

A -Regular/Scholarship/Back Exam - 2082 Shrawan/Bhadra

Program: Diploma in Information Technology

1. What is cyber-crime? Explain different cyber threat with its types. [4+6 Marks]

Cyber-crime is defined as any illegal, criminal, or fraudulent activity performed using computers, mobile devices, or computer networks as a tool to commit the crime or as the primary target of the attack.

Explanation of Cyber Threat & Its Major Types [6 Marks]

A Cyber Threat refers to any potential dangerous event, malicious attempt, or system vulnerability exploit that aims to gain unauthorized access, steal confidential data, destroy digital infrastructure, or disrupt normal computer network operations.

Textbook Diagram: Cyber Threat Vector & Attack Execution Flow

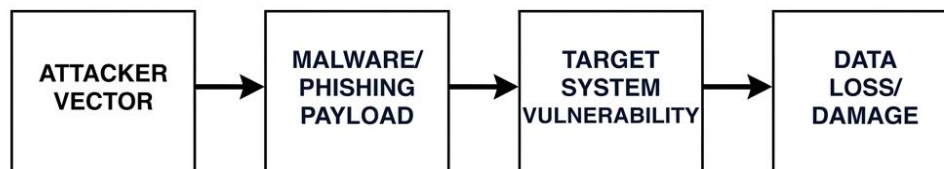


Figure: Textbook Block Diagram of Cyber Threat and Attack Execution Flow

Major Types of Cyber Threats:

1. Malware Threat (Malicious Software):

Malware is unwanted software designed to harm, exploit, or disable computer systems.

2. Phishing & Social Engineering Threat:

Deceptive techniques manipulating human trust to trick users into revealing confidential credentials (passwords, PINs, bank details) via fraudulent emails (Phishing), SMS (Smishing), or phone calls (Vishing).

3. Denial of Service (DoS) & Distributed DoS (DDoS):

An attack designed to flood a targeted server or website with millions of fake traffic requests simultaneously, overwhelming its capacity and rendering it unavailable to legitimate users.

4. Man-in-the-Middle (MitM) Threat:

An attack where a hacker secretly intercepts, reads, or alters communication between two trusting parties (e.g. user and online banking website) over unsecured public Wi-Fi networks.

Q2. Explain different types of firewalls. How does each type function to protect a network?

1. Explanation of Network Firewall []

A Firewall is a critical network security system—available as hardware, software, or a combination of both—that acts as a protective shield between a trusted internal network (like a company LAN) and an untrusted external network (like the public Internet).

Textbook Diagram: Network Firewall Architecture & Traffic Filtering

Network Firewall Architecture

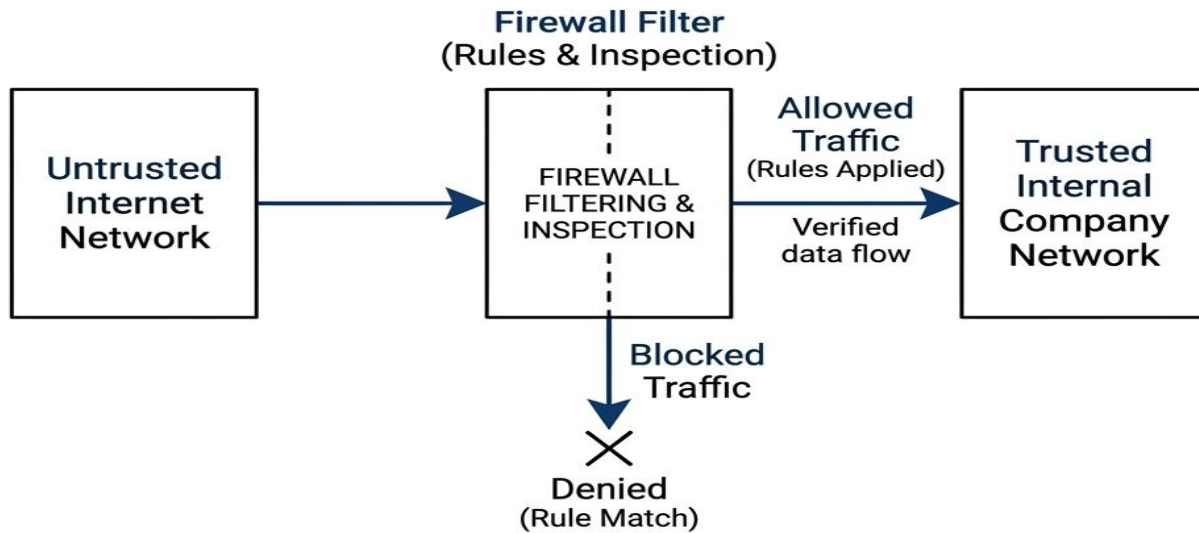


Figure: Textbook Network Firewall Block Diagram

2. Types of Firewalls & How Each Functions to Protect a Network

A. Packet Filtering Firewall (Stateless Firewall)

- Working Mechanism: Inspects data packet headers at the Network (L3) and Transport (L4) layers.
- **Filtering Basis:** Compares Source IP, Destination IP, Port numbers, and Protocol against Access Control Lists (ACLs).
- Function: Evaluates each packet individually in isolation without tracking session state.
- Pros & Cons: Fast and low cost, but cannot inspect packet payload content.

B. Stateful Inspection Firewall

- Working Mechanism: Tracks the active connection state of network sessions in a dynamic State Table.
- Filtering Basis: Verifies if incoming packets belong to an existing, approved outbound session request.
- Function: Automatically drops unexpected incoming traffic while permitting legitimate response packets.
- Pros & Cons: Highly secure against unauthorized intrusion, but requires more system memory.

C. Application-Level Gateway (Proxy Firewall)

- Working Mechanism: Operates at the Application Layer (L7) as a middleman proxy between client and web server.
- Filtering Basis: Performs deep content inspection on HTTP, FTP, and SMTP

Q3. Explain classical encryption/decryption method. What is digital signature and how does it works? [5+5 Marks]

Classical Encryption & Decryption Method [5 Marks]

Classical Encryption is the traditional cryptographic process of taking plain, readable text (Plaintext) and transforming it into an unreadable secret format (Ciphertext) using character substitution or transposition algorithms. Decryption is the reverse mathematical process of converting ciphertext back into original plaintext using a secret key. In classical cryptography, both the sender and receiver share and use the exact same secret key (Symmetric Key Cryptography).

Core Working Process:

1. Sender writes Plaintext message M.
2. Encryption function transforms message: $C = E(M, K)$ using shared secret Key K.
3. Ciphertext C is transmitted safely across untrusted channels.
4. Receiver applies Decryption function: $M = D(C, K)$ using Key K to read message.

Famous Classical Ciphers:

- Caesar Cipher: Substitutes each letter by shifting it a fixed number of alphabet positions (e.g. Shift=3: A becomes D, B becomes E).
- Vigenère Cipher: Uses a keyword to perform polyalphabetic letter substitution.

Limitations: Low security level, easily broken by frequency analysis, and difficult secret key distribution.

Digital Signature & Its Working Mechanism [5 Marks]

A Digital Signature is a modern cryptographic mechanism used to verify the Authenticity (sender identity), Integrity (document not altered), and Non-Repudiation (sender cannot deny signing) of digital documents using Asymmetric (Public-Private Key) Cryptography.

Step-by-Step Working Mechanism:

1. Hash Generation: Sender passes the digital document through a Hash Function (e.g. SHA-256) to produce a fixed-length Hash Value.
2. Digital Signature Creation: Sender encrypts the hash value using their private Private Key to produce the Digital Signature.
3. Transmission: Sender sends the original Document along with the Digital Signature to the receiver.
4. Signature Verification: Receiver decrypts the signature using Sender's Public Key to get Hash A. Receiver also hashes the received document to get Hash B.
5. Final Check: If Hash A matches Hash B, the signature is authentic and document integrity is verified.

DIGITAL SIGNATURE PROCESS SCHEMATIC

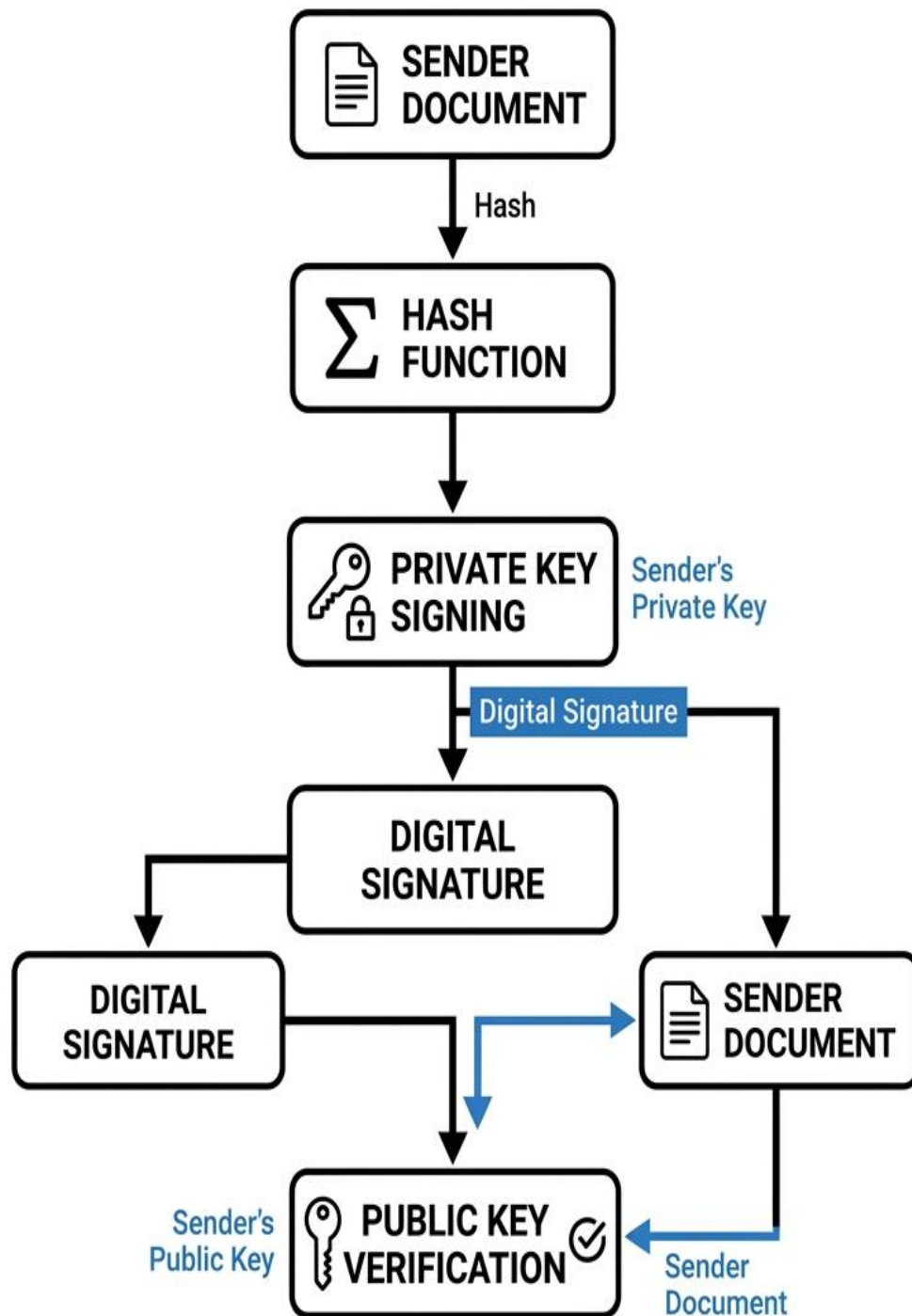


Figure: Textbook Digital Signature Signing and Verification Flowchart

Q4. What is cyber law? Why is it important in context of Nepal? Discuss the key areas it addresses. [2+3+5 Marks]

1. Definition of Cyber Law (2 Marks)

Cyber Law is the legal framework governing the use of computers, internet, digital data, electronic commerce, and cyber security. It defines legal rules, user responsibilities, and criminal penalties for digital offences.

2. Importance of Cyber Law in Context of Nepal (3 Marks)

- Legalizes E-Commerce & Digital Payments: Grants legal recognition to online bank transfers, digital wallets (eSewa, Khalti), and digital signatures.
- Deters & Controls Cyber Crime: Equips Nepal Police (Cyber Bureau) and courts to investigate and punish hackers, online fraudsters, and cyber bullies.
- Protects Citizen Data & Privacy: Establishes data privacy rights and legal protection against online harassment and defamation.

3. Key Areas Addressed by Cyber Law in Nepal (ETA 2063) (5 Marks)

- Digital Signature Regulation: Establishes the Controller of Certification Authorities (CCA) to certify digital keys and contracts.
- Cyber Offence Regulation & Penalties: Defines strict fines and imprisonment for unauthorized computer access, virus spreading, and source code damage (Sections 44-52).
- Intellectual Property Protection: Protects software source code, digital designs, and copyright online.
- IT Tribunal Formation: Establishes specialized IT Tribunals and IT Appellate Tribunals to resolve digital disputes quickly.

Q5. What is forensic technology? Explain incident detection and analysis. [2+8

1. Definition of Forensic Technology (2 Marks)

Forensic Technology (Digital Forensics) is the scientific discipline of identifying, preserving, extracting, analyzing, and presenting digital evidence from electronic storage media in a legally acceptable format for court proceedings.

2. Explanation of Incident Detection and Analysis (8 Marks)

Textbook Diagram: Incident Response & Digital Forensics Lifecycle

Incident Detection & Digital Forensics Process

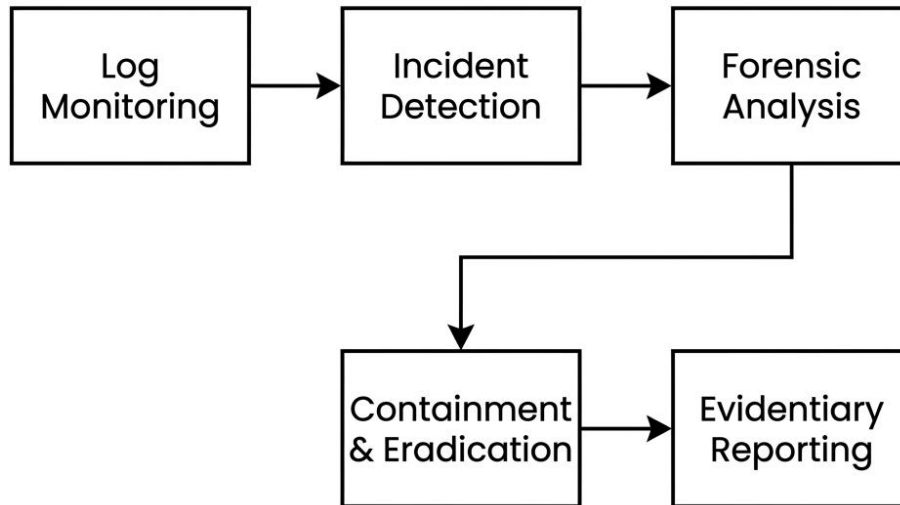


Figure: Textbook Diagram of Incident Detection, Analysis, and Forensics Lifecycle

- **Incident Detection:** The phase of identifying suspicious network activity or security breaches. It relies on Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), antivirus log alerts, and system anomaly reports.
- **Incident Analysis:** Forensic investigators examine extracted log files, memory dumps, disk images, and network traffic captures to confirm if a breach occurred, evaluate damage scope, identify compromised accounts, and trace the attacker's path.

Q6. Explain the key differences between mobile application security and web application security. [10 Marks]

Comprehensive 10-Point Comparison Table: Web Application Security vs Mobile Application Security

S.N.	Comparison Basis	Web Application Security	Mobile Application Security
1	Architecture & Hosting	Hosted on central remote web servers; accessed via web browsers.	Installed directly on client mobile devices (Android / iOS).
2	Primary Attack Surface	Server databases, web APIs, cloud backends, and web forms.	Local device storage, app binary files, device sensors, and IPC.
3	Common Threats	SQL Injection, Cross-Site Scripting (XSS), CSRF, Server Misconfig.	Reverse engineering, APK decompilation, insecure local storage.
4	Code Protection	Backend server source code remains hidden on central server.	Compiled app binaries (.apk / .ipa) can be downloaded & decompiled.

5	Data Storage Risks	Relies on browser cookies, LocalStorage, and SessionStorage.	Uses SQLite databases, Android Keystore, iOS Keychain, SD cards.
6	Sandboxing Mechanism	Enforced by browser sandbox & Same-Origin Policy (SOP).	Enforced by OS-level sandboxing (Android UID, iOS sandbox).
7	Network Security	Relies on standard SSL/TLS (HTTPS) domain certificates.	Requires HTTPS + Certificate Pinning to stop local proxy MITM.
8	Update Management	Server updated instantly for all users nationwide at once.	Requires users to manually update apps from Play/App Store.
9	User Control & Permissions	Users cannot alter web application server environment.	Users control device permissions (Camera, Microphone, GPS).

10

Offline
FunctionalityRarely operates
offline without
an active
internet
connection.Often stores
local data and
operates
offline on
mobile device.

Q7. What are the ethical challenges for cyber security professionals? Explain privacy in brief. [8+2 Marks]

1. Ethical Challenges for Cyber Security Professionals (8 Marks)

1. Privacy vs Surveillance Dilemma: Balancing employee network monitoring against personal privacy rights.
2. Dual-Use Security Tools: Security tools (Nmap, Metasploit) can be used for network defense or illegal hacking.
3. Responsible Vulnerability Disclosure: Deciding whether to report security bugs privately to vendors or disclose publicly.
4. Whistle-Blowing Dilemma: Reporting company security cover-ups to public authorities vs respecting Non-Disclosure Agreements (NDA).
5. Conflict of Interest: Refusing bribes or financial incentives from hackers or business competitors.
6. Data Confidentiality: Protecting customer data accessed during penetration testing security audits.
7. Authorized Scope Limits: Staying strictly within agreed penetration testing scope boundaries.
8. Professional Integrity: Providing accurate security audit reports without hiding or exaggerating risks.

2. Privacy in Brief (2 Marks)

Privacy is an individual's fundamental right to control how their personal identifiable information (PII) is collected, stored, processed, and shared by digital systems. In cyber security, privacy protection ensures that personal user data is

safeguarded against unauthorized tracking, data leaks, and commercial exploitation.

Q8. What is internet fraud? What are some common types of internet fraud that people should be aware of? [2+8 Marks]

1. Definition of Internet Fraud (2 Marks)

Internet Fraud refers to any fraudulent scheme, deceptive trick, or illegal scam conducted online using internet services, email, or web applications to steal money, property, or sensitive personal credentials from victims.

2. Common Types of Internet Fraud (8 Marks)

- Phishing Scams: Sending fake bank emails to trick victims into revealing online passwords.
- Identity Theft: Stealing citizenship numbers or bank details to commit financial crimes in victim's name.
- Advance Fee Fraud (419 Scam): Tricking victims into paying small upfront fees for non-existent cash rewards.
- E-Commerce / Online Shopping Scams: Fake shopping websites taking payment without delivering products.
- Tech Support Scams: Fake browser pop-ups warning of computer viruses and demanding payment to fix them.

Q9. Write short notes on: (a) Containment, eradication, recovery (b) VPN (c) Encryption/Decryption (d) Trademarks [10 Marks]

(a) Containment, Eradication, and Recovery

Containment, Eradication, and Recovery are three essential consecutive phases of the Incident Response lifecycle executed right after a cyber attack or data breach is detected to minimize operational damage.

Key Points (7 Points):

1. **Containment Phase:** Immediately isolates infected systems from the network to prevent malware from spreading to other computers.
2. **Short-Term Containment:** Disconnects network cables or isolates virtual machines while keeping systems powered on for forensic analysis.
3. **Long-Term Containment:** Applies temporary security patches and changes compromised administrator passwords.
4. **Eradication Phase:** Completely cleans the environment by removing malware files, rootkits, and unauthorized backdoor accounts.
5. **Vulnerability Fix:** Identifies and fixes the root security weakness that allowed the hacker to break in.
6. **Recovery Phase:** Restores production systems and services safely using clean, uninfected data backups.
7. **System Validation:** Thoroughly tests restored systems to ensure normal operations before opening them to users again.

(b) Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a network security service that creates a secure, encrypted connection (tunnel) over an untrusted public network like the Internet.

Key Points (7 Points):

1. **Encrypted Tunneling:** Encapsulates data packets inside encrypted outer headers using protocols like OpenVPN or WireGuard.
2. **Data Confidentiality:** Uses strong encryption (such as AES-256) to ensure eavesdroppers cannot read transmitted data payload.
3. **IP Address Masking:** Hides the user's real public IP address and replaces it with the VPN server's location IP.
4. **Secure Remote Access:** Allows remote employees to connect safely to private company internal networks from home.
5. **Wi-Fi Protection:** Neutralizes eavesdropping and packet sniffing risks on public Wi-Fi networks (cafes, airports).

6. **Authentication:** Verifies user credentials and digital certificates before opening the VPN tunnel.
7. **Anonymity & Privacy:** Prevents ISPs and third-party trackers from monitoring user browsing activities.

(c) Encryption and Decryption

Encryption and Decryption are fundamental cryptographic processes used to protect sensitive data confidentiality during storage and transmission.

Key Points (7 Points):

1. **Encryption Process:** Mathematical transformation converting readable plain text (Plaintext) into unreadable secret text (Ciphertext).
2. **Decryption Process:** Reverse mathematical transformation converting unreadable Ciphertext back into original readable Plaintext.
3. **Cryptographic Keys:** Uses mathematical keys (Symmetric shared keys or Asymmetric key pairs) to control encoding and decoding.
4. **Data in Transit:** Protects sensitive financial data flowing across internet cables and Wi-Fi networks (SSL/TLS HTTPS).
5. **Data at Rest:** Protects stored files on hard drives, laptops, and databases against physical theft or unauthorized access.
6. **Prevents Data Breaches:** Ensures that even if hackers intercept packets, the data remains unreadable without the secret key.
7. **Core Security Pillar:** Forms the main technological foundation for modern cyber security, e-commerce, and online banking.

(d) Trademarks

A Trademark is a type of Intellectual Property Right (IPR) that legally protects unique brand signs, names, logos, symbols, or slogans distinguishing a company's products from competitors.

Key Points (7 Points):

1. **Legal Protection:** Grants exclusive legal rights to a company to use its brand name and logo in the marketplace.
2. **Prevents Brand Abuse:** Stops competitors from creating fake copies or using similar confusing logos.
3. **Symbol Representation:** Represented legally by symbols like [™] (Unregistered Trademark) or [®] (Registered Trademark).
4. **Domain Name Relevance:** Protects company web domain names (e.g. google.com, apple.com) from cybersquatt

CTEVT DIPLOMA IN IT (DCOM-IT III/II)

Subject: Cyber Security | Exam Paper Solutions (2081 Kartik/Mangsir -)
Master Solved Exam Question Bank

Q1.a. Define information system and cyber threats. Describe the types of cyber threats. [4+4 Marks]

1. Definition of Information System.

An Information System (IS) is an integrated combination of hardware, software, data, network infrastructure, and people designed to collect, store, process, and transmit information across an organization.

2. Definition of Cyber .

A Cyber Threat is any potential malicious attempt, security vulnerability exploit, or harmful event aimed at gaining unauthorized access, stealing data, or disrupting computer networks.

3. Major Types of Cyber Threats.

- **Malware Threats:** Includes Ransomware (locks files for money), Viruses (infects executable files), Worms (auto-spreads via networks), and Trojans (disguised backdoors).
- **Social Engineering & Phishing:** Manipulating users via fake emails or phone calls to reveal passwords and personal identification numbers.
- **Denial of Service (DoS / DDoS):** Overwhelming a target web server with fake traffic requests so real users cannot access the service.
- **Man-in-the-Middle (MitM):** Intercepting and reading confidential web traffic between a user and website over unsecured Wi-Fi.

Q1.b. What is VPN? Describe the functionality of a VPN in securing a network.

A Virtual Private Network (VPN) is a network security service that creates a safe, encrypted connection (tunnel) over a public network like the Internet. It connects remote workers or branch offices securely to a private company network.

2. Core Features

- **Encrypted Tunneling:** Wraps original data packets inside encrypted outer headers.
- **IP Address Masking:** Hides user's actual IP address and replaces it with VPN server IP.
- **Remote Network Access:** Grants secure access to private company intranet from anywhere.
- **Multi-Factor Authentication:** Requires user credentials and tokens before

opening tunnel.

- Protocol Support: Uses security protocols like IPSec, OpenVPN, and WireGuard.

MINIMALIST SCHEMATIC: VPN TUNNELING AND NETWORK SECURITY

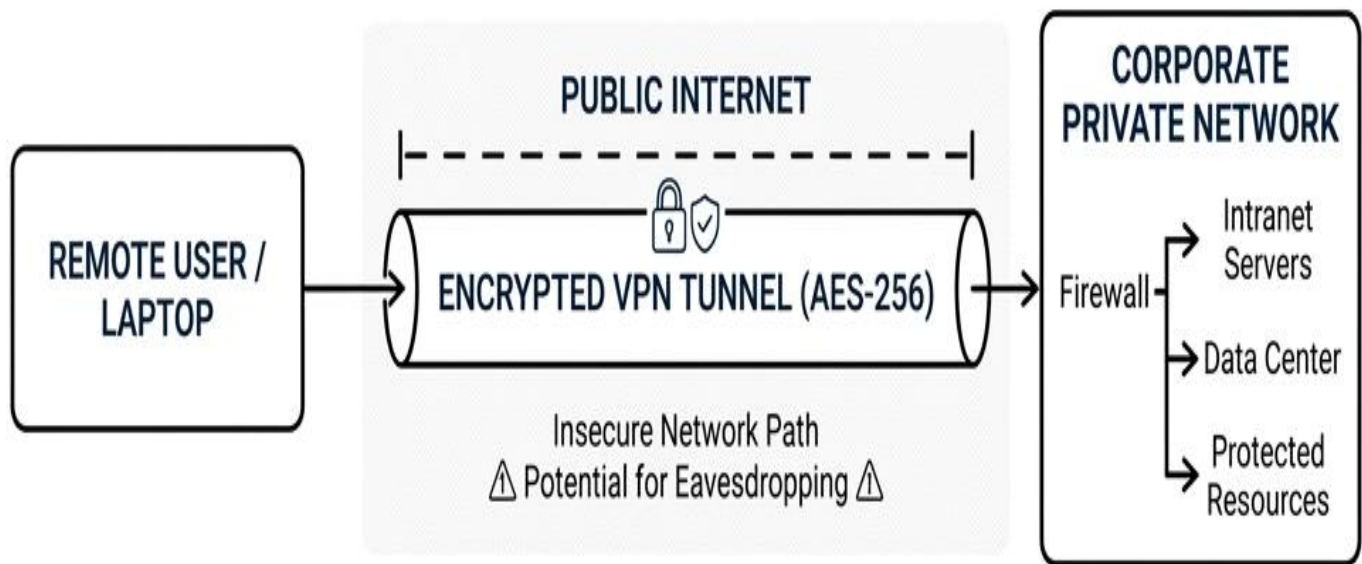


Figure: Textbook Block Diagram of VPN Encrypted Tunneling Architecture

3. Working Functionality in Securing a Network

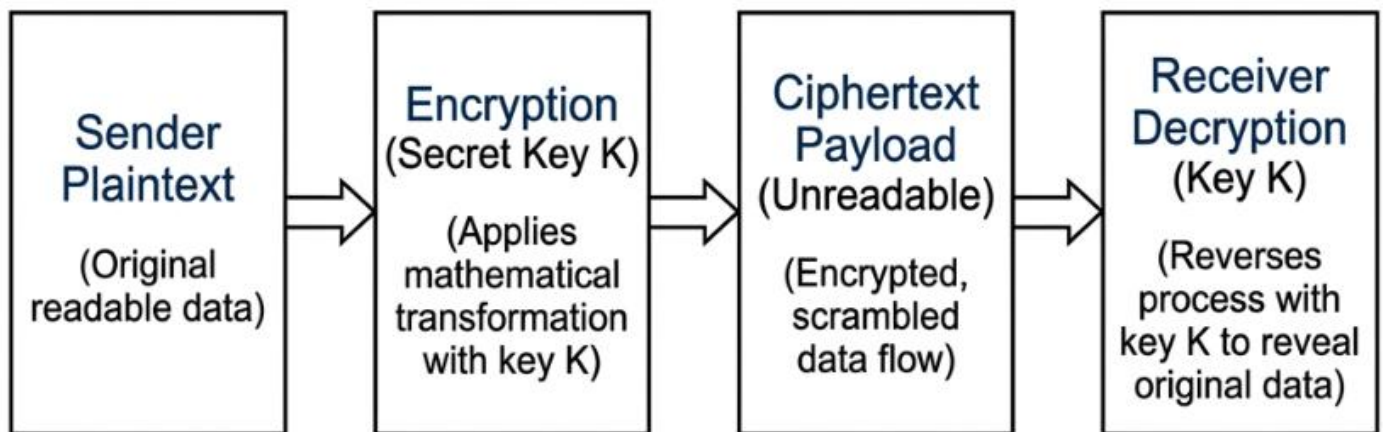
- Tunnel Establishment: VPN client software authenticates with the remote VPN server.
- Data Encryption: Encrypts data packets at origin using strong algorithms like AES-256.
- Safe Transmission: Transmits encrypted packets across public internet safely.
- Decryption & Routing: VPN server decrypts packets and routes them to target internal servers.
- Data Integrity Check: Uses cryptographic hashes (HMAC) to verify packets were not tampered with.

Q2.a. How does encryption help in maintaining data confidentiality? Explain.

How Encryption Guarantees Confidentiality (Key Pillars):

Data Confidentiality ensures that sensitive information is accessible only to authorized users and remains completely hidden from unauthorized individuals. Encryption maintains confidentiality by taking readable plain text (Plaintext) and mathematically transforming it into an unreadable secret format (Ciphertext) using cryptographic keys.

HOW ENCRYPTION ENSURES DATA CONFIDENTIALITY



Features of Confidentiality via Encryption.

- **Mathematical Scrambling:** Converts plain text bits into complex mathematical ciphertext using algorithms like AES-256.
- **Key-Based Access Control:** Ensures data can only be decrypted by individuals holding the correct secret key.
- **Protection in Transit:** Secures data traveling over public networks, cables, and Wi-Fi connections (SSL/TLS HTTPS).
- **Protection at Rest:** Encrypts stored files on hard drives, laptops, databases, and USB drives against physical theft.
- **Render Intercepted Data Useless:** Guarantees that stolen data is unreadable and useless to cyber criminals.

Q2.b. Differentiate between symmetric and asymmetric cryptography. Explain the implementation of RSA with example.

1. Comparison Table: Symmetric vs Asymmetric Cryptography (10 Points)

S.N.	Comparison Basis	Symmetric Cryptography	Asymmetric Cryptography
1	Keys Used	Uses a single shared secret key for encryption & decryption.	Uses a pair of keys: Public Key (encrypt) and Private Key (decrypt).
2	Key Distribution	Difficult (Secret key must be transmitted securely).	Easy (Public key can be shared openly; Private key stays secret).
3	Execution Speed	Very Fast (High throughput, computationally lightweight).	Slower (Requires complex mathematical exponentiation).
4	Resource Usage	Low CPU and memory usage; suitable for bulk data.	High CPU and memory consumption; suitable for small data/keys.
5	Digital Signature	Cannot support digital signatures or non-repudiation.	Provides digital signatures and non-repudiation.
6	Number of Keys	Requires $N*(N-1)/2$ keys for N users.	Requires $2*N$ keys for N users.

RSA Algorithm Implementation & Step-by-Step Numerical Example [6 Marks]

Textbook Diagram: RSA Algorithm Key Generation & Cryptographic Flow

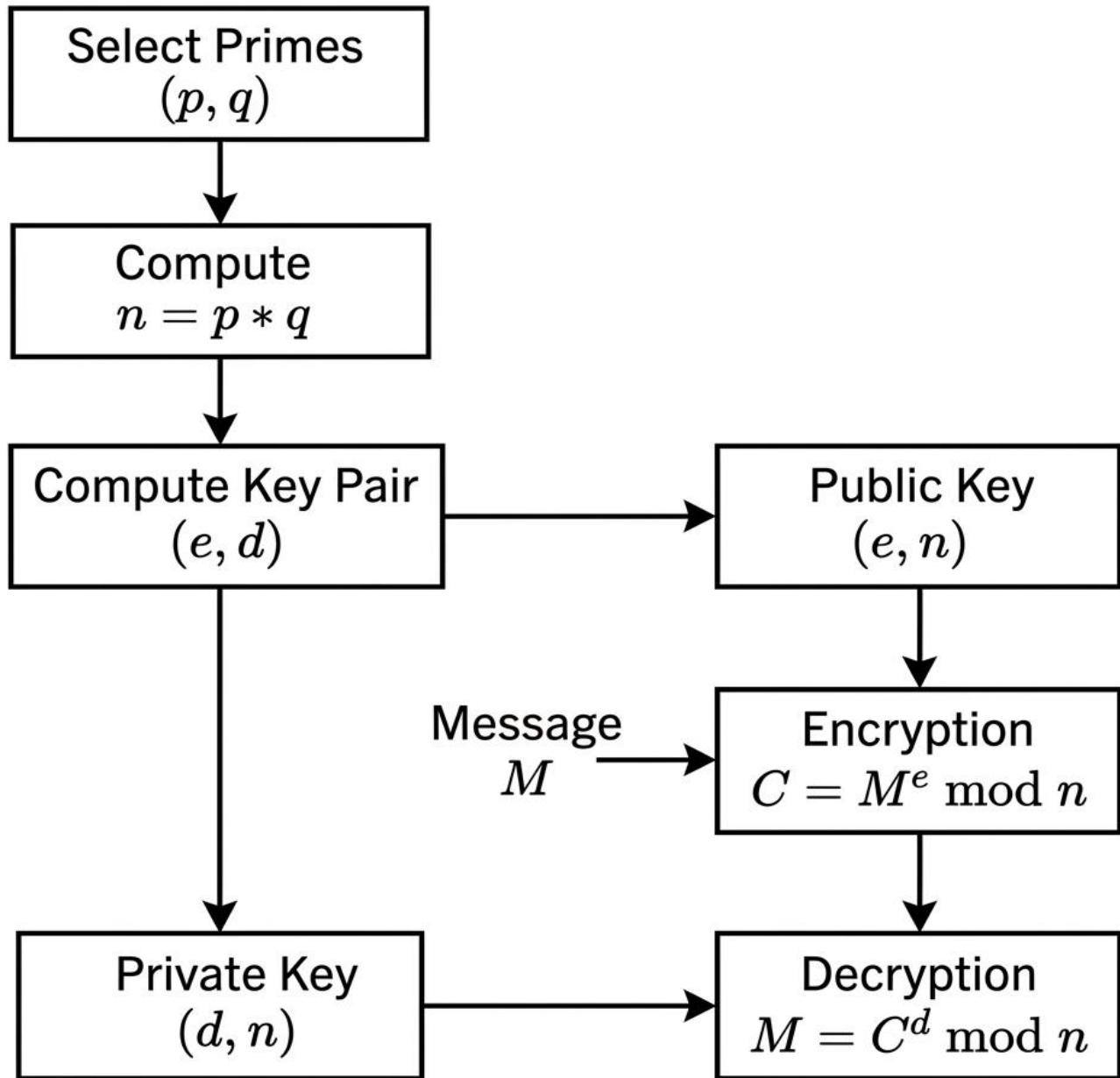


Figure: Textbook Flowchart of RSA Algorithm Implementation

RSA (Rivest-Shamir-Adleman) is an asymmetric algorithm based on the mathematical difficulty of factoring large prime numbers.

Step-by-Step Numerical Example:

- Step 1: Select two prime numbers: $p = 3$, $q = 11$.
- Step 2: Compute modulus $n = p * q = 3 * 11 = 33$.
- Step 3: Compute Euler Totient $\phi(n) = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 2 * 10 = 20$.
- Step 4: Choose Public Exponent 'e' such that $1 < e < \phi(n)$ and $\gcd(e, 20) = 1$. Choose $e = 7$.

- Step 5: Compute Private Exponent 'd' such that $(d * e) \equiv 1 \pmod{\phi(n)}$.
 $(d * 7) \equiv 1 \pmod{20} \Rightarrow$ Choose $d = 3$ (since $3 * 7 = 21 \equiv 1 \pmod{20}$).

Public Key = $(e=7, n=33)$ | Private Key = $(d=3, n=33)$

- Encryption Example (Plaintext $M = 2$):
Ciphertext $C = M^e \pmod{n} = 2^7 \pmod{33} = 128 \pmod{33} = 29$.

- Decryption Example (Ciphertext $C = 29$):
Plaintext $M = C^d \pmod{n} = 29^3 \pmod{33} = 24389 \pmod{33} = 2$.
(Successfully decrypted back to original message Plaintext $M = 2$!)

Q3.a. What do you mean by cyber risk management? Explain cyber risk management process.

Cyber Risk Management is the ongoing systematic process of identifying, analyzing, evaluating, treating, and monitoring digital security risks to an organization's information assets. It ensures that businesses can protect critical data while maintaining operational continuity.

2. Cyber Risk Management Process Textbook Diagram: Cyber Risk Management Lifecycle

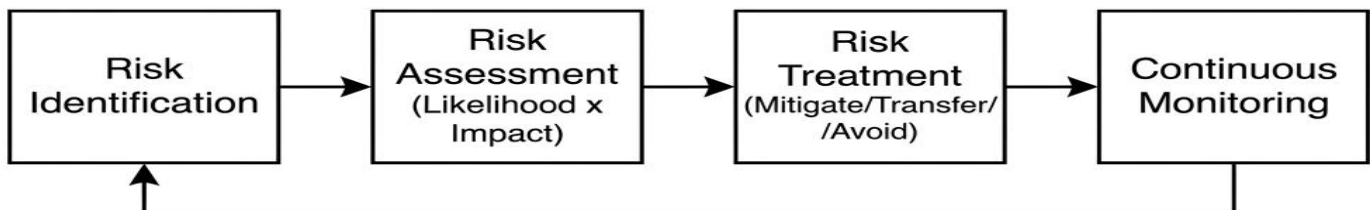


Figure: Textbook Process Flowchart of Cyber Risk Management Lifecycle

- Phase 1: Risk Identification: Cataloging digital assets, identifying vulnerabilities, and listing threat vectors.
- Phase 2: Risk Assessment / Analysis: Calculating Risk Level = Likelihood x Impact to prioritize risks.
- Phase 3: Risk Treatment / Response: Implementing strategies:
 - Risk Mitigation: Deploying firewalls, antivirus, and patches to lower risk.
 - Risk Transference: Buying Cyber Insurance to shift financial impact.
 - Risk Avoidance: Discontinuing high-risk activities or legacy software.
 - Risk Acceptance: Accepting low-impact minor risks.
- Phase 4: Continuous Monitoring: Conducting regular security audits and updating risk registries.

Q3.b. Explain common threats in web application security.

Web Application Security threats target vulnerabilities in web browsers, web servers, databases, and application source code. Major threats include:

- 1. SQL Injection (SQLi):** Attacker enters malicious SQL code into input fields to read or delete database tables.
- 2. Cross-Site Scripting (XSS):** Injecting malicious client-side JavaScript into web pages viewed by other users to steal session cookies.
- 3. Cross-Site Request Forgery (CSRF):** Tricking authenticated users into executing unwanted actions on a web app.
- 4. Broken Authentication:** Weak session management allowing attackers to compromise passwords or session tokens.
- 5. Security Misconfiguration:** Unpatched web servers, default admin passwords, and verbose error messages exposing system internals.

Q4.a. What do you mean by forensic technology? Explain evidentiary reporting in brief.

Forensic Technology is the scientific discipline of identifying, preserving, extracting, analyzing, and presenting digital evidence from electronic storage devices in a court of law.

Evidentiary Reporting in Brief:

Evidentiary Reporting is the formal documentation phase where forensic investigators write a detailed, objective report summarizing digital evidence findings. It details how evidence was collected, tools used, hash values, timeline of events, and Chain of Custody to ensure full legal admissibility in court.

Q4.b. Describe the process of digital evidence collection.

Textbook Diagram: Digital Evidence Collection Process Flowchart

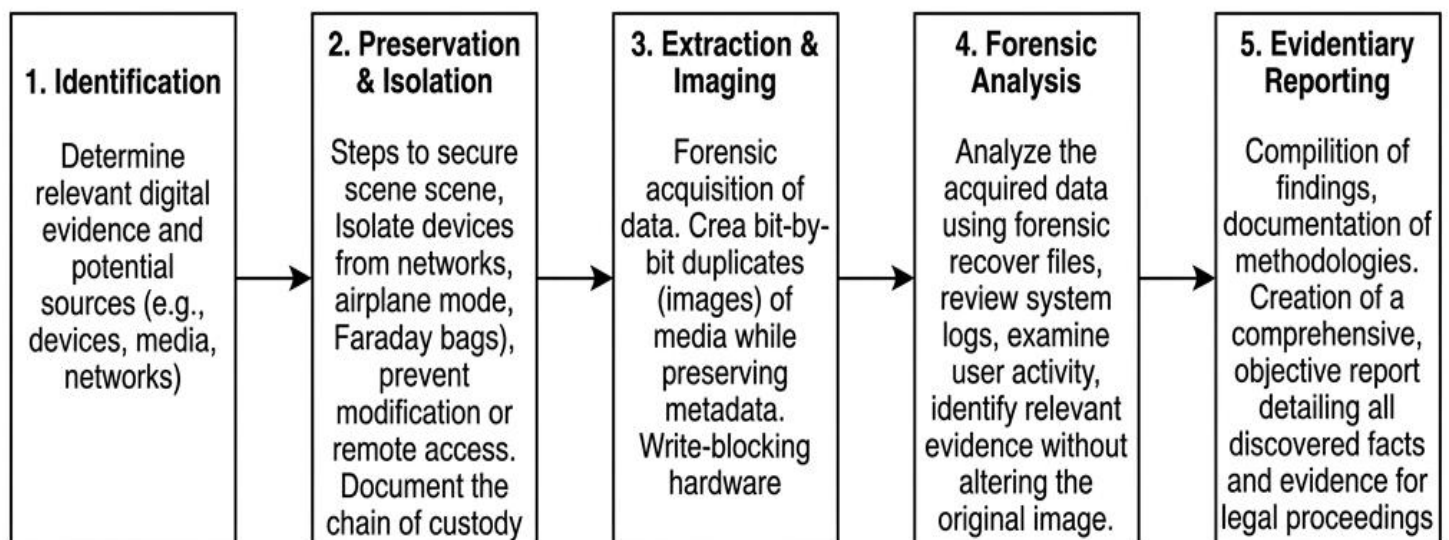


Figure: Textbook Flowchart of Digital Evidence Collection Process

1. Identification: Locating all potential evidence sources (hard drives, RAM, logs, smartphones, cloud backups).
2. Preservation & Isolation: Securing evidence from tampering using write-blocker hardware and Faraday bags. Generating MD5/SHA-256 hash values to prove integrity.
3. Extraction & Forensic Imaging: Creating bit-stream exact copies (disk images) of drives to analyze without altering original evidence.
4. Analysis: Examining extracted images using forensic tools (EnCase, FTK, Autopsy) to locate deleted files and event logs.
5. Documentation & Chain of Custody: Maintaining a strict log of who handled the evidence, when, and where.

Q5.a. Define intellectual property. Explain its relevance to cyber security.

Intellectual Property (IP) refers to intangible creations of the human intellect protected by law, such as software source code, patents, proprietary designs, literary works, and business trademarks.

Relevance to Cyber Security

Intellectual Property is the core digital asset of modern technology companies. Since most IP today is stored, processed, and transmitted in digital format (code, cloud databases, research files), cyber security plays a critical role in protecting IP against corporate espionage, illegal downloading, hacking, and unauthorized distribution.

- **Source Code Protection:** Prevents competitors from hacking and stealing proprietary software algorithms.
- **Trade Secret Protection:** Safeguards business formulas and customer databases from corporate cyber espionage.
- **Prevents Counterfeiting:** Stops malicious actors from creating fake brand websites or pirated software.
- **Data Breach Mitigation:** Ensures legal ownership and recovery rights if digital IP is stolen.

Q5.b. Discuss the codes of ethics, conduct and practice of IT professionals.

A Code of Ethics, Conduct, and Practice for IT Professionals is a set of formal moral guidelines, professional standards, and operational rules established by professional computer bodies (such as IEEE, ACM, or Nepal Engineering Council). Because IT professionals possess high-level administrative access to sensitive user data, financial networks, and critical software systems, these codes ensure that they exercise their technical power responsibly, maintain confidentiality, and protect public safety.

Features / Core Principles of IT Code of Conduct (4 to 5 Points)

- **Data Confidentiality:** Absolute commitment to protecting private customer data and trade secrets from unauthorized disclosure.
- **System Integrity & Honesty:** Refusing to use system administrator access to spy, steal data, or install unauthorized backdoors.
- **Professional Competence:** Delivering high-quality, bug-free, and secure software solutions while continually updating technical skills.
- **Legal Compliance:** Respecting national cyber laws (e.g. ETA 2063 of Nepal), software copyright licenses, and intellectual property rights.
- **Public Safety & Social Responsibility:** Ensuring IT systems cause no physical, financial, or psychological harm to society or individual users.

Step 4: Working / Professional Practice Standards (4 to 5 Points)

- **Authorized Access Only:** Accessing databases, client servers, and user records strictly within written permission limits.
- **Conflict of Interest Avoidance:** Refusing bribes, kickbacks, or secret financial incentives from hackers or competing software vendors.
- **Objective Reporting:** Providing accurate, unbiased vulnerability audit reports without hiding or exaggerating system risks.
- **Respecting Intellectual Property:** Using licensed development tools and refusing to distribute pirated software code.
- **Ethical Vulnerability Handling:** Following Responsible Disclosure protocols when discovering software bugs.

6. Write short notes on: (any FOUR) [4x4 = 16 Marks] [16 Marks]

a. Firewall

A Firewall is a critical network security system that acts as a protective shield between a trusted internal network and an untrusted external network like the Internet. It monitors all incoming and outgoing network traffic based on predefined security rules to block malicious packets.

Key Points:

1. Filters network traffic based on IP address, port numbers, and protocols.
2. Operates at stateless (L3/L4) or stateful/proxy (L7) application layers.
3. Prevents unauthorized hackers from entering private corporate networks.
4. Maintains Access Control Lists (ACLs) and connection state tables.
5. Provides detailed event logs of all blocked intrusion attempts.
6. Hides internal company IP addresses from external internet scanners.
7. Essential perimeter defense tool for corporate cyber security.

b. Cyber Law

Cyber Law is the legal framework that governs the use of computers, internet, digital data, electronic commerce, and cyber security. It provides legal guidelines, user rights, and criminal penalties for digital offences to maintain order in cyberspace.

Key Points:

1. Legalizes electronic contracts, e-banking, and digital signatures.
2. Criminalizes computer hacking, virus spreading, and online fraud.
3. Enforces data privacy rights and protects citizens from online harassment.
4. Protects software source code and digital intellectual property.
5. Governed in Nepal by the Electronic Transaction Act (ETA) 2063.
6. Establishes specialized IT Tribunals to settle digital legal disputes.
7. Promotes safe digital economic growth and user trust online.

c. Containment, Eradication and Recovery

Containment, Eradication, and Recovery are core consecutive phases of the Incident Response lifecycle executed after a cyber security breach is detected to minimize operational damage.

Key Points:

1. Containment limits attack scope by disconnecting infected hosts from network.
2. Short-term containment isolates systems while long-term containment patches bugs.
3. Eradication purges malware artifacts, rootkits, and unauthorized backdoor accounts.
4. Fixes underlying system vulnerabilities before restoring production services.
5. Recovery restores systems safely back to production using clean backups.
6. Tests restored systems thoroughly to confirm malware is completely eliminated.
7. Vital process for business continuity and disaster recovery planning.

d. Electronic Transaction Act (ETA 2063) of Nepal

The Electronic Transaction Act (ETA) 2063 (2006 BS) is the primary cyber legislation of Nepal enacted to legalize electronic transactions and control digital crimes across the country.

Key Points:

1. Grants legal recognition to electronic records and digital signatures in Nepal.
2. Establishes the Controller of Certification Authorities (CCA) for digital keys.
3. Section 44 penalizes unauthorized hacking and system tampering.
4. Section 45 penalizes damage to computer source code and programs.
5. Section 47 penalizes publishing illegal or offensive electronic material.
6. Formed the IT Tribunal and IT Appellate Tribunal for fast legal trial.
7. Foundation law for e-governance and online banking growth in Nepal.

e. Internet Fraud

Internet Fraud refers to any fraudulent scheme, deceptive trick, or illegal scam conducted online using web applications, email, or software to steal money or confidential data from victims.

Key Points:

1. Includes Phishing emails impersonating legitimate bank login portals.
2. Encompasses Identity Theft to open unauthorized financial loans.
3. Involves Advance Fee Fraud (419 scams) promising non-existent payouts.
4. Uses fake e-commerce shopping websites to collect money without delivery.
5. Employs fake tech support pop-ups demanding payment for fake virus fixes.
6. Prevents user safety through digital literacy and multi-factor auth (MFA).

CTEVT DIPLOMA IN COMPUTER ENGINEERING (DCE III/I)

Subject: Cyber Security and Social Ethics | Exam Paper Solutions (2080 Bhadra - Master Solved Exam Question Bank)

Q1.a. Define cyber security. Explain the different types of attack in cyber.

1. Definition of Cyber Security.

Cyber Security refers to the body of technologies, processes, practices, and controls designed to protect computers, networks, programs, and data from unauthorized access, cyber attacks, damage, or theft. Its core goal is to maintain Confidentiality, Integrity, and Availability (CIA Triad).

2. Explanation of Types of Attacks in Cyber.

A Cyber Attack is an intentional exploitation of computer systems, networks, or technology-dependent enterprises by cyber criminals

Cyber Attack	Description
1. Phishing	Fake emails, messages, or websites trick users into revealing passwords or banking details.
2. Malware	Malicious software that damages or steals data from a computer.
3. Virus	Attaches itself to files and spreads when the infected file is opened.
4. Worm	Self-replicates and spreads automatically through networks without user action.
5. Trojan Horse	Disguises itself as legitimate software but secretly performs malicious actions.
6. Ransomware	Encrypts files and demands payment (ransom) to restore access.
7. Spyware	Secretly monitors user activities and steals sensitive information.
8. Adware	Displays unwanted advertisements and may track user behavior.

Step 2: Textbook Block Diagram

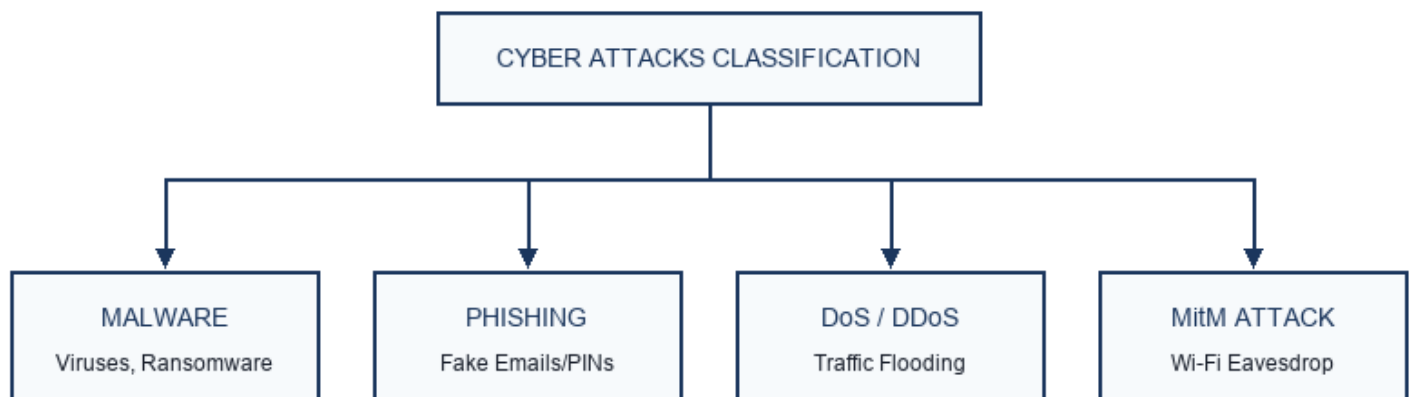


Figure: Textbook Classification Diagram of Cyber Attack Types

Q1.b. What is VPN? Explain about anti malicious software.

1. Definition of VPN.

A Virtual Private Network (VPN) is a network security service that creates a safe, encrypted tunnel over an untrusted public network like the Internet. It masks the user's real public IP address and encrypts all data payload, allowing safe remote access to company networks.

2. Explanation of Anti-Malicious Software.

Anti-Malicious Software (Antivirus/Anti-Malware) is a security program designed to prevent, detect, quarantine, and eliminate malicious software (viruses, worms, ransomware, trojans).

Working Mechanism

- **File Interception:** Intercepts any file being opened, downloaded, or executed on the computer.
- **Signature Matching:** Scans the file code and matches it against the local virus signature library.
- **Behavior Monitoring:** Checks if the file attempts illegal actions (like modifying system registry or encrypting files).
- **Threat Isolation:** If malware is detected, the software blocks execution and moves the file to **Quarantine**.
- **Removal & Cleaning:** Deletes the malicious file or repairs damaged system files.

Q2.a. What is cryptography? Write about digital signature.

Cryptography is the science of protecting information by transforming readable plaintext into unreadable secret ciphertext using mathematical keys, ensuring data confidentiality, integrity, and authenticity.

Explanation of Digital Signature.

A Digital Signature is a cryptographic mathematical technique used to validate the Authenticity (identity of sender), Integrity (message not tampered), and Non-Repudiation (sender cannot deny) of digital documents using Asymmetric Cryptography.

How It Works:

1. Sender hashes document \$M\$ to get Hash Value \$H\$.
2. Sender encrypts Hash \$H\$ using their Private Key to form Digital Signature \$\$.
3. Receiver decrypts Signature \$\$ using Sender's Public Key to get Hash A.
4. Receiver hashes received document to get Hash B. If Hash A == Hash B, signature is authentic.

Q2.b. Explain why SSL is required in an e-commerce website.

Secure Sockets Layer (SSL) / Transport Layer Security (TLS) is a standard security protocol that establishes an encrypted link between a web browser and an e-commerce web server. SSL is essential on e-commerce websites because customers transmit sensitive credit card numbers, passwords, and personal address details that must be protected against online theft.

Step 2: Textbook Block Diagram

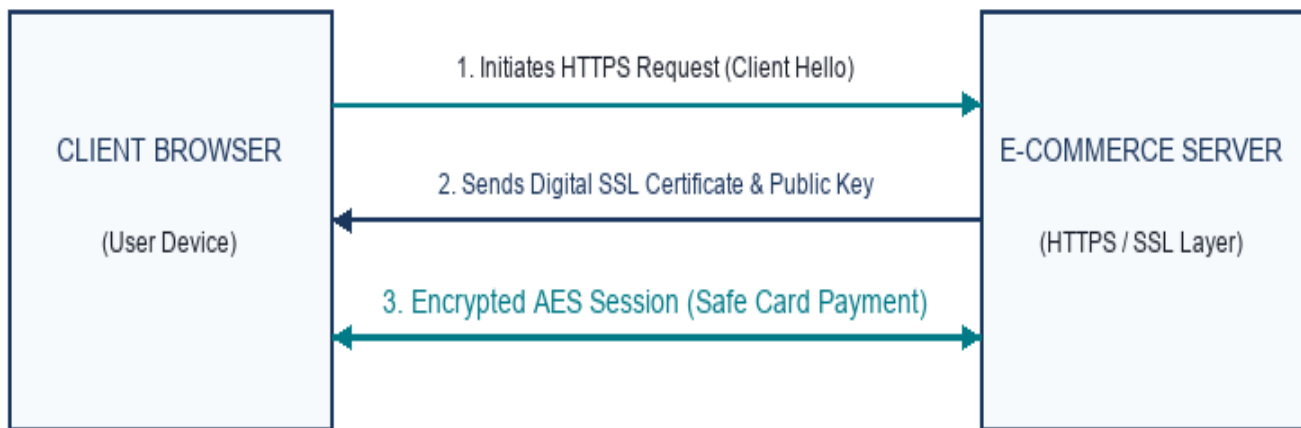


Figure: Textbook Handshake Diagram of SSL/TLS Encrypted E-Commerce Connection

Features of SSL in E-Commerce.

- **HTTPS Protocol:** Enables secure HTTP communication over port 443 with padlock icon.
- **Strong Encryption:** Encrypts data in transit using AES-256 encryption keys.
- **Server Authentication:** Verifies server identity via Digital Certificates from Certificate Authorities.
- **Data Integrity:** Uses HMAC hashing to prevent middleman packet alteration.
- **Session Protection:** Generates unique session keys for every online checkout session.

Step 5: Advantages.

1. **Encrypts Credit Card Data:** Prevents packet sniffers from stealing card PINs.
2. **Prevents Phishing Impersonation:** Validates genuine domain identity to customers.
3. **Boosts Customer Trust:** Green padlock icon increases sales conversions.

Step 6: Disadvantages / Limitations .

1. **Certificate Cost:** Commercial wildcard SSL certificates require yearly renewal fees.
2. **Expiration Risk:** Expired SSL certificates display scary browser warning screens.

Q3.a. What is privacy? Explain cyber law in Nepal.

Privacy is an individual's fundamental right to control how their personal identifiable information (PII) is collected, stored, processed, and shared by digital systems without unauthorized surveillance or data leaks.

#Explanation of Cyber Law in Nepal.

Cyber Law in Nepal is primarily governed by the Electronic Transaction Act (ETA) 2063 (2006 BS). It provides legal governance over electronic records, digital signatures, and cyber crimes across Nepal.

Key Highlights:

- Validates electronic records, e-commerce contracts, and digital signatures legally.
- Criminalizes computer hacking, virus spreading, and source code damage (Sections 44-52).
- Formed Controller of Certification Authorities (CCA) & specialized IT Tribunals.

Q3.b. What is information security process? Explain information security best practice.

Information Security (InfoSec) Process is an ongoing management lifecycle of policy formulation, risk assessment, technical controls implementation, and continuous auditing designed to protect corporate data assets against security threats.

2. Explanation of InfoSec Best Practices.

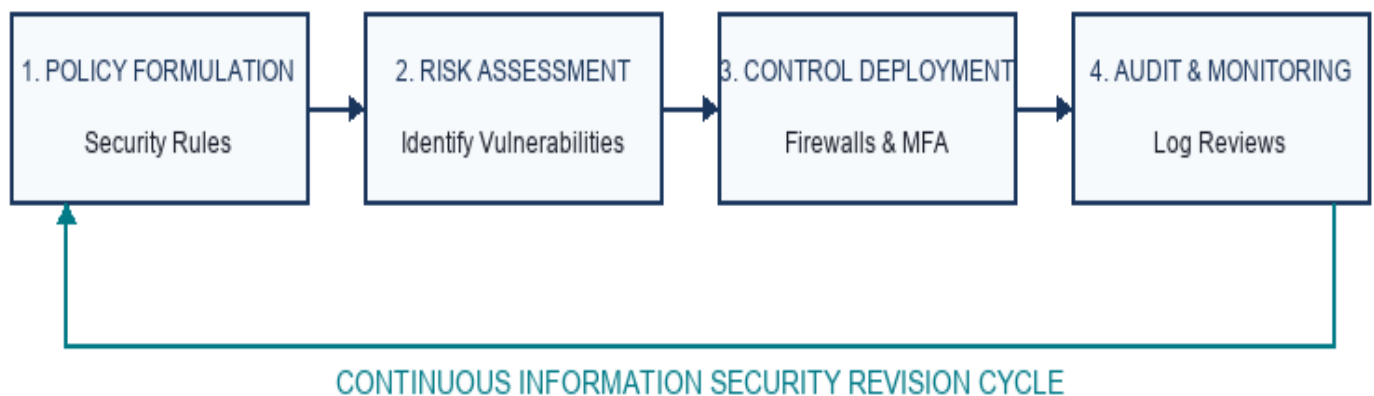


Figure: Textbook Cycle Diagram of Information Security Lifecycle

Core Best Practices:

1. Multi-Factor Authentication (MFA): Enforcing 2FA/MFA for all admin and user logins.
2. Regular Data Backups: Performing automated offline 3-2-1 backups to recover from ransomware.
3. Principle of Least Privilege (PoLP): Granting users minimal system permissions required for work.

4. Patch Management: Updating operating systems and software applications promptly to fix bugs.

5. Employee Security Awareness Training: Educating staff against phishing email traps.

Q4.a. Define intellectual property. What are different types of intellectual property? Explain in brief.

Definition of Intellectual Property (2.5 to 3 Lines):

Intellectual Property (IP) refers to creations of the human mind protected by law, such as software source code, proprietary algorithms, technological inventions, trade secrets, designs, and brand logos.

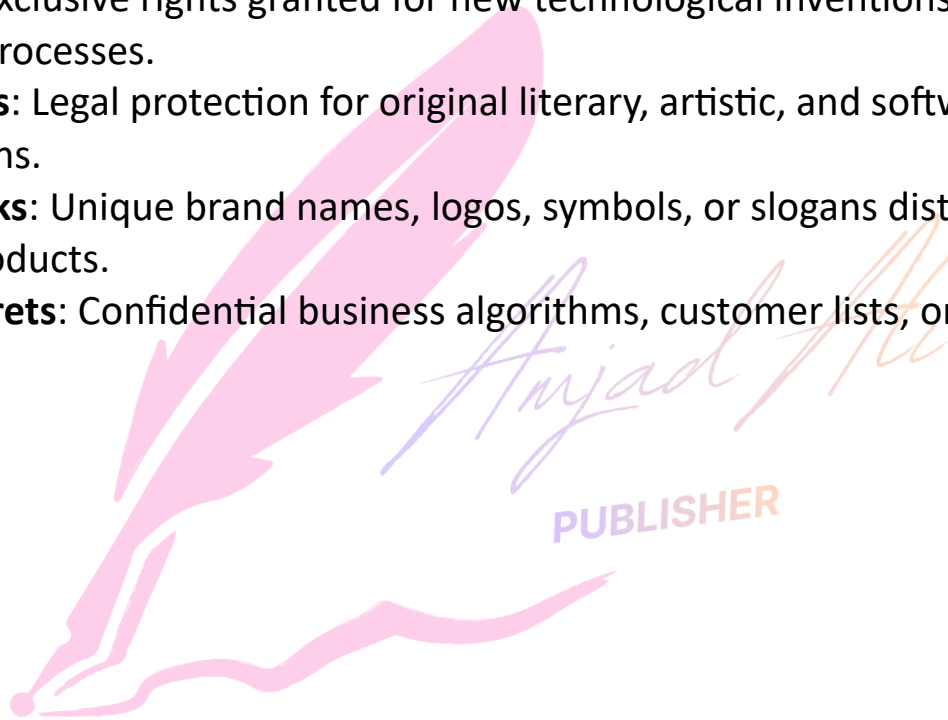
Different Types of Intellectual Property (4 Types Explained in Brief):

1. Patents: Exclusive rights granted for new technological inventions, hardware designs, or processes.

2. Copyrights: Legal protection for original literary, artistic, and software source code creations.

3. Trademarks: Unique brand names, logos, symbols, or slogans distinguishing company products.

4. Trade Secrets: Confidential business algorithms, customer lists, or proprietary source code.



Q4.b. What is ethical dissent and whistle blowing? Explain the role of the professional in public policy.

Ethical Dissent is a professional's internal disagreement with illegal or unethical company actions. Whistle-Blowing is exposing internal corporate wrongdoing, safety violations, or data privacy crimes to public law enforcement when public safety or rights are compromised.

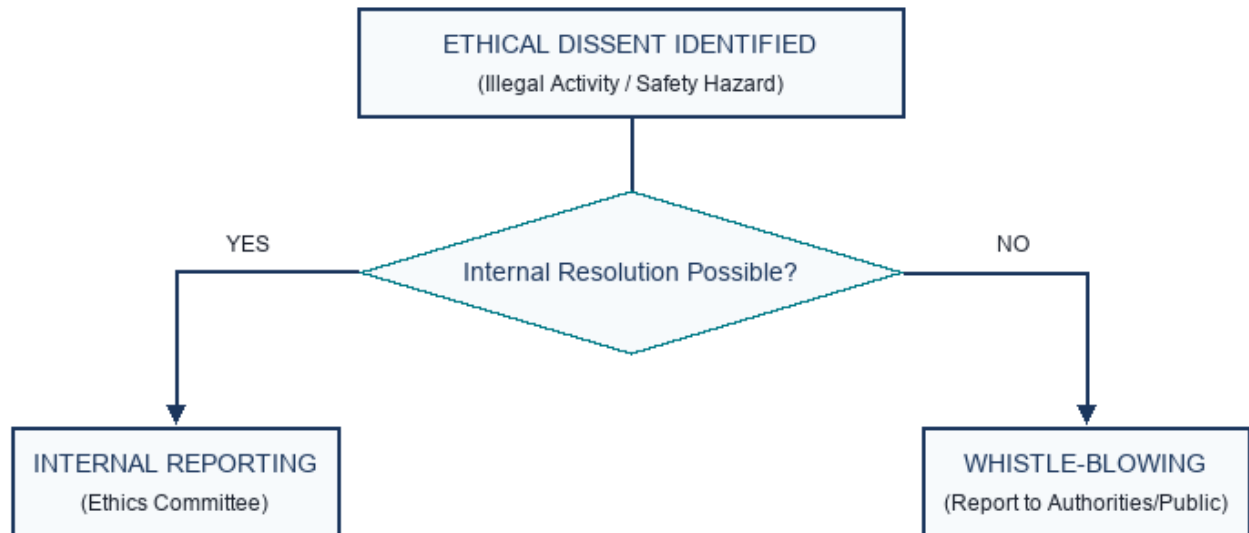


Figure: Textbook Flowchart Diagram of Whistle-Blowing Decision Process
Role of Professional in Public Policy .

1. **Advising Lawmakers:** Providing technical expertise to draft effective cyber security laws.
2. **Protecting Public Safety:** Ensuring digital infrastructure (banking, healthcare) operates ethically.
3. **Reporting System Vulnerabilities:** Responsibly disclosing critical software bugs affecting public users.
4. **Promoting Data Privacy:** Advocating for user privacy rights in government technology projects.

Q5. Write short notes on: (any TWO).

a. Cyber Security and Risk Assessment

Cyber Security Risk Assessment is the formal process of identifying, analyzing, and evaluating security risks to an organization's digital assets. It helps management understand vulnerabilities and deploy appropriate technical controls.

Key Points (7 Points):

1. Identifies critical digital assets like customer databases and payment servers.
2. Evaluates potential threat vectors like ransomware, phishing, and insider leaks.

3. Calculates Risk Score = Likelihood of Attack x Impact on Business.
4. Prioritizes security budgets toward high-risk vulnerabilities.
5. Helps choose risk responses: Risk Mitigation, Avoidance, Transference, or Acceptance.
6. Ensures compliance with national cyber laws and ISO 27001 security standards.
7. Conducted periodically to maintain a strong corporate security posture.

b. Internet Fraud

Internet Fraud refers to any fraudulent scheme or deceptive trick performed online using web applications, email, or software to steal money, property, or sensitive data from victims.

Key Points (7 Points):

1. Includes Phishing emails tricking users into entering online banking passwords.
2. Encompasses Identity Theft to open unauthorized bank loans in victim's name.
3. Involves Advance Fee Fraud (419 scams) promising non-existent cash rewards.
4. Uses fake e-commerce shopping sites to collect money without shipping products.
5. Employs fake tech support pop-ups demanding payment to fix fake viruses.
6. Prevented through user security awareness and Multi-Factor Authentication (MFA).
7. Punished legally under cyber law with heavy fines and prison sentences.

c. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is an automated security monitoring tool that analyzes network traffic and system logs for malicious attack signatures or policy violations and alerts administrators.

Key Points (7 Points):

1. Acts as a passive security monitor analyzing data traffic copies.
2. Signature-Based IDS matches traffic against known attack signature databases.
3. Anomaly-Based IDS detects deviations from normal baseline network traffic.
4. Network IDS (NIDS) monitors network subnet traffic at strategic choke points.
5. Host IDS (HIDS) monitors internal operating system log files and file modifications.
6. Generates real-time alerts for Security Operations Center (SOC) teams.
7. Essential early-warning defense component for corporate cyber security.

CTEVT DIPLOMA IN IT (DCOM-IT III/II)

Subject: Cyber Security & Social Ethics | Exam Paper Solutions (2080 Magh/Falgun
Master Solved Exam Question Bank

Q1.a. Why cyber security is needed? Explain different types of hacker.

Why Cyber Security is Needed.

Cyber Security is needed to protect organizational data assets, financial transactions, and computer networks from unauthorized hacking, data breaches, and malicious malware attacks. It ensures business operational continuity, safeguards user privacy rights, and maintains compliance with national cyber laws.

2. Explanation of Types of Hackers .

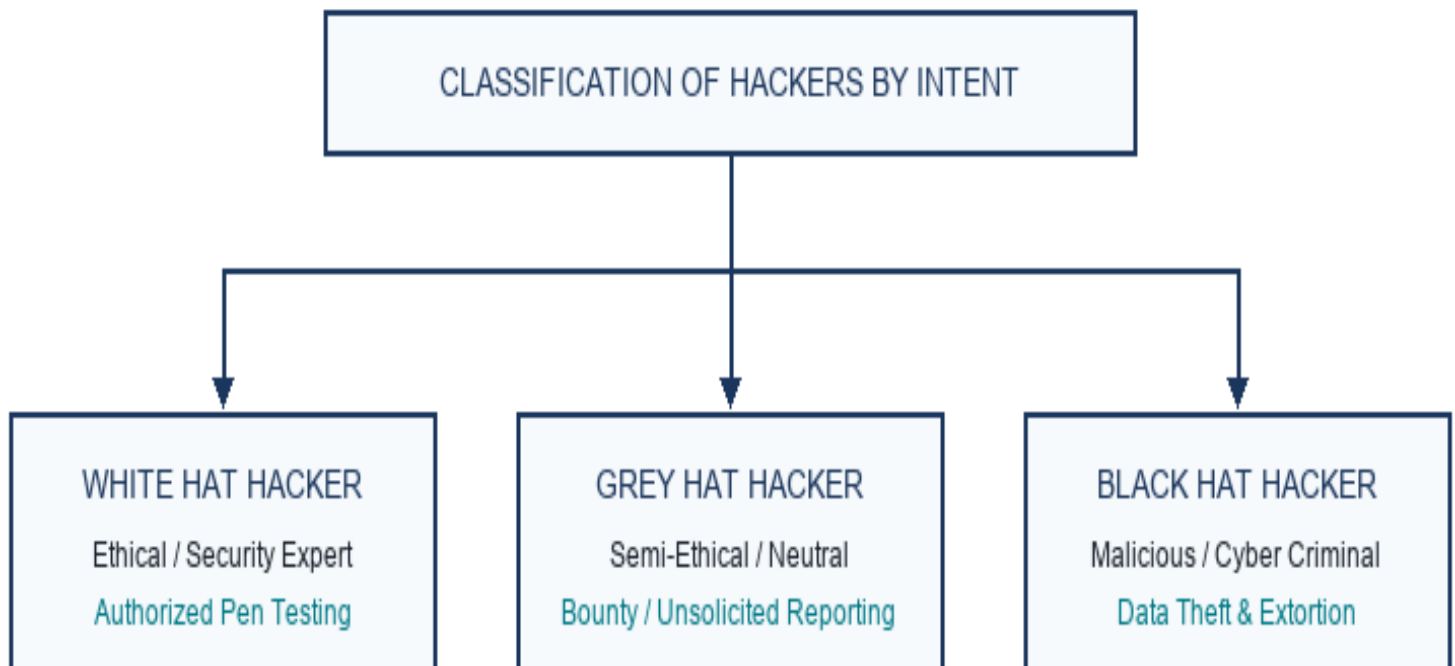


Figure: Textbook Block Diagram of Hacker Classifications

- **White Hat Hacker:** Ethical and authorized security experts who perform penetration testing to locate and patch system vulnerabilities.
- **Black Hat Hacker:** Unethical and illegal malicious hackers who break into computer systems to steal money, lock files, or exfiltrate data.
- **Grey Hat Hacker:** Semi-ethical hackers who find vulnerabilities without authorization, then report them to owners for a bug bounty fee.

Q1.b. Explain about anti-malicious software.

Explanation.

Anti-Malicious Software (Antivirus / Anti-Malware) is a specialized security program designed to prevent, detect, quarantine, and eliminate malicious software (viruses, worms, ransomware, trojans, spyware) from computer systems. It operates 24/7 scanning active memory, incoming downloads, and system files.

Step 2: Textbook Block Diagram

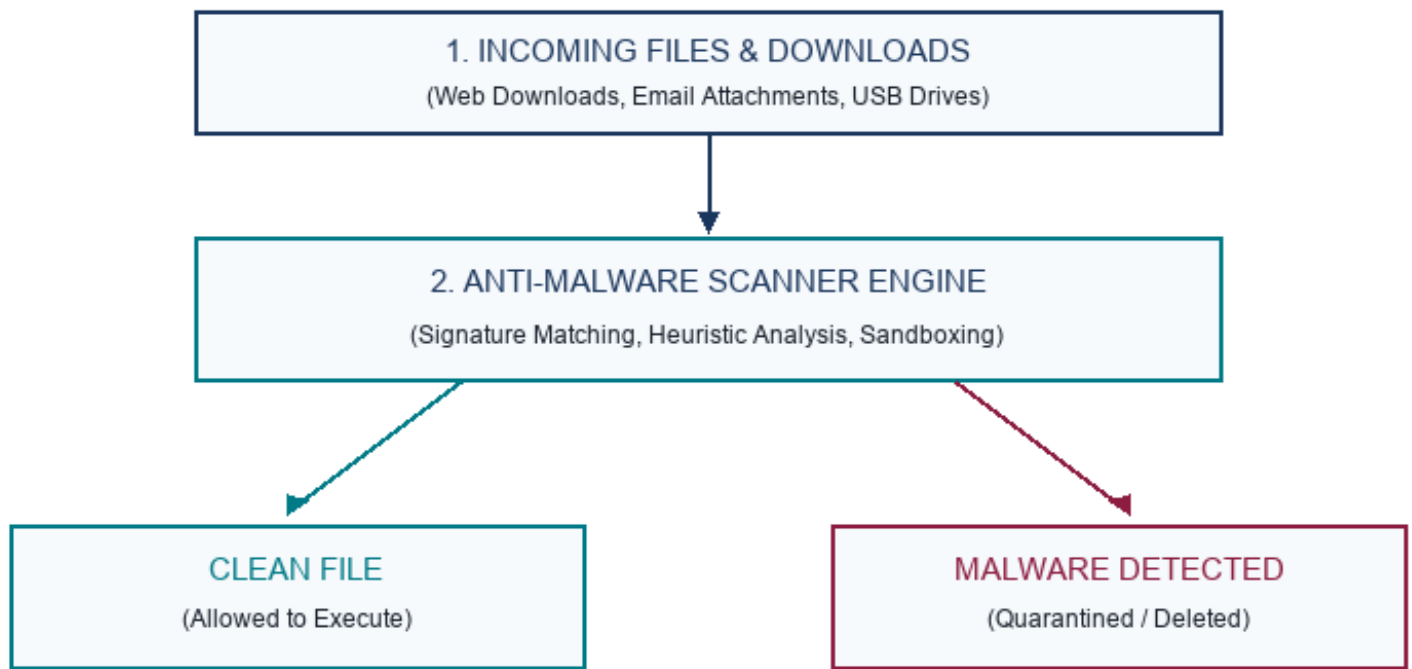


Figure: Textbook Scanning Architecture of Anti-Malicious Software

Features

- Real-Time Monitoring: Scans files being opened, downloaded, or executed continuously.
- Signature Matching: Compares file hash signatures against a known malware database.
- Heuristic Analysis: Examines code structure to detect new unknown malware variants..

Working.

- Intercepts new files arriving via web downloads, USBs, or email attachments.
- Reads file headers and compares code hashes against signature databases.
- Monitors process behavior for unauthorized system modifications.

Step 5: Advantages (5 Points)

1. Blocks Malware Infection: Protects PC from ransomware, worms, and trojans.
2. Safeguards Confidential Data: Prevents spyware from logging banking PINs.
3. Safe Web Browsing: Blocks malicious phishing websites and drive-by downloads.

Step 6: Disadvantages / Limitations (5 Points)

1. System Resource Overhead: Heavy background scanning can slow down low-end PCs.
2. Zero-Day Vulnerability: May miss brand-new malware lacking a signature.

Q2.a. Explain asymmetric key cryptography.

Asymmetric Key Cryptography (Public Key Cryptography) is a cryptographic method that uses a mathematically linked pair of keys: a Public Key (used for encryption and open to everyone) and a Private Key (used for decryption and kept strictly secret by the owner). Data encrypted with the Public Key can only be decrypted by the matching Private Key.

Step 2: Textbook Block Diagram

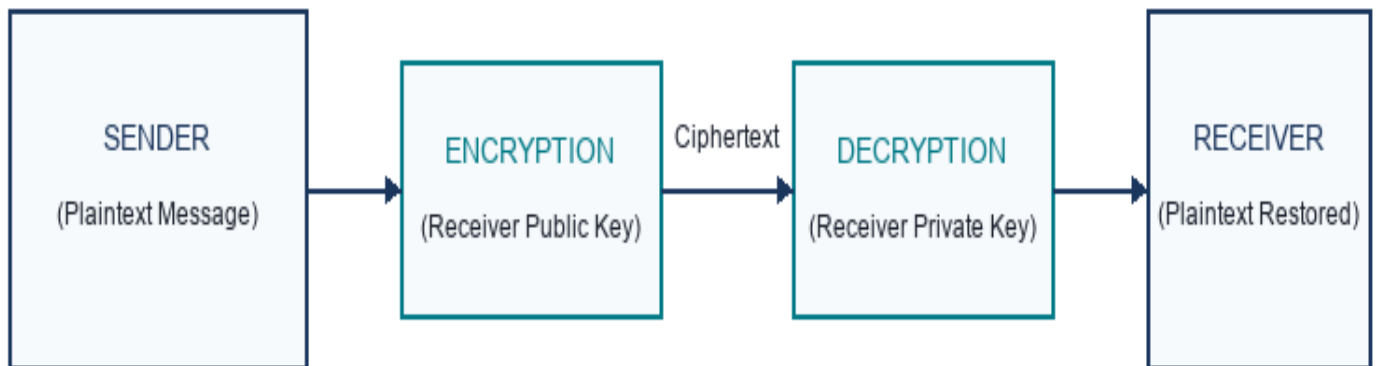


Figure: Textbook Block Diagram of Asymmetric Key Cryptography

Features.

- Dual Key Pair: Uses distinct Public Key (encrypt) and Private Key (decrypt).
- Solves Key Distribution Problem: Public key can be shared openly across public internet.
- Supports Digital Signatures: Provides authentication, integrity, and non-repudiation.

Working

- Key Generation: User generates mathematically linked Public and Private key pair.
- Public Key Sharing: Receiver shares Public Key with Sender openly.
- Encryption: Sender encrypts Plaintext message M using Receiver's Public Key.
- Transmission: Ciphertext C is transmitted safely across public internet channels.
- Decryption: Receiver uses secret Private Key to decrypt C back to Plaintext M.

Advantages

1. High Security Level: Secret private keys never need to be transmitted.
2. Supports Non-Repudiation: Senders cannot deny creating digital signatures.

Disadvantages / Limitations ()

1. Slow Execution Speed: Computationally slower than symmetric AES encryption.
2. High CPU & Memory Usage: Requires heavy mathematical exponentiation.

Q2.b. Write about cyber law in Nepal.

Cyber Law in Nepal is primarily governed by the Electronic Transaction Act (ETA) 2063 (2006 BS). It establishes legal rules for electronic records, digital signatures, e-commerce, and penalizes digital crimes.

Key Highlights of ETA 2063 in Nepal:

- 1. Legal Validation:** Grants legal recognition to electronic contracts, e-banking, and digital signatures.
- 2. Controller of Certification Authority (CCA):** Regulates digital key certificates across Nepal.
- 3. Hacking Penalties (Section 44):** Penalizes unauthorized computer access with fines up to NRs 200,000 and 3 years imprisonment.
- 4. System Damage (Section 45):** Punishes spreading viruses or destroying computer source code.
- 5. Online Content Regulation (Section 47):** Prohibits publishing illegal, obscene, or defamatory content online.
- 6. IT Tribunal Setup:** Formed special IT courts for fast legal trial of cyber crime cases.

Q3.a. What do you mean by freedom of speech? Explain.

Freedom of Speech is a fundamental human right to express opinions, share ideas, and publish information online without fear of government censorship or unlawful retaliation. In the digital age, it empowers citizens to participate in online journalism, social media discussions, and democratic debates.

Key Aspects & Boundaries in Digital Space:

- **Digital Expression:** Protects blogs, social media posts, and online news outlets.
- **Reasonable Restrictions:** Freedom of speech is not absolute; it excludes hate speech, incitement to violence, online child abuse, and criminal defamation.
- **Cyber Security Balance:** Cyber laws must balance national security against over-censorship of public rights.

Q3.b. How can you deal with cyber harassment and discrimination?

Dealing with cyber harassment and discrimination requires a calm, proactive approach. Do not reply to or engage with the abusers, as this often makes things worse. Save all proof by taking screenshots of the posts, messages, or comments, and report the behavior immediately to the website or app

Core Action Steps.

- **Preserve Evidence:** Take clear screenshots of abusive posts, messages, sender profiles, and URLs.
- **Block & Report:** Immediately block the harasser and report the account to social media support.
- **Privacy Hardening:** Change passwords, enable Multi-Factor Authentication (MFA), and restrict post privacy.
- **Do Not Engage:** Refuse to respond to harassers, as reactions encourage further abuse.
- **File Legal Police Complaint:** Report the incident to the Cyber Bureau of Nepal Police with evidence.

Q4.a. What is cryptography? Explain digital signature models.

Cryptography is the science of protecting information by transforming readable plaintext into unreadable ciphertext using secret mathematical keys.

Digital Signature Models:

@ Explain digital signature models.

A Digital Signature Model is a cryptographic framework that defines how a sender generates a digital signature on an electronic document and how a receiver verifies its authenticity. It combines cryptographic hash functions with asymmetric (Public-Private Key) encryption algorithms to guarantee the Authenticity, Data Integrity, and Non-Repudiation of electronic messages and documents.

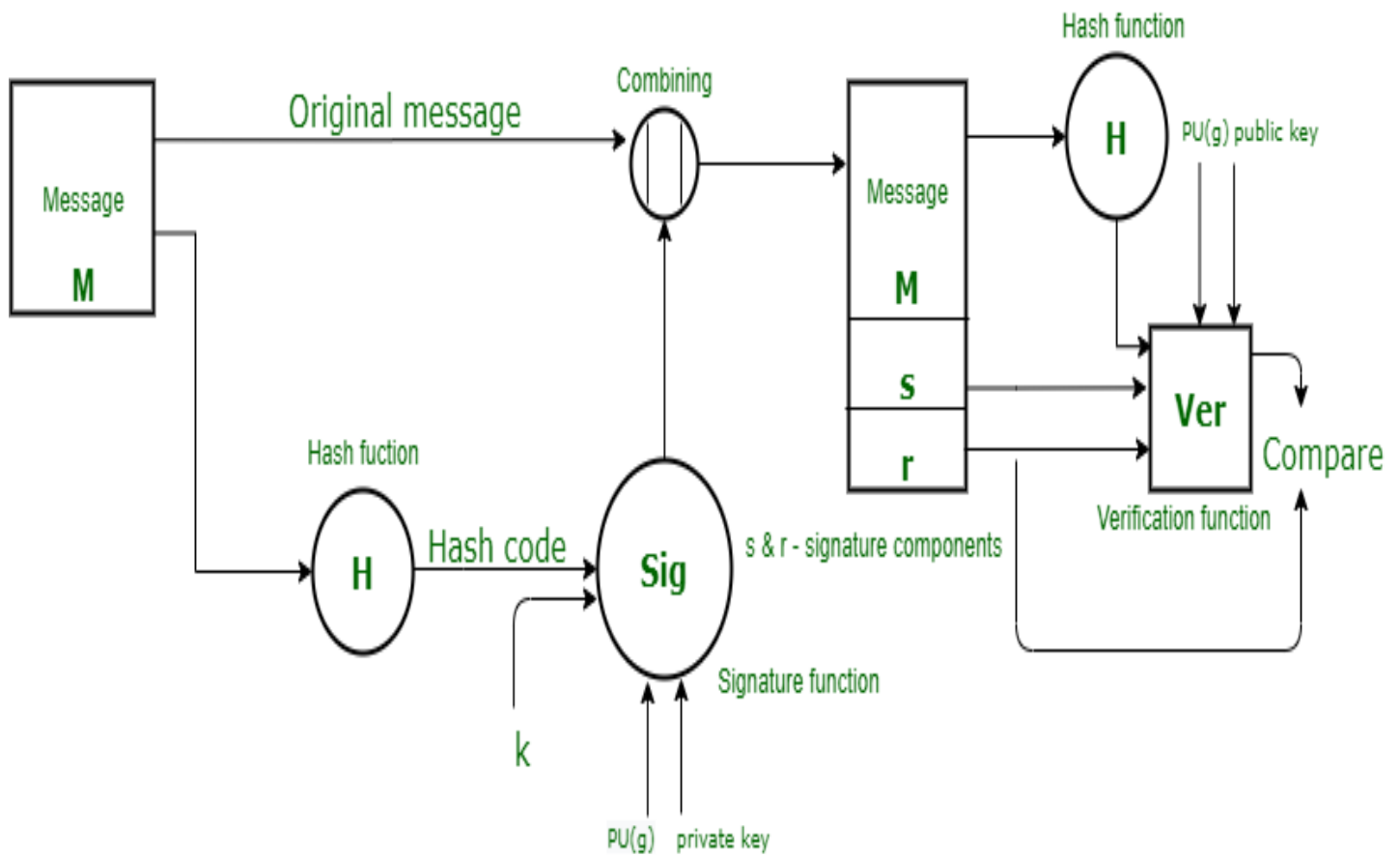
Features & Security Properties of Digital Signature Models.

- **Authentication:** Confirms the true identity of the sender who generated the digital signature.
- **Data Integrity:** Guarantees that the document content was not altered or tampered with during transit.
- **Non-Repudiation:** Prevents the sender from denying having signed and sent the original document.
- **Asymmetric Key Basis:** Relies on a Private Key for signing and a matching Public Key for verification.

- **Fixed-Length Hash Input:** Signs a fixed-length mathematical digest (hash value) rather than the raw large file.

SENDER A

RECEIVER B



Q4.b. Explain whistle-blowing in ethical responsibilities of cyber security.

Whistle-Blowing in cyber security refers to the ethical act of an employee or IT professional exposing internal corporate wrongdoing, hidden security vulnerabilities, or illegal data privacy breaches to public authorities when internal management refuses to act and public safety or citizen privacy is compromised.

Textbook Block Diagram



ETHICAL WHISTLE-BLOWING PROCESS IN CYBER SECURITY

Figure: Textbook Flowchart of Whistle-Blowing Process in Ethical Cyber Security

Core Ethical Responsibilities

- Protecting Public Interest: Exposing severe security risks affecting citizen privacy or financial safety.
- Internal Reporting First: Attempting internal escalation to senior management or ethics committees first.
- Responsible Disclosure: Reporting critical system flaws to law enforcement or bug bounty programs.
- Truthful Evidence: Providing accurate, un-tampered documentary proof of company negligence.
- Protecting User Privacy: Ensuring whistle-blowing actions do not leak innocent customer data.

Q5. Write short notes on: (Any Two).

a. Internet Fraud

Internet Fraud refers to any fraudulent scheme or deceptive trick performed online using web applications, email, or software to steal money or sensitive data from victims.

Key Points (7 Points):

1. Includes Phishing emails tricking users into revealing online banking passwords.
2. Encompasses Identity Theft to open unauthorized bank loans in victim's name.

3. Involves Advance Fee Fraud (419 scams) promising non-existent cash rewards.
4. Uses fake e-commerce shopping sites to collect money without shipping products.
5. Employs fake tech support pop-ups demanding payment to fix fake viruses.
6. Prevented through user security awareness and Multi-Factor Authentication (MFA).
7. Punished legally under cyber law with heavy fines and prison sentences.

b. Software Risk

Software Risk refers to the probability of operational failure, security vulnerabilities, or project delays arising from defects in software requirement, design, or source code.

Key Points (7 Points):

1. Caused by unvalidated user input leading to SQL injection or XSS vulnerabilities.
2. Arises from inadequate security testing during software development lifecycle (SDLC).
3. Includes reliance on outdated third-party open-source code libraries.
4. Can result in system crashes, data corruption, or unauthorized database breach.
5. Mitigated through static code analysis and regular penetration testing audits.
6. Managed by establishing secure coding standards and patch management policies.
7. Essential focus area for software engineers and cyber security auditors.

c. Firewall

A Firewall is a critical network security system that acts as a protective barrier between a trusted internal network and an untrusted external network like the Internet. It monitors and filters incoming and outgoing network traffic based on predefined security rules.

Key Points (7 Points):

1. Filters network traffic based on IP address, port numbers, and protocols.
2. Operates at stateless (L3/L4) or stateful/proxy (L7) application layers.
3. Prevents unauthorized hackers from entering private corporate networks.
4. Maintains Access Control Lists (ACLs) and connection state tables.
5. Provides detailed event logs of all blocked intrusion attempts.
6. Hides internal company IP addresses from external internet scanners.
7. Essential perimeter defense tool for corporate cyber security.

d. Trademarks

A Trademark is an Intellectual Property Right (IPR) that legally protects unique brand signs, names, logos, symbols, or slogans distinguishing a company's products from competitors.

Key Points (7 Points):

1. Grants exclusive legal rights to a company to use its brand logo in marketplace.
2. Prevents competitors from creating fake copies or using similar confusing logos.
3. Represented legally by symbols like [™] (Unregistered) or [®] (Registered).
4. Protects company web domain names (e.g. `esewa.com.np`) from cybersquatting.
5. Preserves customer trust and business brand identity in digital space.
6. Can last indefinitely as long as the owner renews registration periodically.
7. Enforced under intellectual property and cyber laws again.

CTEVT DIPLOMA IN COMPUTER ENGINEERING (DCE III/I)

Subject: Cyber Security & Professional Ethics | Exam Paper Solutions (2079 Bhadra/Ashwin

Master Solved Exam Question Bank

Q1.a. Define cyber Security. Briefly explain about the different techniques used by a hacker.

1. Definition of Cyber Security (2.5 to 3 Lines)

Cyber Security refers to the body of technologies, processes, practices, and controls designed to protect computers, networks, software programs, and data from unauthorized access.

Explanation of Techniques Used by a Hacker

Hackers use different techniques to gain unauthorized access to computers, networks, or online accounts. Some common techniques are:

1. Phishing

- Hackers send fake emails, messages, or websites to trick users into revealing passwords, banking details, or personal information.

2. Malware Attack

- They use malicious software such as viruses, worms, trojans, ransomware, or spyware to damage systems, steal data, or monitor user activities.

3. Password Attacks

- Hackers try to guess or crack passwords using methods like brute force attacks, dictionary attacks, or credential stuffing.

4. Social Engineering

- They manipulate people into sharing confidential information by pretending to be trusted individuals or organizations.

5. SQL Injection

- Hackers insert malicious SQL code into website input fields to access, modify, or delete database information.

6. Cross-Site Scripting (XSS)

- They inject harmful scripts into web pages to steal user cookies, session data, or other sensitive information.

7. Denial-of-Service (DoS/DDoS) Attack

- Hackers flood a server or website with excessive traffic, making it slow or unavailable to legitimate users.

Q1.b. Define Firewall. Explain in brief about its types.

A Firewall is a network security system that acts as a protective barrier between a trusted internal network and an untrusted external network like the Internet

Types of Firewalls Explained in Brief:

- 1. Packet Filtering Firewall (Stateless):** Inspects headers at L3/L4 layers (IP, Port) against ACL rules.
- 2. Stateful Inspection Firewall:** Tracks active TCP connection states in a State Table.
- 3. Application-Level Gateway (Proxy):** Inspects L7 application data payloads (HTTP, FTP).
- 4. Next-Generation Firewall (NGFW):** Integrates stateful filtering with DPI, IPS, and SSL decryption.

Q2.a. Explain why SSL is required in an e-commerce website?

Secure Sockets Layer (SSL) / Transport Layer Security (TLS) is an essential cryptographic protocol that establishes an encrypted link between a web browser and an e-commerce server. SSL is required on e-commerce sites because customers transmit sensitive credit card details, passwords, and personal addresses that must be protected against online eavesdropping.

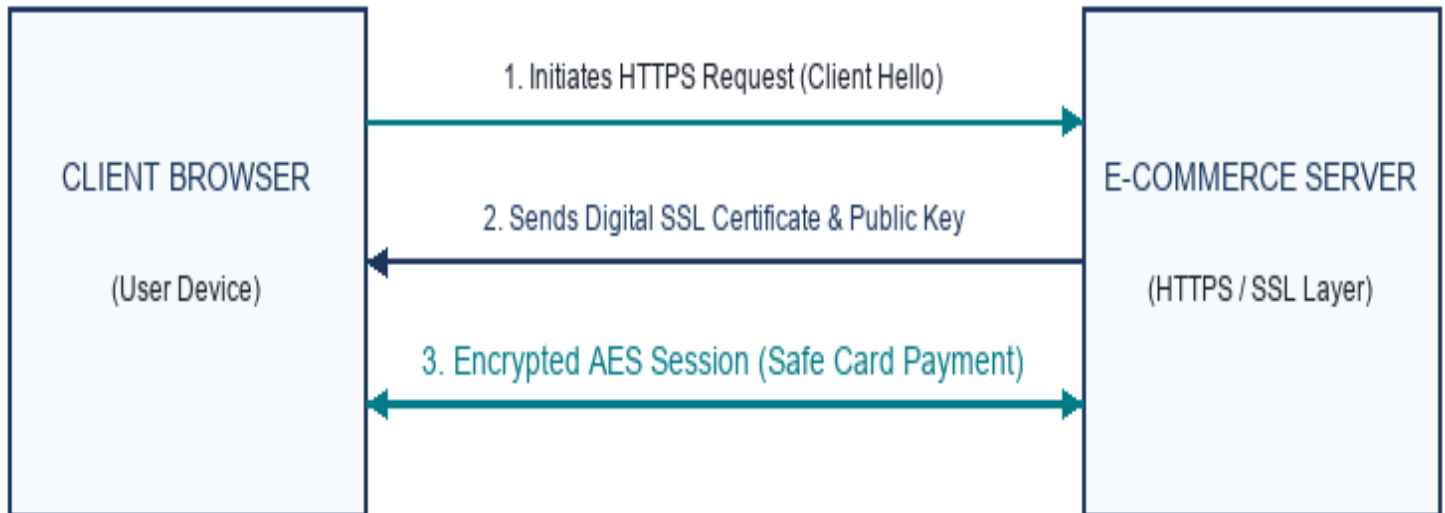


Figure: Textbook SSL/TLS Encrypted E-Commerce Handshake Diagram

Features

- **HTTPS Protocol:** Enables secure HTTP communication over port 443 with padlock icon.
- **Strong Encryption:** Encrypts data in transit using AES-256 session keys.
- **Server Authentication:** Validates server identity via Digital Certificates from trusted CAs.

Why SSL is Required in an E-commerce Website

SSL (Secure Sockets Layer) is a security technology that encrypts the data transferred between a user's browser and an e-commerce website, ensuring safe online transactions.

Importance of SSL in an E-commerce Website

1. Encrypts Sensitive Data

- Protects customer information such as passwords, credit card numbers, and personal details during transmission.

2. Provides Authentication

- Confirms that users are communicating with the genuine website and not a fake one.

3. Protects Against Cyber Attacks

- Prevents hackers from intercepting or stealing data through attacks like Man-in-the-Middle (MITM).

4. Builds Customer Trust

- Displays **HTTPS** and a padlock icon in the browser, assuring customers that the website is secure.

5. Ensures Secure Online Payments

- Safeguards payment transactions and financial information during checkout.

Q2.b. Define Digital Signature? Explain types of Cryptography..

A Digital Signature is a cryptographic mathematical technique used to validate the Authenticity (sender identity), Integrity (message not altered), and Non-Repudiation (sender cannot deny) of a digital document using Asymmetric Cryptography.

Types of Cryptography (Comparison Table & Explanation):

1. Symmetric Key Cryptography (Secret Key)

- Uses **one common key** for both encryption and decryption.
- It is **fast** and suitable for encrypting large amounts of data.
- The main challenge is securely sharing the secret key.
- **Examples:** AES, DES, 3DES.

2. Asymmetric Key Cryptography (Public Key)

- Uses **two different keys**:
 - **Public Key:** Used for encryption.
 - **Private Key:** Used for decryption.
- It provides better security and supports digital signatures.
- It is slower than symmetric encryption.
- **Examples:** RSA, ECC, ElGamal.

3. Hash Function (One-Way Cryptography)

- Converts data into a **fixed-length hash value**.
- It is **one-way**, meaning the original data cannot be recovered from the hash.
- Used to verify data integrity and securely store passwords.
- **Examples:** SHA-256, SHA-3, MD5 (MD5 is no longer considered secure for cryptographic use).

Q3.a. Write about cyber law in Nepal.

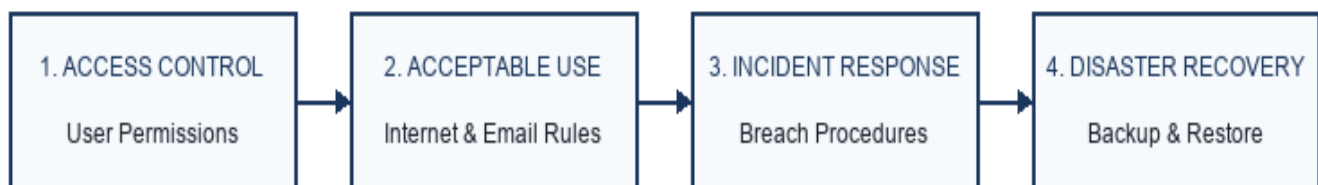
Cyber Law in Nepal is governed by the Electronic Transaction Act (ETA) 2063 (2006 BS). It provides legal governance over electronic records, digital signatures, e-commerce, and penalizes digital crimes across the country.

Key Provisions of ETA 2063:

- **Legal Validation:** Grants legal recognition to electronic records, e-banking, and digital signatures.
- **Controller of Certification Authority (CCA):** Regulates digital keys and certification authorities.
- **Hacking Penalties (Section 44):** Punishes unauthorized computer access with up to NRs 200,000 fine and 3 years jail.
- **Source Code Damage (Section 45):** Penalizes destroying or altering computer programs.
- **Illegal Content (Section 47):** Prohibits publishing offensive or defamatory electronic material.
- **IT Tribunal:** Special courts formed for fast judicial trial of cyber crime cases.

Q3.b. Define Security Policy. Explain brief about its importance.

An Information Security Policy is a formal set of organizational rules, guidelines, and procedures designed to ensure that all employees and IT users comply with data security standards.



CORE COMPONENTS OF INFORMATION SECURITY POLICY

Figure: Textbook Block Diagram of Core Components of Security Policy

Importance of Security Policy .

- **Establishes Clear Security Rules:** Eliminates confusion regarding employee computer usage.
- **Prevents Data Breaches:** Minimizes insider threats and accidental password sharing.
- **Ensures Legal Compliance:** Aligns company operations with Nepal Cyber Law (ETA 2063).

- Guides Incident Response: Speeds up malware containment during security incidents.
- Protects Corporate Reputation: Demonstrates commitment to client data privacy.

Q4.a. Define Ethical dissent and whistle-blowing? Explain the role of the professional in public policy.

Definition of Ethical Dissent & Whistle-Blowing (2.5 to 3 Lines):

Ethical Dissent is a professional's internal disagreement with illegal or unethical company practices. Whistle-Blowing is exposing internal corporate wrongdoing, data privacy violations, or safety hazards to public law enforcement when public safety is threatened.

Role of IT Professional in Public Policy (4 Points):

1. Advising Lawmakers: Providing technical expertise to draft effective cyber security laws.
2. Protecting Public Safety: Ensuring critical digital infrastructure operates ethically.
3. Responsible Bug Disclosure: Reporting system vulnerabilities before hackers exploit them.
4. Advocating Data Privacy: Promoting citizen privacy rights in e-governance projects.

Q4.b. What is code of ethics? How to deal with harassment and discrimination in Nepal? [5 Marks]

Definition of Code of Ethics (2.5 to 3 Lines):

A Code of Ethics is a set of formal moral principles and professional standards established by governing bodies (like IEEE or Nepal Engineering Council) to ensure IT workers exercise technical access honestly and competently.

How to Deal with Cyber Harassment & Discrimination in Nepal (Exact Strategy):

1. Immediate Actions: Save proof (screenshots of messages, posts, URLs), do not reply/engage, block & mute harasser, report abuse on app.
2. Account Privacy: Lock down privacy settings, change passwords, enable Multi-Factor Authentication (MFA).
3. Getting Outside Help: Report to Nepal Police Cyber Bureau (ETA 2063 Section 47), notify HR/school admin, seek support from trusted friends or professionals.

Q5. Write short notes on: (Any Two) [2x5 = 10 Marks] [10 Marks]

a. Software Risk

Software Risk refers to the probability of operational failure, security vulnerabilities, or project delays arising from flaws in software requirements,

architecture, or source code.

Key Points (7 Points):

1. Caused by unvalidated user input leading to SQL injection or XSS bugs.
2. Arises from inadequate security testing during Software Development Lifecycle (SDLC).
3. Includes reliance on outdated third-party open-source code libraries.
4. Can cause system crashes, data corruption, or unauthorized database breach.
5. Mitigated through static code analysis and regular penetration testing audits.
6. Managed by establishing secure coding standards and patch management policies.
7. Essential focus area for software engineers and cyber security auditors.

b. Risk Assessment and Management

Risk Assessment and Management is the systematic process of identifying, analyzing, prioritizing, treating, and monitoring digital risks to an organization's information assets.

Key Points (7 Points):

1. Identifies critical digital assets like databases and payment servers.
2. Evaluates potential threat vectors like ransomware, phishing, and insider leaks.
3. Calculates Risk Score = Likelihood of Attack x Impact on Business.
4. Prioritizes security budgets toward high-risk vulnerabilities.
5. Helps choose risk responses: Risk Mitigation, Avoidance, Transference, or Acceptance.
6. Ensures compliance with national cyber laws and ISO 27001 security standards.
7. Conducted periodically to maintain a strong corporate security posture.

c. Intellectual Property Right (IPR)

Intellectual Property Right (IPR) refers to legal protections granted to creators over intangible innovations, such as software source code, patents, trade secrets, and brand trademarks.

Key Points (7 Points):

1. Protects software source code from unauthorized copying and piracy.
2. Includes Patents for technological hardware inventions and processes.
3. Encompasses Trademarks for unique brand logos and domain names.
4. Safeguards Trade Secrets like proprietary algorithms from corporate espionage.
5. Enables software developers to earn commercial licensing revenue.
6. Enforced digitally via Data Loss Prevention (DLP) and DRM tools.
7. Protected legally under national intellectual property and cyber laws.

d. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is an automated security monitoring tool that analyzes network traffic and system logs for malicious attack signatures or policy violations and alerts administrators.

Key Points (7 Points):

1. Acts as a passive security monitor analyzing data traffic copies.
2. Signature-Based IDS matches traffic against known attack signature databases.
3. Anomaly-Based IDS detects deviations from normal baseline network traffic.
4. Network IDS (NIDS) monitors network subnet traffic at strategic choke points.
5. Host IDS (HIDS) monitors internal operating system log files and file modifications.
6. Generates real-time alerts for Security Operations Center (SOC) teams.
7. Essential early-warning defense component for corporate cyber security.



CTEVT DIPLOMA IN IT ENGINEERING (DCOM-IT III/II)

Subject: Cyber Security & Social Ethics | Exam Paper Solutions (2079/2080 Chaitra/Baishakh -
Master Solved Exam Question Bank

Q1.a. What is cyber crime? Write down different types of attack in cyber.

Cyber Crime refers to any illegal or fraudulent activity performed using computers, mobile devices, or computer networks as a tool to commit the crime or as the primary target.

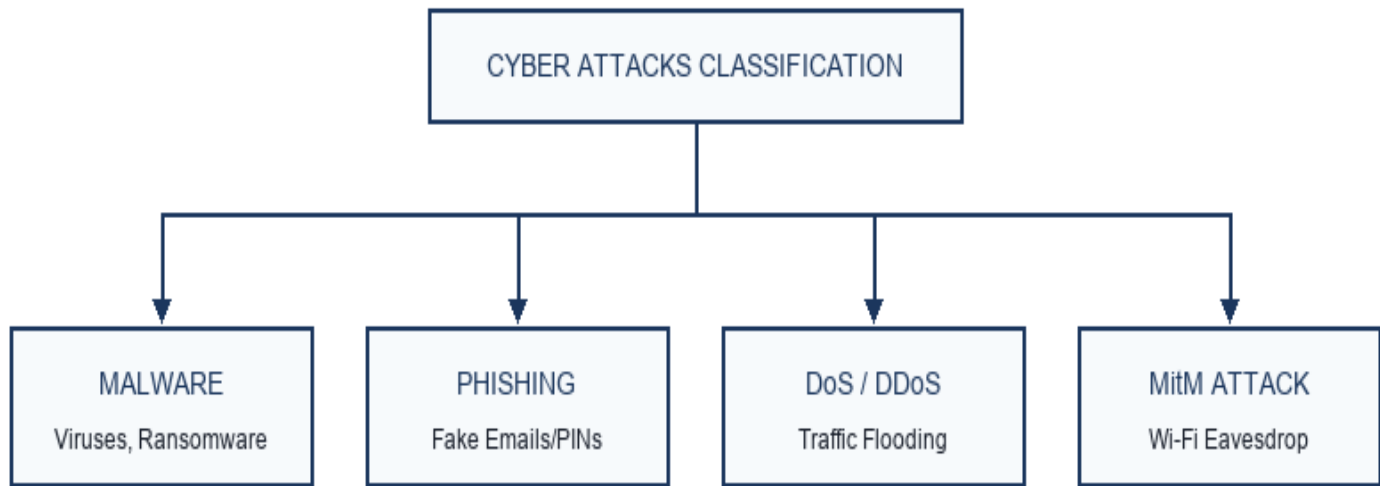


Figure: Textbook Block Diagram of Cyber Attack Types

Types of Cyber Attacks:

- **Malware Attack:** Viruses, Worms, Trojans, and Ransomware locking files or stealing data.
- **Phishing Attack:** Fraudulent emails tricking users into entering credentials on fake websites.
- **Denial of Service (DoS/DDoS):** Flooding servers with fake traffic to crash websites.
- **Man-in-the-Middle (MitM):** Intercepting private Wi-Fi network communications.
- **SQL Injection (SQLi):** Injecting malicious SQL code into web forms to dump backend databases.

Q1.b. Explain SSL and Encryption in brief.

Encryption is the process of scrambling plain data into an unreadable format using mathematical formulas, ensuring only someone with the correct digital key can unlock and read it. SSL (Secure Sockets Layer) is a security protocol that uses this encryption technology to create a safe, private link between a web browser and a website server. [[1](#), [2](#), [3](#), [4](#), [5](#)]

Concepts of Encryption

- Data scrambling: Turns normal readable text into random, jumbled characters.
- Key requirement: Uses specific digital keys to lock (encrypt) and unlock (decrypt) the information.
- Privacy protection: Prevents hackers from reading intercepted data, like passwords or credit card numbers.]

]Concepts of SSL

- Secure connection: Establishes a protected, private pathway for data to travel across the internet.
- The Handshake: Runs a quick background check where your device and the server agree on safety rules and keys.
- Identity check: Verifies that a website is legitimate and belongs to the actual organization, symbolized by the "HTTPS" padlock.
- Modern upgrade: Original SSL has been updated to a newer version called TLS (Transport Layer Security), though most people still call it SSL



Figure: Textbook SSL/TLS Encrypted Connection Block Diagram

Q2.a. What is cryptography? Explain Asymmetric key cryptography.]

Cryptography is the science of protecting information by converting plaintext into ciphertext using secret keys, guaranteeing data confidentiality, integrity, and authenticity.

Explanation of Asymmetric Key Cryptography .

Asymmetric Key Cryptography (Public Key Cryptography) uses a mathematically linked pair of keys: a Public Key (used for encryption and shared openly) and a Private Key (used for decryption and kept strictly secret). Data encrypted with the Public Key can only be decrypted by the matching Private Key.



ASYMMETRIC KEY CRYPTOGRAPHY BLOCK DIAGRAM

Figure: Textbook Block Diagram of Asymmetric Key Cryptography.

: Working

- Receiver generates Public and Private Key pair.
- Receiver shares Public Key with Sender openly.
- Sender encrypts Plaintext message M using Receiver's Public Key.
- Ciphertext C is transmitted across unsecure internet channels.
- Receiver uses secret Private Key to decrypt C back to Plaintext M.

Advantages

1. High Security Level: Secret private key never needs to be transmitted.
2. Supports Non-Repudiation: Senders cannot deny digital signatures.
3. Easy Key Management: Does not require pre-shared secret keys.

Disadvantages / Limitations (

1. Slow Speed: Computationally slower than symmetric AES encryption.
2. High CPU Usage: Requires heavy mathematical exponentiation.
3. Larger Key Sizes: Requires larger key lengths (2048-bit RSA) for security..

Q2.b. What are legal issues in information security? Explain information security process]

Legal issues in information security refer to the complex body of laws, statutory regulations, and legal liabilities that govern how organizations collect, store, process, and protect digital data

' Information Security Process.

Information Security is not a one-time project; it is a continuous, four-step management lifecycle designed to identify, manage, and minimize digital risks. It ensures that an organization's security posture continuously adapts to new cyber threats through an ongoing loop of assessment, protection, monitoring, and incident recovery.



CONTINUOUS 4-STEP INFORMATION SECURITY PROCESS LIFECYCLE

4-Step InfoSec Process (Short Exam Notes)

1. Assess & Identify Risk

- **Asset Inventory:** List all company hardware, software, and sensitive data.
- **Vulnerability Scan:** Find weak spots, unpatched systems, and bugs.

2. Protect & Implement Controls

- **Technical Shields:** Deploy firewalls, encryption, anti-malware, and MFA.
- **Physical Security:** Lock server rooms with biometric access and CCTV..

3. Monitor & Detect Threats

- **24/7 Tracking:** Monitor network traffic continuously for weird anomalies.
- **Log Analysis:** Check system logs to spot unauthorized login attempts.
- **Security Auditing:** Perform regular internal and external security checks.

4. Respond & Recover

- **Incident Response:** Activate IRT team to isolate hacked servers immediately.
- **Business Continuity:** Restore clean offline backups to resume operations fast.

Q3.a. What is computer forensics? What are the steps of collecting computer evidence?.

Computer Forensics is the scientific process of identifying, preserving, extracting, analyzing, and presenting digital evidence from electronic storage media in a court of law.

Steps of Collecting Digital Evidence Block Diagram:



COMPUTER EVIDENCE COLLECTION PROCESS BLOCK DIAGRAM

Figure: Textbook Block Diagram of Digital Evidence Collection Process

Steps of Evidence Collection (Short & Crisp)

1. Identification:

- Locate and identify all target digital media sources (hard disks, SSDs, RAM, USB drives, server logs, mobile phones).

2. Preservation:

- Isolate digital devices from network connections (Faraday bag) and connect hardware **Write-Blockers** to prevent data changes.

3. Extraction / Imaging:

- Create an exact bit-stream duplicate copy (Forensic Image) of the original hard drive using forensic software.
- Generate cryptographic hash values (SHA-256) to prove the copy matches the original.

4. Forensic Analysis:

- Analyze the forensic image using specialized tools (FTK, EnCase, Autopsy) to recover deleted files, chat logs, and browser history.

5. Evidentiary Reporting:

- Compile an objective technical report detailing findings, methods used, and Chain of Custody documentation for court presentation.

Q3.b. Define intellectual property. What are professional ethics.

Intellectual Property (IP) refers to creations of the human mind protected by law, such as software source code, proprietary algorithms, technological inventions, trade secrets, designs, and brand logos.

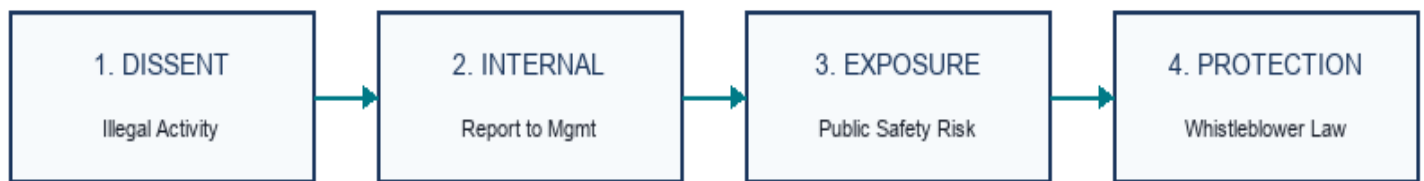
Explanation of Professional Ethics.

Professional Ethics is a set of formal moral principles and standards governing IT workers:

1. Confidentiality: Protecting customer and corporate data privacy.
2. System Integrity: Refusing to use admin access to spy or steal data.
3. Professional Competence: Delivering high-quality, secure code.
4. Legal Compliance: Respecting cyber laws and software copyright licenses.

Q4.a. What is whistle blowing? Write the condition in which whistle blowing is more justified.

Whistle-Blowing is the ethical act of an employee exposing internal corporate wrongdoing, safety hazards, or data privacy crimes to public law enforcement when management refuses to act.



ETHICAL WHISTLE-BLOWING PROCESS BLOCK DIAGRAM

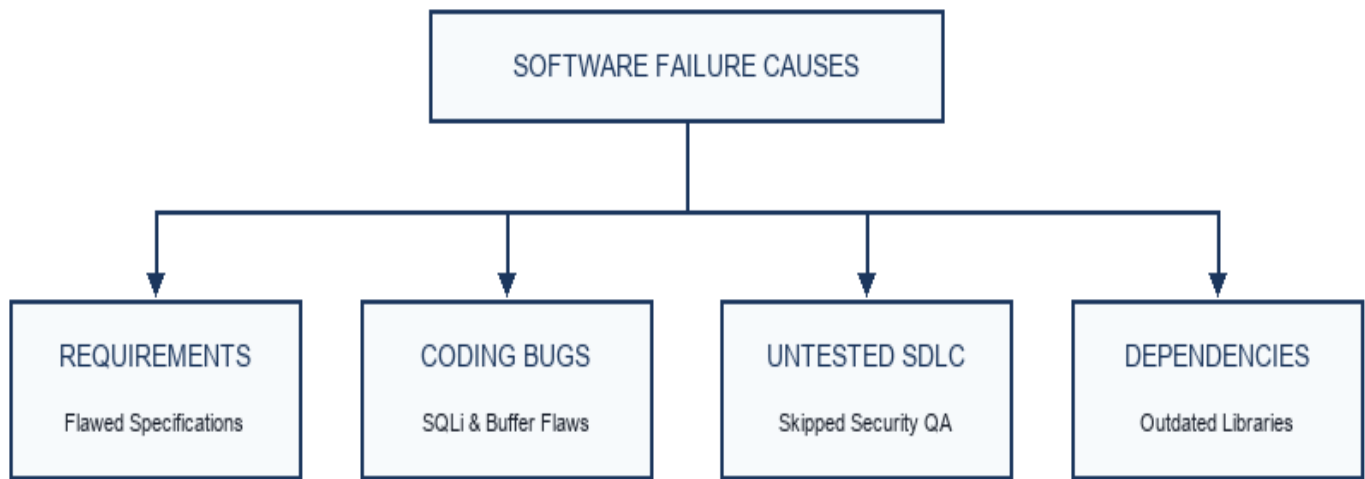
Figure: Textbook Block Diagram of Ethical Whistle-Blowing Process

Conditions When Whistle-Blowing is Justified.

1. Public Safety Risk: Company software flaws directly threaten public health or safety.
2. Illegal Crime: Corporate management is committing severe financial or data privacy fraud.
3. Exhausted Internal Channels: Internal reporting to ethics committees was ignored or suppressed.
4. Clear Documentary Proof: The professional possesses accurate, verified evidence of wrongdoing.

Q4.b. What is software risk? Write the cause of software failure]

Software Risk refers to the probability of operational failure, security vulnerabilities, or project delays arising from flaws in software requirements, architecture, or source code.



PRIMARY CAUSES OF SOFTWARE FAILURE BLOCK DIAGRAM

Figure: Textbook Block Diagram of Causes of Software Failure

Primary Causes (4 Points):

1. Inadequate Requirement Specifications: Misunderstanding user needs or system limits.
2. Unvalidated Code: Poor coding practices leading to SQL injection or buffer overflow bugs.
3. Insufficient Testing: Skipping security testing during Software Development Lifecycle (SDLC).
4. Unpatched Dependencies: Relying on outdated open-source libraries containing known bugs.

Q5. Write short notes on: (Any Two)

a. Trademarks

A Trademark is an Intellectual Property Right (IPR) that legally protects unique brand signs, names, logos, symbols, or slogans distinguishing a company's products from competitors.

Key Points (7 Points):

1. Grants exclusive legal rights to a company to use its brand logo in marketplace.
2. Prevents competitors from creating fake copies or using similar confusing logos.

3. Represented legally by symbols like ™ (Unregistered) or ® (Registered).
4. Protects company web domain names (e.g. `esewa.com.np`) from cybersquatting.
5. Preserves customer trust and business brand identity in digital space.
6. Can last indefinitely as long as the owner renews registration periodically.
7. Enforced under intellectual property and cyber laws against fake websites.

b. Digital Signature

A Digital Signature is a cryptographic mathematical technique used to validate the Authenticity (sender identity), Integrity (message not tampered), and Non-Repudiation (sender cannot deny) of digital documents.

Key Points (7 Points):

1. Uses Asymmetric Cryptography (Private Key signing & Public Key verification).
2. Hashes document using SHA-256 to produce a unique fixed-length hash value.
3. Encrypts hash value with Sender's Private Key to form Digital Signature.
4. Receiver decrypts signature with Sender's Public Key to verify integrity.
5. Legally binding for e-commerce, digital contracts, and banking under ETA 2063.
6. Any single bit change in document invalidates the entire signature.
7. Eliminates paper contracts and enables secure paperless digital workflows.

c. Cyber Law in Nepal

Cyber Law in Nepal is governed by the Electronic Transaction Act (ETA) 2063 (2006 BS). It provides legal rules for electronic records, digital signatures, e-commerce, and penalizes digital crimes.

Key Points (7 Points):

1. Grants legal recognition to electronic records, e-banking, and digital signatures.
2. Establishes the Controller of Certification Authorities (CCA) for digital keys.
3. Section 44 penalizes unauthorized computer hacking and system access.
4. Section 45 penalizes damage to computer source code and software programs.
5. Section 47 penalizes publishing illegal, obscene, or defamatory electronic content.
6. Formed specialized IT Tribunals for fast judicial trial of cyber crime cases.
7. Foundation law for e-governance and online business growth in Nepal.

d. Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a network security service that creates a safe, encrypted tunnel over an untrusted public network like the Internet. It masks user IP addresses and encrypts data payloads.

Key Points (7 Points):

1. Encapsulates data packets inside encrypted outer headers (IPSec, OpenVPN).
2. Encrypts data payload using AES-256 to ensure data confidentiality.
3. Masks real public IP address and replaces it with VPN server IP.
4. Allows remote employees to connect safely to company internal networks.
5. Protects users against Wi-Fi eavesdropping and packet sniffing on public networks.
6. Authenticates user credentials before opening the encrypted tunnel.
7. Prevents ISPs and third-party trackers from monitoring user web browsing.

CTEVT DIPLOMA IN COMPUTER ENGINEERING (DCE III/I)

Subject: Cyber Security & Social Ethics | Exam Paper Solutions (2078 Kartik/Mangsir -
Master Solved Exam Question Bank

Q1.a. What is Cyber Security? Explain types of attack in Cyber Security.

Cyber Security refers to the body of technologies, processes, practices, and controls designed to protect computers, networks, software programs, and data from unauthorized access, cyber attacks, damage, or theft.

2. Explanation of Types of Attacks

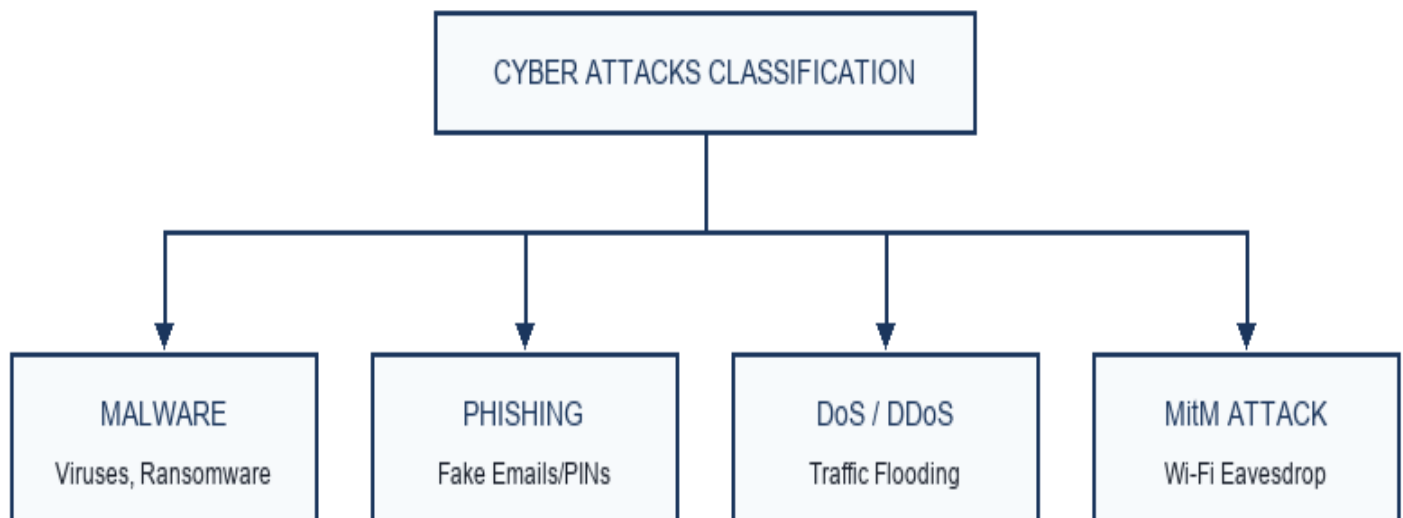


Figure: Textbook Block Diagram of Cyber Attack Vector & Types

Major Attack Types .

- **Malware Attack:** Viruses, Worms, Trojans, and Ransomware locking files or stealing data.
- **Phishing Attack:** Deceptive emails tricking users into entering passwords on fake sites.
- **Denial of Service (DoS/DDoS): Flooding** web servers with fake traffic to crash websites.
- **Man-in-the-Middle (MitM):** Intercepting private unencrypted Wi-Fi communications.
- **SQL Injection (SQLi):** Injecting database queries to dump backend database tables.

Q1.b. What is Firewall? Explain about types of Firewall.]

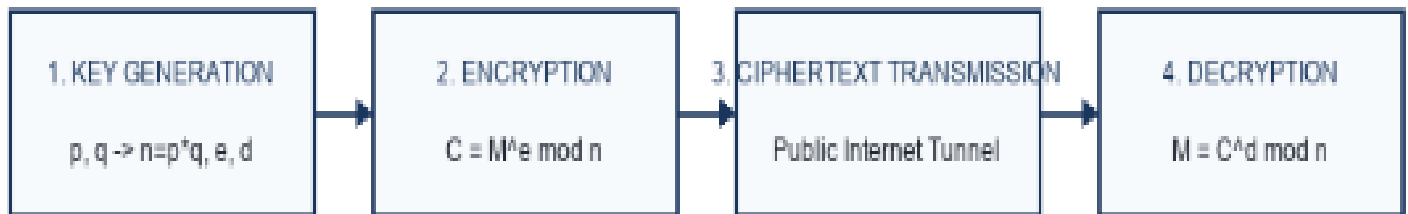
A Firewall is a network security system that acts as a protective barrier between a trusted internal network and an untrusted external network like the Internet.

Types of Firewalls Explained in Brief:

- **Packet Filtering:** Inspects individual packets of data and blocks them based on IP addresses, protocols, or port numbers.
- **Circuit-Level Gateway:** Verifies the network protocol session connection, like a TCP handshake, without inspecting the actual data packets.
- **Stateful Inspection:** Tracks the operating state and characteristics of network connections to allow or block traffic based on context.
- **Application-Level (Proxy):** Acts as an intermediary between two systems, inspecting data at the application layer to block specific malicious content.
- **Next-Generation (NGFW):** Combines traditional firewall capabilities with advanced features like deep packet inspection, intrusion prevention, and antivirus scanning.
- **Cloud Firewall (FWaaS):** A cloud-delivered security service that scales dynamically to protect internet-connected infrastructure and remote users.

Q2.a. Explain RSA algorithm with example.

The RSA Algorithm (named after Rivest, Shamir, and Adleman) is a widely used Asymmetric Key Cryptographic algorithm based on the mathematical difficulty of factoring large prime numbers. It uses a mathematically linked Public Key for encryption and Private Key for decryption.



RSA CRYPTOGRAPHIC ALGORITHM BLOCK DIAGRAM

RSA Algorithm Steps (Formulas):

1. Select two prime numbers p and q .
2. Calculate modulus $n = p \times q$.
3. Calculate Euler's Totient $\phi(n) = (p - 1) \times (q - 1)$.
4. Choose Public Key e such that $1 < e < \phi(n)$ and $\text{gcd}(e, \phi(n)) = 1$.
5. Calculate Private Key d such that $(d \times e) \bmod \phi(n) = 1$.
6. **Encryption**: $C = M^e \bmod n$
7. **Decryption**: $M = C^d \bmod n$

Q2.a RSA Algorithm - Step-by-Step Numerical Solution

Given Data:

Prime $p = 3$

Prime $q = 11$

Plaintext Message $M = 2$

Step 1: Calculate Modulus (n)

$$n = p * q = 3 * 11 = 33$$

Step 2: Calculate Euler Totient $\phi(n)$

$$\phi(n) = (p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 2 * 10 = 20$$

Step 3: Choose Public Key Exponent (e)

Choose $e = 7$ [since $\gcd(7, 20) = 1$]

Public Key = $(e, n) = (7, 33)$

Step 4: Calculate Private Key Exponent (d)

$$(d * e) \bmod \phi(n) = 1 \Rightarrow (d * 7) \bmod 20 = 1$$

For $d = 3$: $(3 * 7) \bmod 20 = 21 \bmod 20 = 1$ [Correct!]

Private Key = $(d, n) = (3, 33)$

Step 5: Encryption Process

Formula: $C = (M^e) \bmod n$

$$C = (2^7) \bmod 33 = 128 \bmod 33 = 29$$

Ciphertext (C) = 29

Step 6: Decryption Process

Formula: $M = (C^d) \bmod n$

$$M = (29^3) \bmod 33 = 24389 \bmod 33 = 2$$

Decrypted Message (M) = 2 [Matches original message!]

Q3.a. Explain Security policy and Security process.

1. Explanation of Security Policy

An Information Security Policy is a formal set of organizational rules, guidelines, and procedures designed to ensure that all employees and IT users comply with data security standards. It defines acceptable computer usage, password rules, access privileges, and incident response steps.

Components of Security Policy,

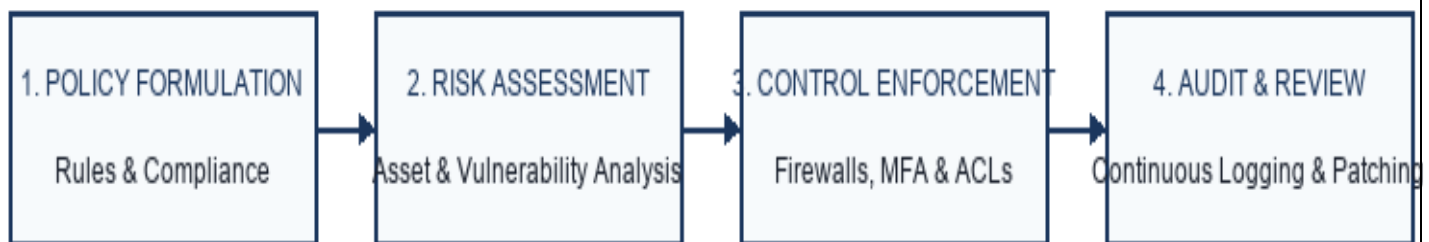
- **Acceptable Use Policy (AUP):** Rules for company internet, email, and laptop usage.
- **Access Control Policy:** Defines who is allowed to access confidential server data.
- **Password Policy:** Sets rules for password length, strength, and regular changes.
- **Incident Response Policy:** Defines steps to report data breaches immediately.

2. Explanation of Security Process

An Information Security Process is the ongoing management lifecycle of policy formulation, risk assessment, security controls implementation, and continuous auditing designed to protect corporate data assets against security threats.

Steps of Security Process (4 Points)

1. **Risk Assessment:** Finding weak spots and scanning system bugs.
2. **Control Enforcement:** Installing firewalls, antivirus, and multi-factor authentication (MFA).
3. **Continuous Monitoring:** Watching network traffic 24/7 for hacking attempts.
4. **Incident Recovery:** Restoring backed-up data and updating system security.



SECURITY POLICY AND MANAGEMENT PROCESS BLOCK DIAGRAM

Figure: Textbook Block Diagram of Security Policy and Management Process

Q3.b. What is Information Security? Explain Information Security Best Practice.

Information Security (InfoSec) refers to the practice of protecting digital and physical information assets from unauthorized access, use, disclosure, disruption, modification, or destruction, maintaining the CIA Triad.

Textbook InfoSec Process Diagram:

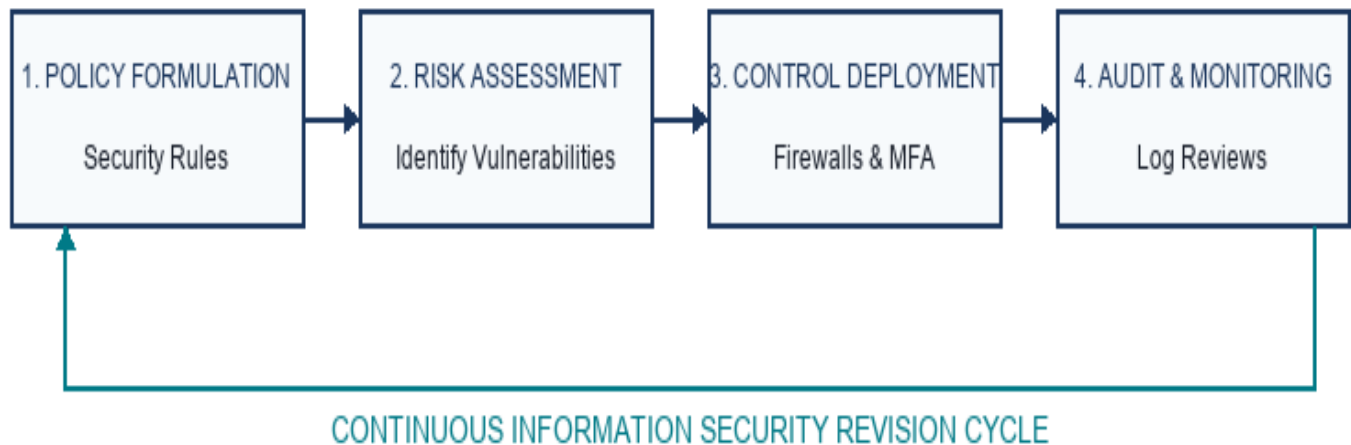


Figure: Textbook Block Diagram of Information Security Best Practice Process
InfoSec Best Practices:

1. Multi-Factor Authentication (MFA): Enforcing 2FA/MFA for all admin and user logins.
2. Regular Data Backups: Performing automated offline 3-2-1 backups to recover from ransomware.
3. Principle of Least Privilege (PoLP): Granting users minimal system permissions required for work.
4. Patch Management: Updating operating systems and software applications promptly to fix bugs.
5. Employee Security Awareness Training: Educating staff against phishing email traps.

Q4.a. What is Ethical Dissent and Whistle Blowing? Explain the role of professional in public policy.

Ethical Dissent is a professional's internal disagreement with illegal or unethical company practices. Whistle-Blowing is exposing internal corporate wrongdoing, data privacy violations, or safety hazards to public law enforcement when public safety is threatened.

Textbook Whistle-Blowing Flowchart:

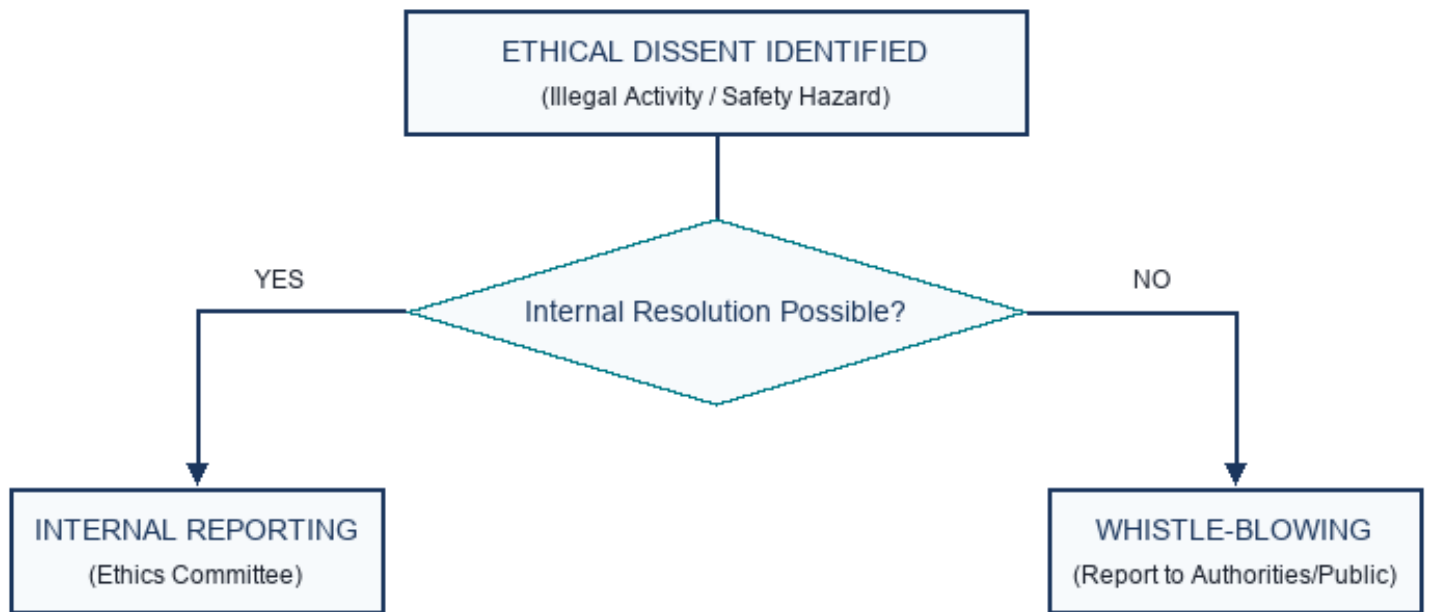


Figure: Textbook Block Diagram of Ethical Dissent and Whistle-Blowing Process
Role of IT Professional in Public Policy.

1. Advising Lawmakers: Providing technical expertise to draft effective cyber security laws.
2. Protecting Public Safety: Ensuring critical digital infrastructure operates ethically.
3. Responsible Bug Disclosure: Reporting system vulnerabilities before hackers exploit them.
4. Advocating Data Privacy: Promoting citizen privacy rights in e-governance projects.

Q4.b. What is Intellectual Property? Explain types of Intellectual Property.

Intellectual Property (IP) refers to creations of the human mind protected by law, such as software source code, proprietary algorithms, technological inventions, trade secrets, designs, and brand logos.

Textbook Diagram of Intellectual Property Types:

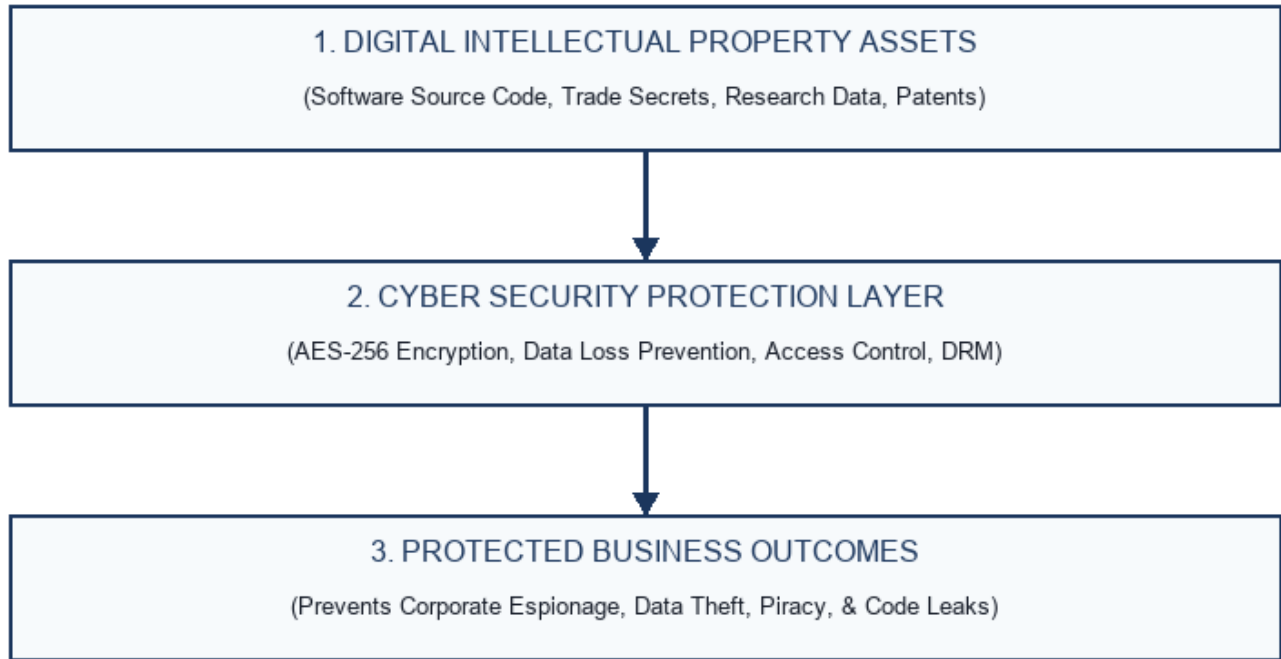


Figure: Textbook Block Diagram of Types of Intellectual Property

Types of Intellectual Property (4 Types Explained in Brief):

1. Patents: Exclusive rights granted for new technological inventions, hardware designs, or processes.
2. Copyrights: Legal protection for original literary, artistic, and software source code creations.
3. Trademarks: Unique brand names, logos, symbols, or slogans distinguishing company products.
4. Trade Secrets: Confidential business algorithms, customer lists, or proprietary source code.

Q5. Write short notes on: (Any Two)

a. Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a network security service that creates a safe, encrypted tunnel over an untrusted public network like the Internet. It masks user IP addresses and encrypts data payloads.

Key Points (7 Points):

1. Encapsulates data packets inside encrypted outer headers (IPSec, OpenVPN).
2. Encrypts data payload using AES-256 to ensure data confidentiality.
3. Masks real public IP address and replaces it with VPN server IP.
4. Allows remote employees to connect safely to company internal networks.
5. Protects users against Wi-Fi eavesdropping and packet sniffing on public networks.
6. Authenticates user credentials before opening the encrypted tunnel.
7. Prevents ISPs and third-party trackers from monitoring user web browsing.

b. Risk Assessment and Management

Risk Assessment and Management is the systematic process of identifying, analyzing, prioritizing, treating, and monitoring digital risks to an organization's information assets.

Key Points (7 Points):

1. Identifies critical digital assets like databases and payment servers.
2. Evaluates potential threat vectors like ransomware, phishing, and insider leaks.
3. Calculates Risk Score = Likelihood of Attack x Impact on Business.
4. Prioritizes security budgets toward high-risk vulnerabilities.
5. Helps choose risk responses: Risk Mitigation, Avoidance, Transference, or Acceptance.
6. Ensures compliance with national cyber laws and ISO 27001 security standards.
7. Conducted periodically to maintain a strong corporate security posture.

c. Anti-Malicious Software

Anti-Malicious Software (Antivirus/Anti-Malware) is a security program designed to prevent, detect, quarantine, and eliminate malicious software (viruses, worms, ransomware, trojans, spyware).

Key Points (7 Points):

1. Scans incoming downloads, email attachments, and active memory 24/7.
2. Signature-Based Detection matches file hashes against known virus databases.
3. Heuristic Analysis detects brand-new unknown malware variants by code behavior.

4. Safely isolates suspicious files inside an isolated Quarantine vault.
5. Automatically updates virus definition libraries from cloud security servers.
6. Protects personal passwords, banking details, and operating system files.
7. Essential endpoint security defense tool for personal PCs and servers.

C TEVT DIPLOMA IN COMPUTER ENGINEERING (DCE III/I)

Subject: Cyber Security & Social Ethics | Exam Paper Solutions (2078 Chaitra / 2079 Baishakh -)

Master Solved Exam Question Bank (Simple Chat-Matched Solutions)

Q1.a. What is cyber crime? Write down different types of attack in cyber. [

Cyber Crime refers to any illegal or fraudulent activity performed using computers, mobile devices, or networks as a tool or target to steal data, cheat money, or harm digital systems.

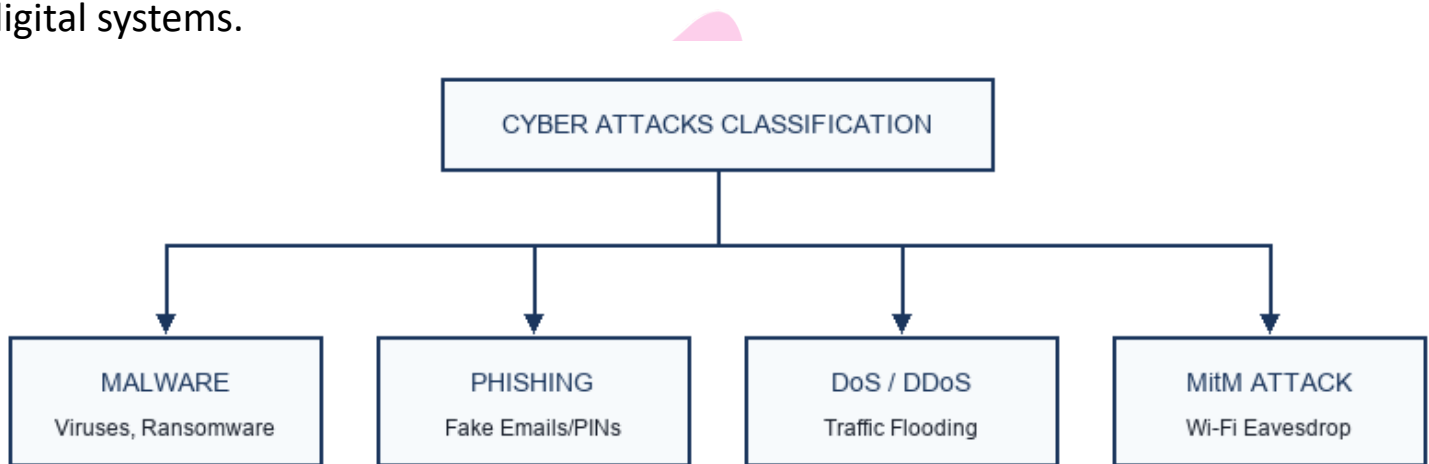


Figure: Textbook Block Diagram of Cyber Attack Types

Types of Cyber Attacks

1. Malware Attack: Viruses, Worms, Trojans, and Ransomware locking files or stealing data.
2. Phishing Attack: Fraudulent emails tricking users into entering credentials on fake websites.
3. Denial of Service (DoS/DDoS): Flooding servers with fake traffic to crash websites.
4. Man-in-the-Middle (MitM): Intercepting private Wi-Fi network communications.
5. SQL Injection (SQLi): Injecting malicious SQL code into web forms to dump backend databases.

Q1.b. What is firewall? Explain about anti malicious software.

A Firewall is a network security system that acts as a protective shield between a trusted private network and the untrusted Internet, filtering traffic based on security rules.

Explain about anti malicious software.

Anti-malware software is a specialized security program designed to detect, block, and remove malicious software—such as viruses, ransomware, spyware, and trojans—from computers, phones, and networks. It protects your data and keeps your devices safe by scanning files and monitoring system behavior. [1, 2, 3]

How It Works

- **Signature-based detection:** Compares file codes against a database of known malware.
- **Behavioral monitoring:** Flags programs that act suspiciously, such as trying to secretly change core system files.
- **Sandboxing:** Tests safe file execution inside an isolated virtual area before letting it run on your real system.
- **Quarantine:** Locks away or deletes infected files so they cannot harm your device. [1, 2]

Explanation of Anti-Malicious Software:

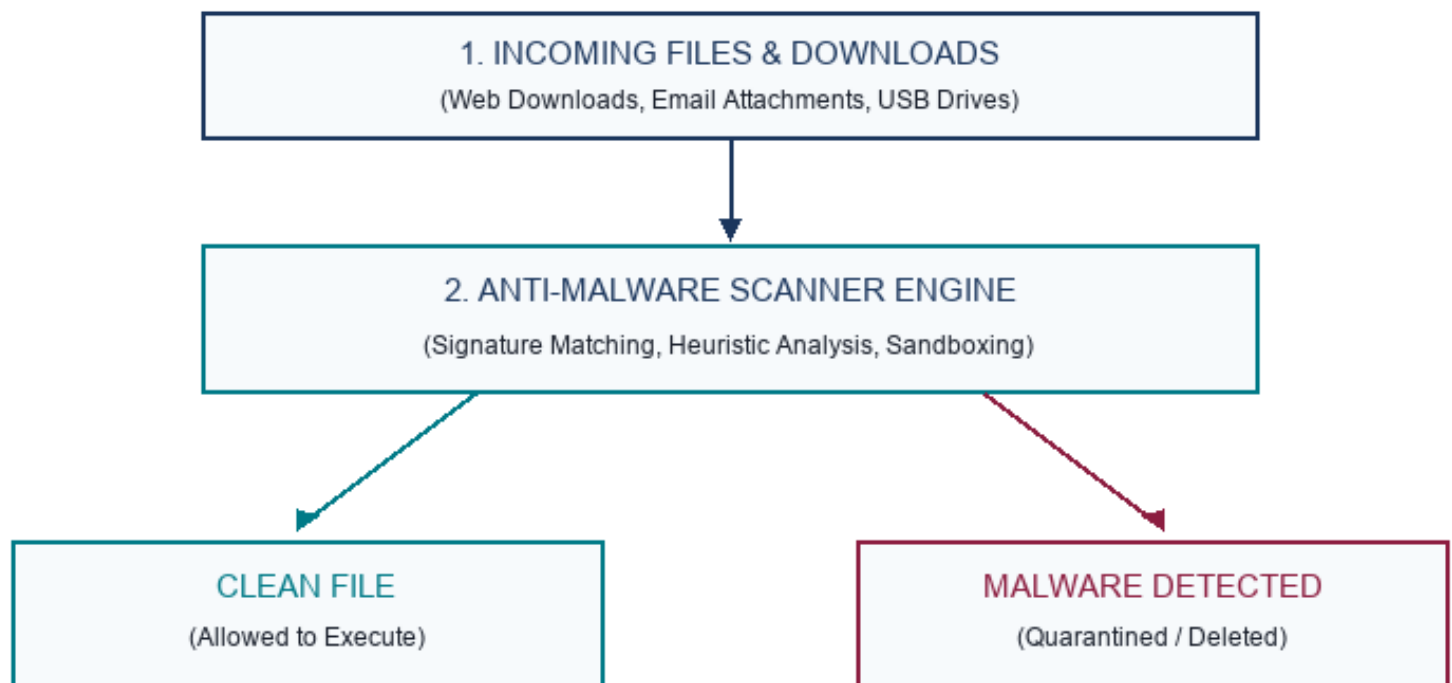


Figure: Textbook Block Diagram of Anti-Malicious Software Engine

Core Features (

- Real-Time Monitoring: Scans files being opened, downloaded, or executed continuously.
- Signature Matching: Compares file hash signatures against a known malware database.
- Heuristic Analysis: Examines code structure to detect new unknown malware variants.
- Threat Quarantine: Safely isolates infected files to prevent malware execution.
- Automatic Updates: Fetches latest virus definitions daily from cloud security servers.

Q2.a. Explain asymmetric key cryptography.

Asymmetric Key Cryptography (Public Key Cryptography) uses a pair of mathematically linked keys: a Public Key for encryption and a secret Private Key for decryption.



ASYMMETRIC KEY CRYPTOGRAPHY BLOCK DIAGRAM

Figure: Textbook Block Diagram of Asymmetric Key Cryptography

1. Dual Key Pair: Public Key (encrypt) and Private Key (decrypt).
2. Solves Key Distribution: Public keys can be shared openly over the Internet.
3. Digital Signatures: Provides sender authentication, message integrity, and non-repudiation.
4. Mathematical Basis: Based on prime factoring (RSA) or elliptic curves (ECC).
5. High Security: Private keys never need to be transmitted.

Q2.b. Write about cyber law in Nepal.

Cyber Law in Nepal is governed by the Electronic Transaction Act (ETA) 2063 (2006 BS). It provides legal rules for electronic records, digital signatures, e-commerce, and penalizes digital crimes.

Key Provisions of ETA 2063:

1. Legal Validation: Grants legal recognition to electronic records, e-banking, and digital signatures.
2. Controller of Certification Authority (CCA): Regulates digital keys and certification authorities.
3. Hacking Penalties (Section 44): Punishes unauthorized computer access with up to NRs 200,000 fine and 3 years jail.
4. Source Code Damage (Section 45): Penalizes destroying or altering computer programs.
5. Illegal Content (Section 47): Prohibits publishing offensive or defamatory electronic material.
6. IT Tribunal: Special courts formed for fast judicial trial of cyber crime cases.

Q3.a. What do you mean by freedom of speech? Explain.

Freedom of Speech is a fundamental human right to express opinions, share ideas, and publish information online without fear of government censorship or unlawful retaliation. In the digital age, it empowers citizens to participate in online journalism and social media discussions.

Parts of Free Speech

- **Sharing Ideas:** You can talk about politics, art, science, and social issues.
- **Challenging Power:** You can criticize the government or leaders safely.
- **Access to Truth:** It helps people hear many views and learn facts.

Important Limits

- **No Direct Harm:** You cannot use speech to cause immediate physical harm or start a riot.
- **No False Damage:** You cannot tell cruel lies that ruin a person's reputation, known as defamation.
- **Public Safety:** Laws can stop speech that puts public safety or national security in extreme danger.

Key Aspects & Boundaries:

- **Digital Expression:** Protects blogs, social media posts, and online news outlets.
- **Reasonable Restrictions:** Excludes hate speech, incitement to violence, online child abuse, and criminal defamation.

Q3.b. How can you deal with cyber harassment and discrimination?

To deal with cyber harassment and discrimination, do not reply or engage with the abusers. Instead, capture screenshots of all hurtful posts and messages as evidence, block the accounts, and report the abuse directly to the platform or local law enforcement if you feel unsafe.

Action Steps

- **Save Proof:** Take clear screenshots of the abusive text, profile name, and URL links before they can be deleted.
- **Block and Filter:** Cut off contact by blocking the user and setting your social media profiles to private.
- **Report the Content:** Use the built-in report tools on the website or app to flag the harassment or discriminatory speech.
- **Involve Authorities:** Contact local police or cybercrime units if the behavior includes physical threats, doxxing, or severe hate speech]

Prevention and Support

- **Tighten Security:** Use strong passwords and turn on two-step verification for all personal accounts.
- **Limit Personal Details:** Keep private data, phone numbers, and daily locations off public profiles.
- **Seek Support:** Talk to a trusted friend, family member, or counselor to manage stress and get emotional support.]

PUBLISHER

Q4.a. What is cryptography? Explain digital signature models,

Cryptography is the science of protecting information by transforming readable plaintext into unreadable ciphertext using mathematical keys.

Digital Signature

A Digital Signature Model is a cryptographic framework that defines how a sender signs an electronic document using their secret Private Key, and how a receiver verifies its authenticity using the matching Public Key.

DIGITAL SIGNATURE PROCESS SCHEMATIC

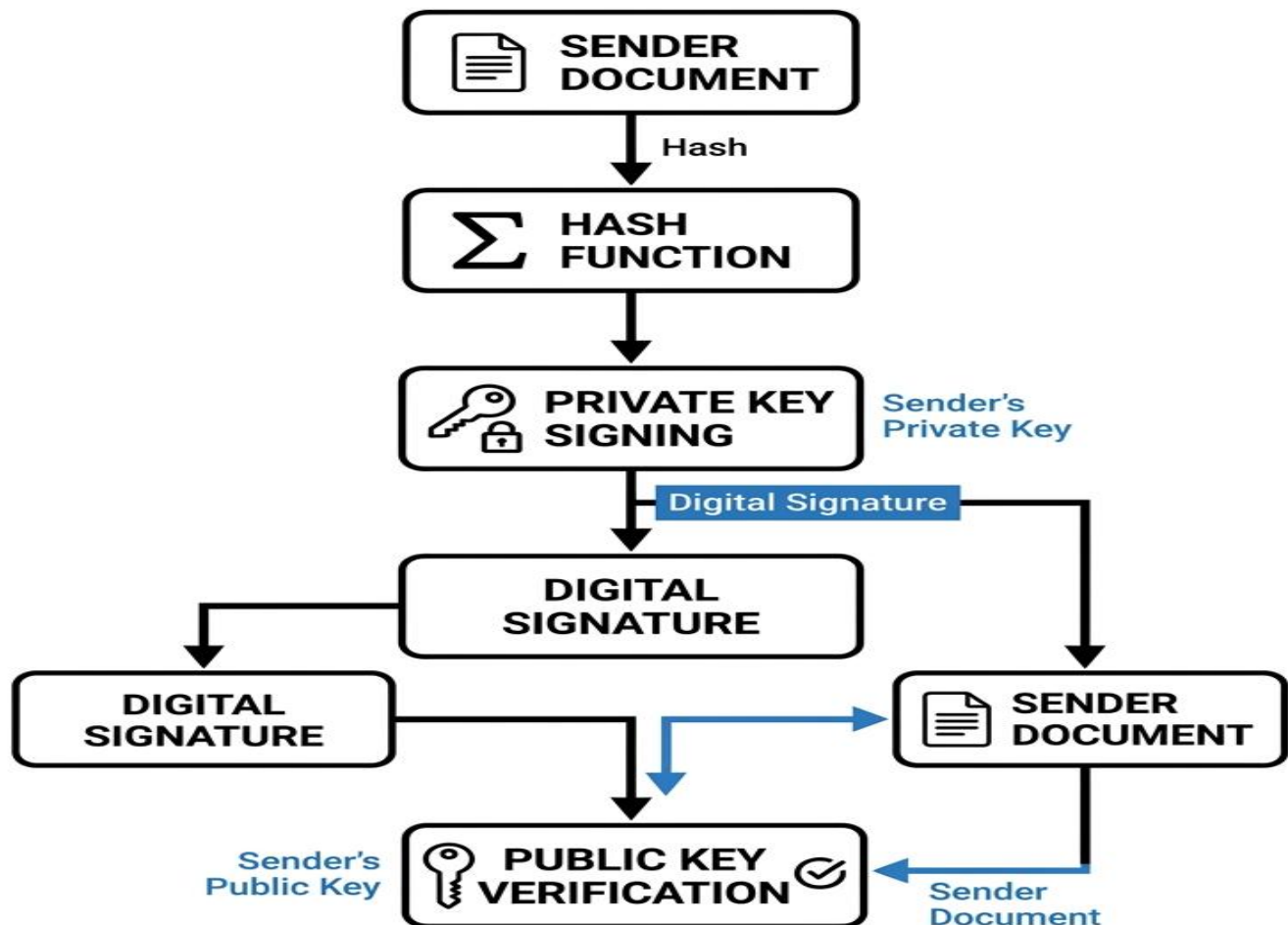


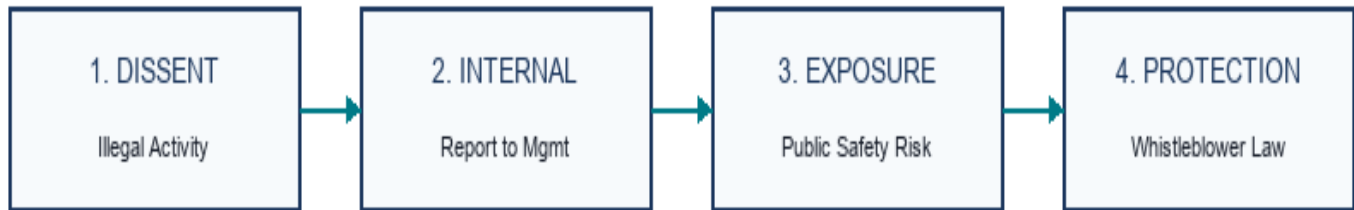
Figure: Textbook Block Diagram of Digital Signature Model Workflow

1. **RSA Digital Signature Model:** Document is hashed using SHA-256 and encrypted with Sender's Private Key. Receiver verifies using Sender's Public Key.
2. **DSA (Digital Signature Algorithm) Model:** Federal standard model relying on discrete logarithm mathematics for signature generation and verification.
3. **ECDSA (Elliptic Curve Digital Signature Algorithm) Model:** Modern high-security model offering shorter key lengths and faster processing for mobile devices.

Q4.b. Explain whistle blowing in ethical responsibilities of cyber security

Whistle-Blowing is the ethical act of an employee exposing internal corporate wrongdoing, safety hazards, or data privacy crimes to public law enforcement when management refuses to act.

Textbook Block Diagram:



ETHICAL WHISTLE-BLOWING PROCESS BLOCK DIAGRAM

Figure: Textbook Flowchart of Whistle-Blowing Process in Cyber Security

Core Ethical Responsibility.

- Protecting Public Interest: Exposing severe security risks affecting citizen privacy or financial safety.
- Internal Reporting First: Attempting internal escalation to senior management or ethics committees first.
- Responsible Disclosure: Reporting critical system flaws to law enforcement or bug bounty programs.
- Truthful Evidence: Providing accurate, un-tampered documentary proof of company negligence.

Q5. Write short notes on: (Any Two) [2x5 = 10 Marks] [10 Marks]

a. Internet Fraud

Internet Fraud refers to any fraudulent scheme performed online using web applications, email, or software to steal money or sensitive data from victims.

Key Points (7 Points):

1. Includes Phishing emails tricking users into revealing online banking passwords.
2. Encompasses Identity Theft to open unauthorized bank loans in victim's name.
3. Involves Advance Fee Fraud (419 scams) promising non-existent cash rewards.
4. Uses fake e-commerce shopping sites to collect money without shipping products.
5. Employs fake tech support pop-ups demanding payment to fix fake viruses.
6. Prevented through user security awareness and Multi-Factor Authentication

b. Software Risk

Software Risk refers to the probability of operational failure, security vulnerabilities, or project delays arising from flaws in software requirements, architecture, or source code.

Key Points (7 Points):

1. Caused by unvalidated user input leading to SQL injection or XSS bugs.
2. Arises from inadequate security testing during Software Development Lifecycle (SDLC).
3. Includes reliance on outdated third-party open-source code libraries.
4. Can cause system crashes, data corruption, or unauthorized database breach.
5. Mitigated through static code analysis and regular penetration testing audits.
6. Managed by establishing secure coding standards and patch management policies.
7. Essential focus area for software engineers and cyber security auditors.

c. Firewall

A Firewall is a critical network security system that acts as a protective barrier between a trusted internal network and an untrusted external network like the Internet.

Key Points (7 Points):

1. Filters network traffic based on IP address, port numbers, and protocols.
2. Operates at stateless (L3/L4) or stateful/proxy (L7) application layers.
3. Prevents unauthorized hackers from entering private corporate networks.
4. Maintains Access Control Lists (ACLs) and connection state tables.
5. Provides detailed event logs of all blocked intrusion attempts.
6. Hides internal company IP addresses from external internet scanners.
7. Essential perimeter defense tool for corporate cyber security.

d. Trademarks

A Trademark is an Intellectual Property Right (IPR) that legally protects unique brand signs, names, logos, symbols, or slogans distinguishing a company's products from competitors.

Key Points (7 Points):

1. Grants exclusive legal rights to a company to use its brand logo in marketplace.
2. Prevents competitors from creating fake copies or using similar confusing logos.
3. Represented legally by symbols like [™] (Unregistered) or [®] (Registered).
4. Protects company web domain names (e.g. `esewa.com.np`) from cybersquatting.

5. Preserves customer trust and business brand identity in digital space.
6. Can last indefinitely as long as the owner renews registration periodically.
7. Enforced under intellectual property and cyber laws against fake websites.

