DegreeLive

BBA	SEMESTER I	UNIVERSITY OF KERALA	COURSE CODE: UK1DSCMGT103

E-COMMERCE AND CYBER LAW

EXAM REVISION NOTES

JOIN WHATSAPP CHANNEL →

MODULE I

FOUNDATIONS OF E-COMMERCE AND DIGITAL BUSINESS ARCHITECTURE

Internet Infrastructure and Protocol Foundations: Decentralized packet-switched network operating on the foundational TCP/IP protocol suite:

- **TCP/IP Protocol Suite:** TCP provides reliable connection-oriented packet sequencing and retransmission; IP handles 32-bit (IPv4) and 128-bit (IPv6) logical addressing and routing; HTTPS provides TLS 1.3 encrypted browser sessions on port 443; DNS maps human-readable domains to machine IP addresses.
- **N-Tier Microservices Architecture:** Presentation Layer (React, Next.js), Edge CDN caching, API Gateways, autonomous decoupled microservices (catalog, cart, payments), and distributed SQL/NoSQL databases.
- **Headless Commerce & MACH Principles:** Decoupling frontend presentation from backend commerce engines communicating via APIs; Microservices, API-first, Cloud-native, and Headless architectures.
- **Traditional Commerce vs E-Commerce:** Traditional is localized, bound by business hours, high real-estate overhead, physical tactile inspection, and multi-layered intermediaries; E-Commerce offers global borderless reach, 24/7 availability, low physical overhead, automated warehousing, and disintermediation.
- **Electronic Data Interchange (EDI):** Computer-to-computer structured B2B document exchange using ANSI X12 and UN/EDIFACT standards, transmitted securely over public Internet via AS2 protocols.

E-Commerce Business Models and Organizational Taxonomy: Classification by participating economic entities:

- **Business-to-Business (B2B):** Accounts for over 80% of global transaction value; bulk order volumes, complex contract negotiation, negotiated credit payment terms (IndiaMART, Udaan, Alibaba).
- **Business-to-Consumer (B2C):** High frequency, smaller basket sizes; Marketplace model (neutral platform charging seller commission with zero inventory risk) vs Inventory-Led model (platform buys and stocks goods, prohibited under 100% Indian FDI retail rules).
- **Direct-to-Consumer (D2C):** Brand manufacturers bypassing retail middlemen to sell directly to consumers via proprietary webstores (Mamaearth, boAt), retaining 100% customer data and margins.
- **Consumer-to-Consumer (C2C) & C2B:** Peer-to-peer trading platforms (OLX, eBay classifieds) vs freelance and influencer creative monetization portals (Upwork, Fiverr).
- **Open Network for Digital Commerce (ONDC):** Open, unbundled network initiative by Government of India democratizing e-commerce by connecting independent buyer apps, seller apps, and logistics providers without central platform lock-in.

Digital Marketing Mechanics and Emerging Retail Paradigms: Customer acquisition and conversion engineering:

- **SEO vs SEM:** SEO is organic optimization of meta tags, page speed, structured data, and backlink authority; SEM is paid pay-per-click (PPC) keyword bidding auctions (Google Ads) with immediate search visibility.
- **Programmatic Advertising Ecosystem:** Real-Time Bidding (RTB) auctions executing in milliseconds via Demand-Side Platforms (DSPs), Supply-Side Platforms (SSPs), and Ad Exchanges; evaluated by CTR, CPM, CAC, and ROAS.
- **Customer Retention & RFM Modeling:** RFM customer segmentation evaluates Recency (time since last purchase), Frequency (purchase cadence), and Monetary Value (total spend) to maximize Customer Lifetime Value (CLV).
- **Quick Commerce and Dark Stores:** 10-to-15 minute grocery fulfillment using micro-warehouses (dark stores) within a 2-3 km urban radius stocking 3,000-5,000 fast-moving SKUs.
- **Omnichannel Integration:** Buy Online Pick Up In Store (BOPIS), ship-from-store inventory routing, harmonizing Showrooming (inspecting in store, buying online) and Webrooming (researching online, buying in store).
- **Chris Anderson's Long Tail Theory:** Infinite digital shelf space allows platforms to monetize millions of obscure, niche products whose aggregate revenue equals or surpasses blockbuster hits.
- **Digital Auction Dynamics:** English auctions (open ascending bids); Dutch auctions (descending price clock until bidder accepts); Sealed-bid second-price Vickrey auctions (highest bidder wins but pays second-highest bid); Reverse auctions (suppliers submit descending bids to win institutional procurement contracts).
- **E-Commerce Supply Chain & Reverse Logistics:** Drop-shipping models (merchant transfers orders to third-party supplier who ships directly to consumer without merchant holding stock); Cross-docking in automated fulfillment centers; Return to Origin (RTO) minimization via automated address validation, cash-on-delivery (COD) risk scoring, and reverse tracking.

MODULE II

ELECTRONIC PAYMENT SYSTEMS AND DIGITAL BANKING INFRASTRUCTURE

Digital Banking Architecture and Core Banking Solutions (CBS): Centralized real-time networking of bank ledgers:

- **Core Banking Solution (CBS):** Customer accounts are unified across all channels (Finacle, BaNCS); customer belongs to the entire bank rather than a specific physical branch.
- **Defense-in-Depth Security Layers:** TLS 1.3 browser encryption, mandatory Two-Factor Authentication (2FA / AFA), virtual keyboards preventing keylogger spyware, and real-time behavioral fraud scoring.
- **Payment and Settlement Systems Act 2007 (PSSA):** Designated RBI as supreme regulatory authority over payment systems; Section 23 grants absolute legal finality to netting and settlement operations.
- **Electronic Payment System (EPS) Requirements:** Confidentiality, data integrity, authentication, non-repudiation, high scalability, and low merchant discount rates (MDR).

Digital Cash, E-Wallets, and Pre-Paid Payment Instruments (PPIs): Tokenized stored-value payment mechanisms:

- **Central Bank Digital Currency (CBDC):** Sovereign legal tender issued directly on central bank digital ledgers (RBI Digital Rupee e-Rupee); direct central bank liability, non-interest bearing, offering peer-to-peer offline settlement.
- **RBI PPI Classification:** Closed System PPIs (usable only at issuing merchant, e.g., brand gift cards, no license needed); Semi-Closed PPIs (usable across contracted merchant networks, cash withdrawal barred, e.g., Paytm Wallet); Open System PPIs (issued only by commercial banks, usable everywhere including ATM cash withdrawals).
- **Buy Now Pay Later (BNPL):** Point-of-sale micro-credit underwriting at checkout splitting payments into interest-free installments, financed by higher merchant discount rates.
- **Account Aggregator (AA) Framework:** Consent-based financial data sharing connecting Financial Information Providers (banks) with Financial Information Users (fintech lenders) via data-blind NBFC-AAs.

Card-Based Payment Architecture and Payment Gateways: Global payment rail mechanics:

DegreeLive

- **Card Taxonomy:** Debit cards (pay now from demand deposits); Credit cards (pay later against revolving lines of credit); EMV Chip Cards (microprocessors generating dynamic single-use cryptographic cryptograms, eliminating magstripe cloning); Contactless NFC cards (13.56 MHz RFID tap-and-pay).
- **Card-on-File Tokenization (CoFT):** RBI mandate prohibiting merchants from storing raw 16-digit card numbers; converted into merchant-specific randomized cryptographic tokens immune to merchant database leaks.
- **Payment Gateway Four-Party Model:** Customer submits checkout data → Gateway encrypts and routes to Acquiring Bank → Acquiring Bank routes to Card Network (Visa/Mastercard/RuPay) → Issuing Bank validates balance, fraud score, and 3D-Secure OTP → Settlement executes at day-close minus MDR.
- **Chargeback Dispute Lifecycle:** Disputed transactions charged back to merchants; resolved via representment evidence (courier delivery proofs, verified 3D-Secure IP logs) under card network arbitration.

Interbank Clearing Networks and the UPI Revolution: National payments infrastructure:

- **Interbank Clearing Systems:** NEFT (24/7 half-hourly deferred net settlement batches); RTGS (continuous gross transaction-by-transaction settlement for high-value > INR 2 Lakh transfers); IMPS (instant 24/7 retail fund transfers up to INR 5 Lakh); NACH (bulk recurring corporate salary and dividend clearing); National Financial Switch (NFS interconnecting 260,000 ATMs); Bharat Bill Payment System (BBPS standardized utility bill collection).
- **Unified Payments Interface (UPI - NPCI):** Built on IMPS rails; Virtual Payment Address (VPA / UPI ID) acting as an abstract financial alias eliminating exposure of bank account numbers; single-click mobile 2FA (SIM device binding + UPI PIN); Bharat QR and dynamic QR code standards; 3-tier open API architecture (NPCI Switch + Bank PSPs + Third-Party Apps like PhonePe, Google Pay).
- **Cross-Border Settlement:** SWIFT network transmitting standardized financial messages (MT103, ISO 20022) across bilateral Nostro/Vostro correspondent banking accounts.
- **Payment Card Industry Data Security Standard (PCI-DSS):** 12 baseline security mandates including firewall configuration, rendering cardholder data unreadable via AES-256 encryption at rest and TLS in transit, strict role-based access control, quarterly vulnerability scans, and comprehensive audit logs.
- **3D Secure 2.0 & Risk-Based Authentication:** Evaluates over 100 contextual risk parameters (device fingerprint, geolocation, transaction velocity, IP reputation) to enable frictionless checkout for low-risk purchases while reserving biometric/OTP challenges strictly for elevated risk profiles.

MODULE III

CYBER LAW FRAMEWORKS AND INTELLECTUAL PROPERTY RIGHTS

Cyber Law Genesis and Jurisdictional Dilemmas: Regulating the non-physical, decentralized digital realm:

- **Jurisdictional Breakdown:** Cyberspace transcends traditional territorial sovereignty; conflicts resolved via Extraterritorial Jurisdiction, the Effects Doctrine (adjudicating foreign actions causing domestic harm), and the Zippo sliding scale test of website interactivity.
- **UNCITRAL Model Laws:** UNCITRAL Model Law on Electronic Commerce (1996) establishing Non-Discrimination (electronic records carry full legal validity) and Functional Equivalence (electronic messages fulfill writing and signature functions); Model Law on Electronic Signatures (2001).
- **Digital Taxation & Equalisation Levy:** India's Equalisation Levy (6% on digital advertising, 2% on foreign e-commerce supply) overcoming obsolete physical Permanent Establishment rules; OECD BEPS Pillar One and Pillar Two (15% global minimum corporate tax).

Consumer Protection, Data Sovereignty, and Privacy Rights: Safeguarding public welfare in digital commerce:

- **Consumer Protection (E-Commerce) Rules 2020:** Mandatory disclosure of seller entities and country of origin; statutory ban on unfair trade practices and dark patterns; fall-back liability on marketplace platforms if third-party sellers fail to deliver; resident grievance officers.
- **Right to Privacy (Puttaswamy 2017 Ruling):** Nine-judge constitutional bench declared privacy a fundamental right under Article 21; protects informational privacy and personal data autonomy.
- **Data Protection Principles (DPDP Act 2023 / GDPR):** Notice and explicit consent; Purpose limitation; Data minimization; Storage limitation; Robust security safeguards; Rights of data principals (access, correction, erasure); Significant Data Fiduciaries (SDFs) and Data Protection Board of India penalties up to INR 250 Crores.
- **Cookie Governance:** Strictly necessary session cookies vs persistent third-party tracking cookies; mandatory upfront cookie consent banners and anti-tracking rights.

Intellectual Property Rights and Domain Name Disputes: Intangible digital asset protection:

- **Digital Copyright & Software Protection:** Computer programs protected as literary works under Copyright Act 1957; Idea-Expression dichotomy (expression protected, algorithms not); Digital Rights Management (DRM) and criminal penalties for circumventing technological protection measures (Sections 65A/65B).
- **Software Patentability under Section 3(k):** Indian Patents Act excludes computer programmes per se; patentable strictly if producing a tangible technical contribution or technical effect (Ferid Allani ruling).
- **Online Trademark Conflicts:** Prohibiting hidden metatag stuffing, trademark keyword bidding causing confusion, deep linking, and framing.
- **Domain Name Piracy:** Cybersquatting (bad-faith registration of famous brand domains to sell for extortionate profit) vs Typosquatting (registering common misspellings to harvest traffic); resolved via ICANN Uniform Domain Name Dispute Resolution Policy (UDRP) administered by WIPO arbitration, and INDRP in India; Satyam Infoway v. Sifynet confirmed domain names carry full trademark rights.
- **Digital Millennium Copyright Act (DMCA) & Safe Harbor:** Section 512 notice-and-takedown safe harbor immunizing service providers from copyright damages upon prompt removal of infringing material; matched by Section 52(1)(c) transient storage safe harbor under Indian Copyright Act.
- **Cross-Border Data Sovereignty & Localization:** RBI 2018 payment data storage directive mandating entire end-to-end payment chain data reside solely on domestic Indian servers; DPDP Act 2023 black-listing model for international data transfer jurisdictions.
- **Taxonomy of Cyber Threats:** Computer viruses and self-replicating network worms; Trojan horses and keylogger spyware; Ransomware (asymmetric encryption demanding cryptocurrency); Phishing, Smishing, and Vishing social engineering; Distributed Denial of Service (DDoS) botnets; Generative AI Deepfakes (criminalized under Sections 66D, 66E, and defamation).

MODULE IV

CYBER SECURITY ARCHITECTURE, CRYPTOGRAPHY AND DEFENSIVE CONTROLS

Information Security Fundamentals and Identity Governance: Safeguarding corporate digital assets:

- **The CIA Triad:** Confidentiality (preventing unauthorized data disclosure via encryption); Integrity (preventing unauthorized modification via hash functions); Availability (ensuring uninterrupted access via redundancy and DDoS defense); Non-repudiation (guaranteeing proof of origin).
- **Identity and Access Management (IAM):** Multi-Factor Authentication (something you know, have, and are); emerging FIDO2/WebAuthn passwordless passkeys; Role-Based Access Control (RBAC); Principle of Least Privilege (PoLP).

Cryptography and Mathematical Ciphers: Transforming plaintext into secure ciphertext:

- **Symmetric vs Asymmetric Cryptography:** Symmetric uses a single shared secret key (AES-256, ultra-fast for bulk data); Asymmetric uses mathematically linked public/private key pairs (RSA-2048, Diffie-Hellman, ECC; slower, solves key distribution).
- **Cryptographic Hash Functions:** Deterministic one-way mathematical compression (SHA-256 Merkle-Damgard 64-round compression); pre-image resistance, second pre-image resistance, collision resistance, and avalanche effect; MD5 and SHA-1 deprecated due to collision flaws.
- **Digital Signature Mechanics:** Signer computes SHA-256 message digest of document → encrypts digest using strictly confidential Private Key to create Digital Signature → Recipient decrypts signature using sender's Public Key → compares recovered digest with freshly computed digest; verified match proves authentic authorship and document integrity.
- **End-to-End Encryption (E2EE):** Double Ratchet Algorithm combining Symmetric-key and Diffie-Hellman ratchets, providing Forward Secrecy and Post-Compromise Security.

Public Key Infrastructure (PKI) and Certifying Authorities: Institutional framework for digital trust:

- **Digital Signature Certificates (DSC):** X.509 standardized electronic credential issued by licensed CAs legally binding an individual's identity to their public key.
- **Regulatory Hierarchy under IT Act:** Controller of Certifying Authorities (CCA) holds National Root Key and licenses Certifying Authorities (eMudhra, NIC, NSDL); CAs issue DSCs to subscribers; revocation managed via Certificate Revocation Lists (CRL) and real-time OCSP protocols.
- **Key Management Lifecycle:** NIST SP 800-57 guidelines for key generation using hardware entropy, Hardware Security Modules (HSMs with physical zeroization), scheduled rotation, and cryptographic shredding.

Network Defense Systems and Defensive Architecture: Multi-layered enterprise perimeter protection:

- **Firewalls:** Packet-filtering firewalls (inspecting IP/port headers at Layers 3/4); Stateful inspection firewalls (tracking active TCP connection handshakes); Next-Generation Firewalls - NGFW (Deep Packet Inspection up to Layer 7 with integrated IPS).
- **Defensive Systems:** Intrusion Detection and Prevention Systems (IDS/IPS); Endpoint Detection and Response (EDR) software; Security Operations Centers (SOC) utilizing SIEM platforms (Splunk) and automated SOAR response playbooks; Air-gapped networks and hardware data diodes enforcing unidirectional physical transmission.
- **Zero-Trust Architecture (ZTA):** "Never Trust, Always Verify"; eliminating obsolete perimeter castle-and-moat models through micro-segmentation and continuous context-aware authentication.
- **Post-Quantum Cryptography (PQC):** Developing lattice-based algorithms (CRYSTALS-Kyber) to resist Shor's quantum computing algorithm threatening to break RSA and ECC.
- **OWASP Top 10 Web Vulnerabilities:** Preventing SQL Injection (parameterized queries), Cross-Site Scripting (XSS input sanitization), and Cross-Site Request Forgery (anti-CSRF tokens).
- **Cryptographic Attack Vectors & Mitigations:** Replay attacks countered by unique cryptographic nonces and monotonically increasing timestamps; Man-in-the-Middle (MitM) attacks neutralized by X.509 certificate chains and Public Key Pinning; Birthday attacks on hash functions countered by expanding digest length (SHA-256 offering 128-bit collision resistance).
- **Disaster Recovery & Business Continuity:** Recovery Point Objective (RPO specifying tolerable data loss duration) and Recovery Time Objective (RTO specifying maximum acceptable system restoration downtime); 3-2-1 backup topology (3 data copies across 2 distinct media types with 1 copy held air-gapped offsite).

MODULE V

CYBER REGULATIONS, INFORMATION TECHNOLOGY ACT AND DIGITAL FORENSICS

Information Technology Act, 2000 Overview and Scope: India's foundational cyber statute:

- **Legislative Scope:** Enacted October 17, 2000; provides legal recognition for e-commerce, electronic records, electronic signatures, and e-governance; 2008 amendments introduced electronic signatures, cyber terrorism, and CERT-In.
- **Extraterritorial Jurisdiction (Section 75):** Act applies to any person committing cyber offenses anywhere in the world provided the offense involves a computer system located within India.
- **Electronic Records & Governance (Sections 4-10A):** Section 4 (legal recognition of electronic records); Section 5 (legal recognition of electronic signatures); Section 10A (validity of contracts formed electronically).
- **Online Contract Mechanics (Sections 11-13):** Section 11 (attribution of electronic records); Section 12 (acknowledgment of receipt); Section 13 (dispatch occurs when record leaves originator's control; receipt occurs at addressee's principal place of business).

Cyber Crimes, Penalties, and Landmark Judicial Rulings: Criminal offenses and statutory punishments:

- **Key Penal Provisions:** Section 43 (civil compensation for unauthorized data copying, virus injection); Section 65 (tampering with computer source code); Section 66 (hacking); Section 66C (identity theft, password stealing); Section 66D (cheating by personation); Section 66E (privacy violation); Section 66F (Cyber Terrorism - punishable with **Imprisonment for Life**); Section 67/67A/67B (obscenity, sexually explicit content, child sexual abuse material).
- **Shreya Singhal Landmark Ruling (2015):** Supreme Court struck down Section 66A in its entirety as unconstitutional violation of Article 19(1)(a) freedom of speech, declaring it unconstitutionally vague and overbroad.
- **Bail and Compoundability (Section 77B):** Offenses punishable with 3 years or less are bailable as of right; offenses exceeding 3 years (cyber terrorism, repeat child pornography) are non-bailable.

DegreeLive

- **Adjudication Hierarchy:** IT Secretaries appointed as Adjudicating Officers with civil court powers under Section 46; appeals heard by Telecom Disputes Settlement and Appellate Tribunal (TDSAT) under Section 57.

Intermediary Liability and the Section 79 Safe Harbor: Immunity and due diligence obligations:

- **Section 79 Safe Harbor:** Intermediaries (telecoms, social media, marketplaces) are exempt from liability for third-party user content provided they act as neutral pipelines, do not modify content, and observe statutory due diligence.
- **Intermediary Guidelines 2021:** Notice-and-takedown within 36 hours upon court order or government notice; Significant Social Media Intermediaries (SSMIs) must appoint resident Chief Compliance Officers, Nodal Officers, and Grievance Officers.
- **Critical Information Infrastructure (CII):** Section 70 empowers Central Government to declare critical computer resources; protected by NCIIPC; hacking CII attracts up to 10 years imprisonment.
- **CERT-In Directives 2022:** Mandatory 6-hour reporting of cyber security incidents to CERT-In; mandatory 180-day system log retention within Indian jurisdiction; NTP time server synchronization.

Cyber Forensics and Electronic Evidence Admissibility: Scientific investigation and courtroom proof:

- **Forensic Investigation Stages:** (1) Securing scene and placing mobile devices in Faraday bags; (2) Preserving volatile memory (RAM) following the Order of Volatility; (3) Creating forensic bit-stream duplicate images using hardware Write-Blockers (never examining original media); (4) Cryptographic hash verification (SHA-256 byte-exact match); (5) Analysis via EnCase/Autopsy; (6) Meticulous Chain of Custody documentation.
- **Mobile Device Extraction:** Logical extraction (OS APIs), file system extraction, and physical raw NAND flash memory carving; SQLite database parsing for deleted WhatsApp/Signal chat records.
- **Section 65B Indian Evidence Act Admissibility:** Section 65B(4) written certificate is a **mandatory condition precedent** for the admissibility of any secondary electronic evidence (printouts, CDs, hard drive copies), conclusively established by the Supreme Court three-judge bench in *Arjun Panditrao Khotkar (2020)*.
- **Four Statutory Conditions of Section 65B(2):** (a) Computer output produced during regular operational use; (b) Information fed into computer in ordinary course of activities; (c) Computer operating properly throughout the period without material malfunction; (d) Duplicate accurately reproduces original electronic data.
- **Digital Forensic Toolkits:** Hardware write-blockers (Tableau, WiebeTech) preventing write-signals to suspect drives; FTK Imager for bit-stream disk imaging; Volatility framework for volatility carving in volatile RAM dumps; Autopsy and The Sleuth Kit for unallocated cluster and file slack recovery.
- **International Cooperation:** Budapest Convention on Cybercrime 2001 and Mutual Legal Assistance Treaties (MLATs) for cross-border evidentiary seizure.

DegreeLive