DegreeLive

BBA | Semester I | UK1DSCMGT103

E-Commerce and Cyber Law

Course Code: UK1DSCMGT103 • Module 4 Notes

Module IV: Cyber Security Architecture, Cryptography and Defensive Controls

1. Foundational Information Security Principles: The CIA Triad and Beyond

In modern e-commerce and networked computing, information is a vital strategic asset. Information Security (InfoSec) is formally defined as the practice of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Enterprise cyber security architectures are anchored upon the classic **CIA Triad**, augmented by essential governance principles:

- **Confidentiality:** Ensuring that sensitive electronic information is accessible strictly to authorized individuals, entities, or processes. Confidentiality prevents unauthorized disclosure of proprietary commercial data, trade secrets, consumer passwords, and payment card numbers. Technical mechanisms include symmetric/asymmetric data encryption, strict access control lists (ACLs), and data classification policies.
- **Integrity:** Protecting the accuracy, completeness, and authenticity of data and software from unauthorized modification, deletion, or tampering in storage or transit. If a cyber criminal intercepts a digital banking transfer and alters the beneficiary account number or monetary value, data integrity is compromised. Technical mechanisms include cryptographic hash functions (SHA-256), message authentication codes (MAC), and digital signatures.
- **Availability:** Ensuring that authorized users possess timely, reliable, uninterrupted access to critical information assets, e-commerce webstores, and cloud databases whenever required. A business with perfect confidentiality is economically useless if a Distributed Denial of Service (DDoS) attack shuts down its customer checkout portals. Technical mechanisms include fault-tolerant hardware clustering, redundant cloud availability zones, automated data backups, and high-capacity network bandwidth.
- **Non-Repudiation:** Guaranteeing that a party to an electronic communication or financial transaction cannot subsequently deny having authored, signed, or transmitted the message. Achieved through asymmetric digital signatures combined with trusted timestamping authorities.
- **Authentication and Authorization:** *Authentication* is the rigorous process of verifying the claimed identity of a user, device, or system. *Authorization* is the subsequent process of determining whether an authenticated entity possesses the legitimate permissions and rights to access specific files, databases, or administrative commands.
- **Accountability and Auditability:** Maintaining immutable chronological audit trails and system event logs (SIEM) recording every user login, administrative modification, and data query, enabling post-incident forensic attribution.

Degreelive

2. Identity and Access Management (IAM): Multi-Factor Authentication and Access Controls

Identity and Access Management (IAM) represents the security framework that governs digital identities, ensuring appropriate users gain timely access to enterprise technology resources while preventing unauthorized intrusion.

A. Multi-Factor Authentication (MFA) and Modern Passwordless Paradigms

Traditional single-factor authentication relying exclusively on memorized alphanumeric passwords is systematically broken due to human password reuse, credential stuffing attacks, and phishing. Multi-Factor Authentication enforces verification across at least two independent, distinct authentication factors:

- **Knowledge Factor (Something You Know):** Passwords, PINs, security passphrases, answers to secret questions.
- **Possession Factor (Something You Have):** Physical cryptographic hardware security keys (YubiKey), Time-based One-Time Password (TOTP) authenticator apps (Google Authenticator, Microsoft Authenticator), SIM card mobile devices receiving cryptographic push prompts, smart cards.
- **Inherence Factor (Something You Are):** Physiological and behavioral biometrics, including capacitive fingerprint scanning, 3D infrared facial recognition, iris scanning, and keystroke dynamics.
- **Emerging FIDO2 / WebAuthn Standards:** Replacing passwords entirely with public-key cryptography and device-bound passkeys. The user authenticates locally to their hardware device (via fingerprint or biometric face scan); the device securely signs an asymmetric cryptographic challenge from the relying web server, eliminating phishing risks.

B. Enterprise Access Control Models

- **Role-Based Access Control (RBAC):** Access permissions are assigned to specific organizational roles (e.g., Marketing Associate, Database Administrator, Billing Specialist) rather than individual employees. When an employee changes jobs or resigns, updating their role automatically reconfigures their system permissions, eliminating orphan privileges.
- **Discretionary Access Control (DAC):** The creator or owner of a file possesses personal discretion to grant read, write, or execute access permissions to other users (common in standard desktop operating systems).
- **Mandatory Access Control (MAC):** Centralized security policy where access is governed by formal security classifications (Confidential, Secret, Top Secret). Operating systems evaluate user clearance levels against object security labels, preventing unauthorized data exfiltration.
- **Principle of Least Privilege (PoLP):** A fundamental security paradigm dictating that every user, software process, or program must be granted strictly the absolute minimum permissions and access rights necessary to perform its legitimate functional tasks, minimizing the potential blast radius of compromised credentials.

DegreeLive

3. Cryptography: Symmetric vs Asymmetric Cryptographic Systems

Cryptography (derived from the Greek *kryptos*, meaning "hidden," and *graphein*, meaning "to write") is the mathematical science of transforming human-readable information (Plaintext) into unintelligible secret code (Ciphertext) using algorithmic mathematical functions and secret keys, and reversing the process through Decryption.

Cryptographic Dimension	Symmetric Key Cryptography (Secret-Key)	Asymmetric Key Cryptography (Public-Key)
Key Architecture	Uses a **single, identical shared secret key** for both encryption and decryption.	Uses a mathematically linked **asymmetric key pair**: a Public Key (freely distributed) and a Private Key (kept strictly confidential).
Computational Speed	Extremely fast and computationally lightweight; processes gigabytes of data per second with minimal CPU overhead.	Computationally slow and resource-intensive; requires complex modular exponentiation and large prime factoring.
Primary Use Case	Bulk data encryption (encrypting hard disk drives, databases, file systems, and active network payloads).	Key exchange protocols, digital signatures, identity authentication, and secure session handshakes.
Key Distribution Problem	Severe: How do two parties exchange the secret key over an insecure network without an eavesdropper intercepting it?	Solved: Public keys are published openly; private keys never leave the owner's secure cryptographic module.
Prominent Algorithms	AES (Advanced Encryption Standard - 128, 192, 256-bit keys), DES (obsolete), Triple-DES (3DES), ChaCha20.	RSA (Rivest-Shamir-Adleman - 2048, 4096-bit), Diffie-Hellman (DH), Elliptic Curve Cryptography (ECC), Ed25519.

A. Advanced Encryption Standard (AES)

Established by the U.S. National Institute of Standards and Technology (NIST) in 2001 to replace the vulnerable Data Encryption Standard (DES), AES is a symmetric block cipher that processes 128-bit blocks of data using substitution-permutation networks across 10 rounds (128-bit keys), 12 rounds (192-bit keys), or 14 rounds (256-bit keys). AES-256 is globally recognized as the gold standard for securing enterprise databases, cloud storage, and government classified communications; an exhaustive brute-force attack would require billions of years using modern supercomputers.

B. Asymmetric Cryptography: The RSA Algorithm and Diffie-Hellman

- **The RSA Algorithm (Rivest, Shamir, Adleman - 1977):** Derives its cryptographic strength from the extreme mathematical difficulty of factoring the product of two colossal prime numbers (the Integer Factorization Problem). If Alice wishes to send an encrypted message to Bob, Alice encrypts the plaintext using *Bob's Public Key*. Only Bob, possessing the mathematically linked *Bob's Private Key*, can decrypt and read the ciphertext.
- **Diffie-Hellman Key Exchange (DH):** A breakthrough protocol allowing two parties who have no prior knowledge of each other to establish a shared secret key over an unsecure public

communications channel using discrete logarithms in cyclic groups, forming the technical foundation for modern SSL/TLS handshakes.

- **Hybrid Cryptography:** Practical secure web protocols (HTTPS / TLS 1.3) integrate both paradigms: asymmetric cryptography (RSA or ECC) is deployed during the initial handshake to authenticate server identity and securely negotiate a temporary single-use symmetric session key; subsequent bulk web page data and payment payloads are encrypted using ultra-fast symmetric AES-256.

4. Cryptographic Hash Functions, Message Digests, and Digital Signatures

To verify data integrity and establish legal non-repudiation in e-commerce, cryptographers deploy one-way mathematical functions.

A. Cryptographic Hash Functions

A Cryptographic Hash Function is a deterministic mathematical algorithm that takes an arbitrary-length digital input (a single word, an email, or a 10-gigabyte database file) and computes a fixed-length numerical output string termed a **Hash Value** or **Message Digest**. A robust cryptographic hash function must satisfy three non-negotiable security properties:

- **Pre-Image Resistance (One-Way Property):** Computationally infeasible to reverse the process; given a hash value h, it is impossible to calculate the original input message m such that $hash(m) = h$.
- **Second Pre-Image Resistance (Weak Collision Resistance):** Given an input m_1, it is computationally impossible to find a different input m_2 such that $hash(m_1) = hash(m_2)$.
- **Collision Resistance (Strong Collision Resistance):** Computationally infeasible to find any two arbitrary, distinct input messages that produce the identical hash output. (MD5 and SHA-1 were broken due to collision vulnerabilities; modern security relies strictly on **SHA-256 and SHA-3**).
- **Avalanche Effect:** Changing even a single bit in the input message (e.g., changing a single comma to a period) causes the resulting hash digest to change radically and unpredictably across over 50% of its bits.

B. The Architecture of Digital Signatures

A **Digital Signature** is a mathematical scheme for demonstrating the authenticity, message integrity, and non-repudiation of an electronic document. A digital signature is NOT a scanned graphic image of a handwritten signature pasted onto a PDF. Rather, it is a cryptographic computation linking a unique individual to an electronic record.

The digital signature creation and verification process executes in two distinct phases:

1. **Signing Process (Executed by Sender / Signer):**
   - The sender's software feeds the electronic document through a secure hash algorithm (SHA-256) to generate a unique, fixed-length 256-bit *Message Digest*.

- The sender's private software uses the sender's strictly confidential **Private Key** to encrypt this message digest. The resulting encrypted digest is the **Digital Signature**.
- The digital signature is appended to the original electronic document and transmitted to the recipient.

2. **Verification Process (Executed by Recipient / Relying Party):**
   - The recipient uses the identical hash algorithm (SHA-256) to compute a fresh message digest from the received document.
   - The recipient takes the attached digital signature and decrypts it using the sender's openly published **Public Key**, recovering the original message digest computed by the sender.
   - The recipient compares the two digests: if both digests match identically, it proves two absolute facts: (1) *Authenticity / Non-Repudiation:* The document was signed by the owner of the private key (since only the matching private key could create a signature readable by that public key); and (2) *Integrity:* The document was not altered or tampered with by a single character during transit (any alteration would produce a radically mismatched fresh hash digest).

5. Public Key Infrastructure (PKI) and Certifying Authorities

While asymmetric cryptography solves the key distribution problem, it introduces a dangerous vulnerability: the *Public Key Spoofing Problem*. How does Alice know that a public key published online under Bob's name genuinely belongs to Bob, and not to an imposter attacker conducting a man-in-the-middle attack? To establish trusted identity verification, cyberspace relies upon **Public Key Infrastructure (PKI)**.

A. Digital Signature Certificates (DSC) and X.509 Standards

A Digital Signature Certificate (DSC) is an electronic credential issued by a trusted third party that legally binds an individual's or organization's verified identity to their specific public key. Conforming to international ITU-T X.509 standards, a DSC contains: (1) Name of the certificate owner / subject; (2) Owner's public key; (3) Digital signature of the issuing Certifying Authority; (4) Serial number; (5) Validity time period; and (6) Permitted cryptographic usage algorithms.

B. The Regulatory Hierarchy under the Indian IT Act, 2000

The Information Technology Act, 2000 establishes a formal, multi-tiered statutory trust architecture for electronic governance in India:

- **Controller of Certifying Authorities (CCA):** Appointed by the Central Government under Section 17 of the IT Act, the CCA is the apex statutory regulatory authority overseeing the entire Indian PKI ecosystem. The CCA holds the National Root Key of India, issues electronic licenses to operational Certifying Authorities, establishes technical and security standards, and audits operational compliance.
- **Certifying Authorities (CAs):** Licensed commercial and governmental bodies authorized under Section 24 of the IT Act to issue Digital Signature Certificates to the public (e.g., eMudhra, National

Degreelive

Informatics Centre - NIC, NSDL, IDRBT). CAs verify the physical identity, government documents, and business charters of applicants before cryptographically signing their DSCs.

- **Registration Authorities (RAs):** Intermediary entities appointed by CAs to collect identity proofs, verify biometrics, and forward applications to CAs.
- **Subscribers:** The end individuals, corporate directors, or government officials to whom a Digital Signature Certificate is issued.
- **Certificate Lifecycle Management:** Includes certificate issuance, periodic renewal, and revocation. When a subscriber's private key is compromised, lost, or the employee leaves an organization, the CA must immediately revoke the certificate and publish its serial number to the public **Certificate Revocation List (CRL)** or provide real-time status through the **Online Certificate Status Protocol (OCSP)**, alerting relying systems to reject the compromised key.

6. Network Defense Architectures: Firewalls, EDR, and Zero-Trust Engineering

Securing enterprise e-commerce networks requires deploying defense-in-depth perimeter and internal network controls:

Defensive Technology	Operating Mechanics and Filtering Layer	Strategic Enterprise Role
Packet-Filtering Firewalls	Operates at the Network and Transport layers (OSI Layers 3 and 4), inspecting individual packet headers against static access rules based on source IP, destination IP, protocol (TCP/UDP), and destination port numbers.	Fast, low-cost baseline perimeter screening; incapable of inspecting packet payload contents.
Stateful Inspection Firewalls	Maintains an active state table tracking established, ongoing TCP communication sessions. Packets are evaluated not in isolation, but in the context of their verified connection handshake state.	Prevents unauthorized external incoming packet injection and spoofed port scans.
Next-Generation Firewalls (NGFW)	Integrates traditional stateful filtering with Deep Packet Inspection (DPI) up to the Application Layer (Layer 7), integrated Intrusion Prevention Systems (IPS), real-time SSL/TLS decryption inspection, and malware sandboxing.	Identifies and blocks advanced application-layer exploits, SQL injection, and unauthorized data exfiltration.
Intrusion Detection & Prevention (IDS / IPS)	Continuously monitors network traffic for suspicious anomalies and known exploit attack signatures. An *IDS* passively detects attacks and generates alerts; an *IPS* actively intercepts malicious traffic in-line, dropping packets and resetting connections.	Early warning detection of lateral threat movement and zero-day network exploitation.
Endpoint Detection and Response (EDR)	Software agents installed on all corporate laptops, mobile devices, and servers continuously logging file changes, registry	Replaces legacy signature-based antivirus, detecting

Defensive Technology	Operating Mechanics and Filtering Layer	Strategic Enterprise Role
	updates, process execution trees, and network sockets, utilizing behavioral AI to isolate compromised endpoints.	novel polymorphic ransomware attacks.

The Zero-Trust Architecture (ZTA) Paradigm

Historical enterprise security operated on the **Perimeter Security Model (Castle-and-Moat)**: everything inside the corporate internal corporate network was trusted by default, while everything outside on the public Internet was untrusted. Modern cloud architectures and remote working rendered this model obsolete; once an attacker breached the perimeter, they moved laterally across internal networks unimpeded.

Modern cyber security enforces the **Zero-Trust Architecture (NIST SP 800-207)**, governed by the foundational maxim: *"Never Trust, Always Verify."* Under zero trust: (1) All network traffic—internal and external—is treated as hostile; (2) Micro-segmentation divides networks into tiny isolated zones; (3) Identity and device health are authenticated and authorized dynamically for every individual transaction; and (4) Access is granted strictly via least-privilege context-aware policies.

In conclusion, cyber security architecture and cryptographic engineering form the indispensable technological foundation of e-commerce trust. By combining robust identity governance, mathematical cryptography, licensed public key infrastructures, and defense-in-depth zero-trust networks, digital enterprises protect national critical infrastructure and secure private commerce against relentless global cyber warfare.

7. Post-Quantum Cryptography (PQC) and the Quantum Threat

All modern asymmetric public-key cryptography (RSA, Diffie-Hellman, Elliptic Curve Cryptography) relies upon mathematical problems—namely, prime integer factorization and discrete logarithms—that are computationally impossible for classical binary supercomputers to solve. However, the emergence of **Quantum Computing** threatens to dismantle modern digital security.

In 1994, mathematician Peter Shor formulated **Shor's Algorithm**, proving that a sufficiently powerful fault-tolerant quantum computer utilizing quantum superposition and entanglement can solve prime factorization in polynomial time. A quantum computer could crack a 2048-bit RSA key in mere minutes, shattering global e-commerce security, banking handshakes, and blockchain ledgers. To combat this impending "Y2Q" quantum crisis, the National Institute of Standards and Technology (NIST) standardized **Post-Quantum Cryptography (PQC)** algorithms—such as *CRYSTALS-Kyber* (for general encryption) and *CRYSTALS-Dilithium* (for digital signatures)—which rely on complex lattice-based mathematical problems that resist both classical and quantum computing attacks.

8. Security Operations Centers (SOC) and SIEM Architecture

Modern enterprise cybersecurity is orchestrated through a centralized **Security Operations Center (SOC)**—a dedicated facility where cybersecurity analysts monitor, detect, analyze, and respond to cyber security incidents 24/7/365. The core technological engine of a SOC is the **Security**

Information and Event Management (SIEM) system (e.g., Splunk, IBM QRadar, Microsoft Sentinel):

- **Log Ingestion and Normalization:** SIEM collectors continuously ingest gigabytes of raw event logs per second from firewalls, network switches, web application servers, databases, and employee endpoints, converting disparate proprietary formats into structured records.
- **Correlation Rules and Behavioral Analytics:** Advanced analytics correlate seemingly unrelated events across the enterprise (e.g., three failed SSH logins on a server followed immediately by an outbound data transfer to an unknown overseas IP address), automatically elevating incidents to analysts.
- **Security Orchestration, Automation, and Response (SOAR):** Automates routine defensive responses through digital playbooks: automatically isolating compromised endpoints from the network, revoking compromised user credentials, and blocking malicious IP addresses at the firewall in milliseconds without waiting for human intervention.

9. Cryptographic Key Management Lifecycle: NIST SP 800-57 Standards

The security of any cryptographic system depends entirely upon the confidentiality, integrity, and administrative governance of its secret keys. Even the most mathematically unbreakable 256-bit AES encryption collapses if an administrator writes the decryption key into a public GitHub repository. Modern enterprise key governance follows the **NIST SP 800-57 Lifecycle Stages**:

- **Cryptographic Key Generation:** Keys must be generated using cryptographically secure pseudo-random number generators (CSPRNG) seeded with true physical hardware entropy (thermal noise, radioactive decay, clock jitter) to ensure mathematical unpredictability.
- **Hardware Security Modules (HSMs):** Critical corporate root keys must reside inside specialized, tamper-resistant physical **Hardware Security Modules (HSMs)** conforming to FIPS 140-2 / 140-3 Level 3 or 4 standards. HSMs perform cryptographic operations internally; private keys can never be exported or read in plaintext. If physical tampering is detected (drilling, temperature spikes), the HSM initiates automatic physical *zeroization*, instantly erasing key material.
- **Key Rotation and Destruction:** Cryptographic keys must be rotated at pre-scheduled intervals (cryptoperiods) to limit the amount of ciphertext encrypted under a single key. When decommissioned, keys must be destroyed through cryptographic shredding, ensuring zero recovery.

10. Common Web Application Attack Vectors: The OWASP Top 10

The Open Web Application Security Project (OWASP) maintains the authoritative global taxonomy of critical application vulnerabilities that imperil e-commerce web applications:

- **Injection Flaws (SQL Injection - SQLi):** Occurs when untrusted user input (entered into search bars or login forms) is concatenated directly into database SQL queries without input sanitization or parameterized prepared statements. Attackers inject malicious SQL commands

(e.g., `' OR '1'='1`), tricking the database into dumping the entire customer credit card database or granting unauthorized administrative bypass.

- **Cross-Site Scripting (XSS):** Occurs when an application includes untrusted data in a web page without proper HTML sanitization or contextual escaping. The attacker injects malicious client-side JavaScript code into product review fields; when legitimate consumers view the review, the malicious script executes in their browser, stealing their session cookies and hijacking accounts.
- **Cross-Site Request Forgery (CSRF):** Forces an authenticated victim's browser to send forged HTTP requests to a vulnerable web application (e.g., transferring funds or changing an account email) without the user's knowledge, mitigated via anti-CSRF synchronization tokens and SameSite cookie attributes.

11. Cloud Security Architectures and the Shared Responsibility Model

As enterprise e-commerce applications migrate from on-premise physical data centers to hyper-scale cloud environments (Amazon Web Services, Microsoft Azure, Google Cloud Platform), cybersecurity is governed by the **Cloud Shared Responsibility Model**:

- **Security OF the Cloud (Cloud Service Provider's Responsibility):** The cloud provider owns and manages the physical security of data centers, hardware servers, storage facilities, hypervisor virtualization layers, and global network backbones.
- **Security IN the Cloud (Customer's / Enterprise's Responsibility):** The enterprise customer retains absolute responsibility for configuring and managing guest operating systems, database access controls, application code, firewall routing rules, user IAM credentials, and customer data encryption. A breach resulting from an unencrypted public AWS S3 storage bucket is entirely the enterprise customer's liability.
- **Cloud Security Posture Management (CSPM):** Specialized automated security software that continuously scans multi-cloud environments, detecting misconfigurations, overly permissive IAM roles, unencrypted storage buckets, and ensuring regulatory compliance with PCI-DSS and ISO 27001.

12. Vulnerability Assessment and Penetration Testing (VAPT)

To uncover security flaws before malicious black-hat hackers exploit them, enterprises conduct systematic **VAPT Exercises**:

- **Vulnerability Assessment (VA):** An automated, high-level technical scan of network devices, servers, and web applications using specialized diagnostic tools (Nessus, OpenVAS, Qualys) to identify known software vulnerabilities, unpatched libraries, and open ports, generating prioritized vulnerability reports based on CVSS (Common Vulnerability Scoring System) scores.
- **Penetration Testing (PT):** A goal-oriented, simulated cyber attack conducted by certified ethical hackers (white-hat penetration testers). Testers actively exploit identified vulnerabilities, bypass security controls, escalate privileges, and simulate data exfiltration, testing human, physical, and digital defenses through Red Team versus Blue Team adversarial exercises.

Degreelive

13. Mathematical Architecture of the SHA-256 Compression Function

The Secure Hash Algorithm-256 (SHA-256), designed by the United States National Security Agency (NSA), processes data blocks using the classic **Merkle-Damgård Construction**. The mathematical sequence executes through precise algorithmic phases:

- **Padding and Parsing:** The input message is padded with a single bit '1', followed by '0' bits, and an 8-byte big-endian integer representing original message length, such that total bit length is an exact multiple of 512 bits. The padded bitstream is parsed into 512-bit message blocks.
- **Message Schedule Expansion:** Each 512-bit block is expanded into sixty-four 32-bit words using modular bitwise rotation, shift, and XOR operations.
- **The 64-Round Compression Loop:** Eight 32-bit working state variables (initialized to the fractional parts of the square roots of the first eight prime numbers) undergo 64 sequential computational rounds. Each round utilizes six distinct logical bitwise operations: *Ch* (Choose), *Maj* (Majority), Σ_0, Σ_1, σ_0, σ_1, and sixty-four constant 32-bit K-values (derived from the cube roots of prime numbers). The final working variables are added to the previous state, producing an unforgeable, collision-resistant 256-bit message digest.

14. End-to-End Encryption (E2EE) and the Double Ratchet Protocol

In modern digital messaging (WhatsApp, Signal), communication privacy is preserved through **End-to-End Encryption (E2EE)**. E2EE guarantees that data is encrypted on the sender's device and decrypted strictly on the recipient's device; no intermediate telecom service provider, server operator, or government interceptor can read the plaintext communications.

Modern E2EE relies on the **Double Ratchet Algorithm** (developed by Trevor Perrin and Moxie Marlinspike), which provides two advanced cryptographic guarantees:

- **Forward Secrecy:** The system continuously derives fresh, ephemeral symmetric session keys for every individual message using cryptographic key ratchets. If an attacker compromises a user's device and steals the current session key, they cannot decrypt any past messages sent or received by that user.
- **Post-Compromise Security (Future Secrecy):** Once an attacker loses access to a compromised device, the continuous Diffie-Hellman ratchet automatically regenerates fresh, uncompromised keys, preventing the attacker from reading future messages.

15. Air-Gapped Networks and Hardware Data Diodes

For ultra-critical national infrastructure—such as nuclear power generation controllers, military defense communications, and central bank high-value settlement vaults—standard software firewalls are deemed insufficient because firmware exploits can be bypassed. Highly secure institutions enforce **Air-Gapped Isolation**: physical network architectures where critical operational technology networks have zero physical or wireless connectivity to external public networks.

Where data must be transferred into an air-gapped facility (e.g., streaming telemetry logs out to an analytics dashboard), organizations install **Hardware Data Diodes (Unidirectional Security**

Gateways). A data diode utilizes physical fiber-optic hardware with a LED transmitter on one side and a photodetector on the receiving side, but physically lacks the reverse optical link. Data can physically flow strictly in one direction, making it physically impossible for an external cyber attacker to send malicious commands back into the protected network.

DegreeLive