: Digital vs. Electronic Signatures

While terms are frequently mixed up in everyday conversation, the Act draws a strict technical and legal line between these two validation methods:

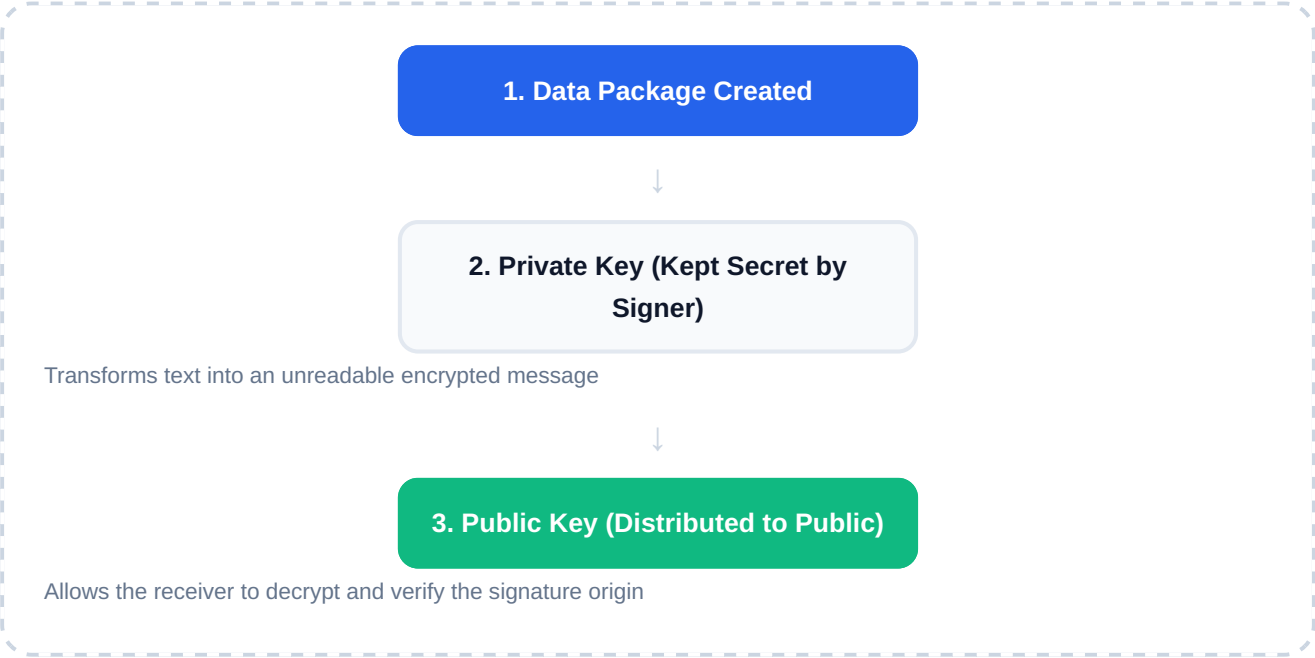
Analytical Dimension	Digital Signature Framework (Sec. 2(1)(p))	Electronic Signature Umbrella (Sec. 3A)
Technical Definition	A secure authentication layer built on an Asymmetric Crypto-system and a mathematical Hash Function.	A broad legal category representing any approved electronic authentication mechanism.
Architectural Scope	Highly specific math-based infrastructure using twin cryptographic keys (Public & Private).	Expansive class containing biometrics, Aadhaar OTPs, or digital signature methods alike.
Core Principle	Every digital signature is a valid electronic signature, but not every electronic signature qualifies as a digital signature.	Relies directly on official central government schedule approvals and standard verification updates.

The Asymmetric Key Architecture Mechanics

The digital signature framework utilizes two distinct, mathematically linked keys to secure data transmissions:

- **The Private Key:** Kept entirely secret, confidential, and secure by the signature owner. It runs through a hash function to transform plain text into an unreadable, encrypted message string.
- **The Public Key:** Distributed openly across public networks to anyone. It allows the recipient of a data packet to decrypt the message string and instantly verify the signature's origin and integrity.

Visual Framework: Asymmetric Crypto-System Flow



17. CYBER SPACE, CYBER CRIME AND ITS TYPES

Defining Cyberspace

Cyberspace is the virtual, borderless environment created by interconnected computer networks, servers, databases, and communication channels. Because it does not have physical boundaries, traditional territory-based enforcement mechanisms face significant challenges.

The Three-Tier Classification Taxonomy

Cyber crime refers to any unlawful activity where a computer or digital device acts either as the target of the attack or the primary tool used to commit the offense. These crimes are classified based on the intended target:

👤 Against Individuals

- **Cyber Stalking:** Harassing or monitoring an individual online continuously.
- **Phishing:** Using deceptive emails or fake websites to steal passwords and financial info.
- **Identity Theft:** Stealing personal details to impersonate someone for financial gain.

🏢 Against Property

- **Hacking:** Gaining unauthorized access to systems or private networks.
- **Malware Injection:** Deploying viruses or ransomware to damage data systems.
- **Intellectual Theft:** Stealing proprietary software source code illegally.

🏛️ Against Government

- **Cyber Terrorism:** Attacking critical infrastructure (like power grids or defense systems).
- **Website Defacement:** Hacking and altering official government portal landing pages.

18. PENALTIES AND OFFENCES (IT ACT, 2000)

Civil Penalties vs. Criminal Offences

The IT Act divides violations into two categories: civil wrongs that require financial compensation, and criminal offences that carry prison sentences and criminal fines.

Civil Violations and Damages (Section 43)

If a person accesses, downloads, damages, introduces a virus into, or disrupts a computer network without the owner's permission, they are liable under Section 43. The culprit must pay compensation for the full value of the damages to the affected party.

Primary Criminal Offences Matrix

Statutory Section	Nature of the Criminal Offence	Maximum Prescribed Punishment
Section 65	Intentionally tampering with or destroying computer source code documents required by law.	Imprisonment up to **3 years** or fine up to **₹2 Lakhs**, or both.
Section 66	Committing a dishonest or fraudulent cyber act outlined under Section 43 (Hacking/Identity Theft).	Imprisonment up to **3 years** or fine up to **₹5 Lakhs**, or both.
Section 66C	Fraudulently using another person's electronic signature, password, or unique identification feature.	Imprisonment up to **3 years** and a fine up to **₹1 Lakh**.
Section 66F	Engaging in **Cyber Terrorism** to threaten the unity, integrity, security, or sovereignty of India.	Mandatory **Life Imprisonment**.
Section 67	Publishing or transmitting obscene, explicit material in electronic form.	First conviction: Up to **3 years** in prison and fine up to **₹5 Lakhs**.

19. AN OVERVIEW OF INTELLECTUAL PROPERTY RIGHTS

The Rationale of Intellectual Property

Intellectual Property Rights (IPR) are legal frameworks designed to protect creations of the mind. They grant creators exclusive economic rights to use and commercialize their innovations, preventing unauthorized duplication and encouraging research and development.

The Four Essential Pillars of IPR Architecture

🎨 1. Copyright

Scope: Protects original literary, dramatic, musical, artistic, and cinematograph works.
Software Value: In India, computer software source codes are protected as literary works under the Copyright Act, 1957.
Duration: Lifetime of the author plus **60 years**.

🔬 2. Patents

Scope: Protects new, non-obvious industrial inventions that are capable of practical application.
Nature: Grants an exclusive right to manufacture, use, or sell the patented invention, preventing market competitors from copying it.
Duration: Strictly limited to **20 years**.

🏷️ 3. Trademarks

Scope: Protects unique symbols, logos, brand names, or slogans used to distinguish products or services in the marketplace.
Value: Guards corporate brand equity and protects consumers from deceptive lookalike brands.
Duration: Valid for **10 years**, with unlimited renewals allowed.

📍 4. Geographical Indications

Scope: Identifies products that originate from a specific geographic location and possess qualities or a reputation unique to that region.
Examples: Darjeeling Tea, Aranmula Kannadi, Basmati Rice, Palakkadan Matta Rice.
Duration: Valid for **10 years**, with renewals allowed.

Summary Matrix: Cyber Law and IPR Integration

Digital Security Layer (IT Act)

Provides legal validity for digital commerce, verifies transactions via asymmetric public/private keys, and establishes clear penalties for unauthorized access, malware deployment, or system data breaches.

Intellectual Asset Layer (IPR)

Protects software source codes under copyright law, safeguards hardware innovations with utility patents, and preserves business brand equity through trademark registration frameworks.