ICS PYQ Dec 2024 Solved

---

1. List any two components of security architecture.

Security architecture consists of multiple controls. Two core components are:
Authentication, which verifies the identity of users or systems, and
Authorization, which specifies what actions an authenticated entity is allowed to perform.
Both work together to ensure only legitimate, permitted users access system resources.

---

2. Differentiate between a threat and vulnerability.

A **threat** is any event or actor with the potential to cause harm to information assets — for example, malware, hackers, or natural disasters.
A **vulnerability** is a weakness in a system — such as outdated software or weak passwords — that can be exploited by a threat.
Threat = potential danger; Vulnerability = weakness the danger exploits.

---

3. Describe classical encryption.

Classical encryption refers to early cryptographic methods based on simple operations like **substitution** (replacing characters) and **transposition** (rearranging characters).
Algorithms such as the Caesar Cipher and Vigenère Cipher belong here.
They rely on manual or basic mathematical operations and are not secure by modern computational standards.

---

4. State why AES is considered more secure than DES.

AES supports key sizes of **128, 192, and 256 bits**, making brute-force attacks practically impossible.
DES uses only a **56-bit key**, which can be cracked in hours with modern hardware.
AES also has stronger internal structure and more robust rounds of encryption.

---

5. Define risk assessment.

Risk assessment is the systematic process of identifying possible security threats, evaluating vulnerabilities, and determining the potential impact of each risk.
Its goal is to prioritize risks and guide decision-making for security controls.

---

6. List two common risk control strategies.

Two common strategies are:
Risk Avoidance – eliminating the activity that creates the risk, and

Risk Mitigation – implementing controls to reduce the likelihood or impact of the risk.
Other strategies include risk transfer (insurance) and risk acceptance.

---

7. Define the term "software piracy."

Software piracy refers to the illegal copying, distribution, sharing, or use of software without the required license or permission from the copyright holder.
It violates intellectual property rights and causes financial loss to developers.

---

8. State how Social Engineering attacks exploit human psychology.

Social engineering manipulates human emotions such as trust, fear, urgency, greed, or curiosity.
Attackers use these psychological triggers to trick victims into revealing confidential information, clicking malicious links, or performing unsafe actions.

---

9. Define Password Cracking.

Password cracking is the technique used to recover passwords by using methods like brute force, dictionary attacks, rainbow tables, or exploiting system flaws.
The aim is to gain unauthorized access to accounts or systems.

---

10. State SQL Injection.

SQL Injection is a database attack where an attacker inserts malicious SQL queries into input fields.
These injected statements manipulate the backend database, allowing unauthorized data access, modification, or even deletion.

PART B – (4 × 15 = 60 Marks)

11(a)(i) Given a hypothetical scenario where a company faces a ransomware attack, apply your understanding of security attacks and propose an incident response plan.

A ransomware attack is a **malicious software attack** where the attacker encrypts the company's data and demands payment for decryption. It typically starts through phishing emails, malicious downloads, or exploitation of vulnerabilities. The attack qualifies as both a **malware attack** and an **active attack**, since the attacker deliberately modifies data and disrupts operations.

A strong incident response plan must follow a structured approach:

1. Identification
The security team detects unusual system behavior: inaccessible files, sudden file extensions,

ransom notes, or abnormal CPU/network activity. Logs, IDS alerts, and user reports help confirm that ransomware is active in the network.

2. Containment
Immediate containment prevents the malware from spreading.
Actions include:
– Isolating infected systems from the network
– Blocking malicious IPs and domains
– Disabling shared folders and network drives
– Stopping automated backup sync to protect clean backups
Short-term containment limits damage; long-term containment includes patching systems and disabling compromised accounts.

3. Eradication
The next step is cleaning the environment.
This involves:
– Removing ransomware files, scripts, and persistence mechanisms
– Closing the exploited vulnerability (patching OS, updating antivirus, disabling RDP if misused)
– Scanning the entire network for dormant malware
Eradication ensures the threat actor cannot regain access.

4. Recovery
Systems are restored to normal using verified clean backups.
Steps include:
– Rebuilding affected servers/workstations
– Restoring data from offline backups
– Re-enabling services gradually
– Monitoring systems for any signs of reinfection
Recovery must be cautious to avoid reinfection from leftover malware fragments.

5. Preventive Measures
To avoid future attacks:
– Mandatory employee awareness training
– Regular patching and updates
– Multi-factor authentication (MFA)
– Maintaining offline backups
– Deploying IDS/IPS and endpoint security solutions
– Zero-trust access model
These reduce the chances of a similar attack recurring.

11(a)(ii) Discuss the key components of security architectures and how they work together to ensure system protection.

Security architecture defines how security controls are structured to protect an organization. Key components include:

1. Authentication – Verifies the identity of users or systems using passwords, biometrics, tokens, or certificates.

2. Authorization – Defines what actions authenticated users are allowed to perform through access control policies.

3. Confidentiality Controls – Mechanisms like encryption, VPNs, and secure communication protocols (TLS) to prevent unauthorized data access.

4. Integrity Controls – Hashing, digital signatures, and checksums ensure data is not modified or tampered during storage or transmission.

5. Availability Mechanisms – Backups, redundancy, failover systems, and DDoS protection maintain system uptime.

These components work together to secure data, systems, and communication across the entire organization.

11(b)(i) Analyze a case where an organization's security measures were effective in protecting data but failed to address privacy concerns. Discuss how the balance between security and privacy can be managed and propose strategies for achieving this balance. (10)

Organizations sometimes deploy strong security measures that unintentionally compromise user privacy. For instance, heavy monitoring tools, CCTV, extensive logging, and intrusive authentication may protect data but can invade employee privacy.

A good analysis includes:

1. Security vs Privacy Conflict
– Security seeks to protect data and systems from threats.
– Privacy ensures personal data is collected minimally and used lawfully.
Security controls like monitoring, biometric access, and surveillance may conflict with privacy rights.

2. Reasons for Failure
– Excessive data collection
– Lack of transparency on how user data is monitored
– Weak privacy policies
– No consent or justification for intrusive controls

3. How to Achieve Balance
– Apply the principle of **data minimization** (collect only what is required).
– Use **role-based access control** to limit who can see personal data.
– Mask, anonymize, or pseudonymize logs containing user information.
– Ensure monitoring focuses on system behavior, not personal behavior.
– Perform **Privacy Impact Assessments (PIA)** before introducing new security controls.

4. Strategies to Improve Balance
– Comply with privacy laws (IT Act 2000, PDP Bill, GDPR principles).
– Provide clear data-collection notices to users.
– Encrypt all stored personal data.

– Implement strict retention and deletion policies.
– Separate security data from personally identifiable data.

Balancing both ensures strong protection without violating individual rights.

11(b)(ii) Discuss the fundamental principles of cryptography and its applications in securing digital information

Cryptography secures digital information using mathematical techniques. Its fundamental principles include:

1. Confidentiality – Ensures information is accessible only to authorized users through encryption.

2. Integrity – Hashing and digital signatures ensure that data is not altered by unauthorized parties.

3. Authentication – Verifies identity using keys, certificates, and protocols.

4. Non-repudiation – Digital signatures prevent users from denying actions they performed.

5. Key Management – Secure generation, distribution, storage, rotation, and revocation of keys is essential.

Applications include secure communication (TLS), secure email (PGP), digital payments, authentication systems, and protecting databases and cloud data.

12(a)(i) Compare and contrast the security and efficiency of RSA with that of Elliptic Curve Cryptography (ECC). Under what scenarios might ECC be preferred over RSA?

RSA and Elliptic Curve Cryptography (ECC) are both public-key cryptography algorithms, but they differ strongly in mathematical foundation, key size, performance, and security strength.

1. Mathematical Basis
– **RSA** is based on the difficulty of factoring large prime numbers.
– **ECC** relies on solving the Elliptic Curve Discrete Logarithm Problem, which is significantly harder mathematically.
This makes ECC stronger per bit of key length.

2. Key Size and Security Strength
RSA requires extremely large keys to maintain security.
– RSA 2048-bit ≈ ECC 224-bit in strength
– RSA 3072-bit ≈ ECC 256-bit
– RSA 15360-bit ≈ ECC 521-bit
ECC achieves the same security with drastically smaller keys, reducing computational overhead.

3. Performance
ECC offers faster:

– Key generation
– Encryption
– Digital signatures
– Verification
ECC is lightweight, which is crucial for resource-limited devices.
RSA operations become slower and more expensive as key size increases.

4. Memory and Bandwidth Efficiency
ECC uses less memory, storage, and network bandwidth due to smaller keys and signatures. This helps performance-critical applications like IoT, mobile devices, and embedded systems.

5. Scenarios Where ECC Is Preferred
ECC is chosen over RSA in situations that require:
– High performance on low-power devices (IoT sensors, wearables, smart cards)
– Fast SSL/TLS handshakes on mobile networks
– Smaller certificate sizes in HTTPS (improves page load time)
– Blockchain and cryptocurrency systems (Bitcoin, Ethereum)
– Secure messaging apps (Signal, WhatsApp)
– Devices with low CPU, RAM, or battery

In modern systems, ECC is becoming the default because it delivers stronger security with minimal computational cost.

12(a)(ii) Explain the basic working of Public Key Cryptography and RSA algorithm.

Public Key Cryptography (PKC) is an encryption system using two keys:
– **Public key** (shared with everyone)
– **Private key** (kept secret)
Data encrypted with one key can only be decrypted with the other. This provides secure communication, authentication, and digital signatures without exchanging secret keys.

Working of RSA Algorithm

1. Key Generation
a. Select two large prime numbers **p** and **q**.
b. Compute **n = p × q** (modulus).
c. Compute **φ(n) = (p − 1)(q − 1)**.
d. Choose public exponent **e** such that gcd(e, φ(n)) = 1.
e. Compute private key **d** such that **d × e ≡ 1 (mod φ(n))**.

Public key = (e, n)
Private key = (d, n)

---

2. Encryption
Sender converts plaintext into a number *m*.
Ciphertext: **$c = m^e \bmod n$**

---

3. Decryption
Receiver computes:
Plaintext: **$m = c^d \bmod n$**

Only the private key can decrypt the ciphertext encrypted with the public key, ensuring confidentiality.

Alright, moving to **Q12(b)**.
Again, full-length, expanded, examiner-friendly answers for **10 marks + 5 marks**.

12(b)(i) Discuss the structure and key features of the AES encryption algorithm. Why is AES considered secure compared to previous encryption standards?

Advanced Encryption Standard (AES) is a symmetric block cipher adopted by NIST to replace DES. It encrypts data in **128-bit blocks** and supports **128, 192, or 256-bit keys**.

1. Structure of AES

AES works as a **Substitution–Permutation Network (SPN)** and performs encryption in multiple rounds:

a. Key Expansion

The original key is expanded into a series of round keys using Rijndael’s key schedule. Longer keys → more rounds.

b. Initial Round : AddRoundKey – XOR the plaintext block with the first round key.

c. Main Rounds

Each round contains four operations:

1. **SubBytes**
   – Non-linear byte substitution using a fixed S-Box.
   – Provides *confusion* (harder to analyze patterns).
2. **ShiftRows**
   – Cyclically shifts rows in the state matrix.
   – Creates diffusion by spreading byte influence.
3. **MixColumns**
   – Matrix multiplication that mixes column bytes.
   – Increases diffusion across state.
4. **AddRoundKey**
   – XOR current state with the round key.

d. Final Round

Same as main round **but excludes MixColumns**.

e. Output

Ciphertext is generated after the final AddRoundKey.

---

2. Key Features of AES

– **Block size 128 bits** ensures uniform, predictable memory usage.
– **Strong S-box** resistant to differential and linear cryptanalysis.
– **Multiple key sizes** (128/192/256) allow scalable security.
– **Fast in hardware & software** compared to older algorithms.
– **Parallelizable operations**, improving performance on modern CPUs.
– **No known practical attacks** when implemented correctly.

---

3. Why AES Is Considered More Secure than DES

1. **AES has a much larger key size**
   – DES: 56-bit key → can be brute-forced in hours.
   – AES-128 requires 3.4×10^{38} operations → practically impossible to brute force.
2. **Modern cryptographic design**
   AES uses strong substitution-permutation structure, unlike DES's outdated Feistel network.
3. **More rounds and stronger round functions**
   AES's nonlinear operations make cryptanalysis extremely complex.

12(b)(ii) Discuss the steps involved in risk assessment and its significance in cybersecurity.

Risk assessment systematically identifies and evaluates risks to an organization's assets.

Steps in Risk Assessment

1. Asset Identification

Identify what needs protection — servers, databases, networks, employees, processes.

2. Threat Identification

Determine potential threats such as malware, insider misuse, phishing, hardware failure.

3. Vulnerability Assessment

Check weaknesses like outdated software, weak passwords, misconfigured networks.

4. Risk Evaluation

Calculate risk using:
Risk = Threat × Vulnerability × Impact
Helps in prioritizing the most dangerous risks.

5. Control Recommendation

Suggest security measures like firewalls, encryption, MFA, patching, monitoring.

Significance of Risk Assessment

– Helps organizations **understand their security weaknesses**.
– Improves decision-making on where to invest in security controls.
– Reduces chances of data breaches and system downtime.
– Supports compliance with standards like ISO 27001, PCI-DSS.
– Ensures **proactive** security rather than reactive firefighting.

13(a)(i) Apply the risk assessment process to a specific scenario, such as a company transitioning to cloud computing. Identify and assess potential risks related to data security, privacy, and operational continuity.

When an organization transitions from on-premise infrastructure to cloud computing, it faces new risks in data security, privacy, and operational continuity. Applying the risk assessment process helps identify, evaluate, and control these risks.

---

1. Asset Identification

Identify what is being moved to the cloud:
– Customer databases
– Application servers
– User accounts and credentials
– API gateways
– Virtual machines
– Backup systems
– Business workflows
These assets become accessible over the internet, increasing exposure.

---

2. Threat Identification

Common cloud threats include:
– Unauthorized access
– Account hijacking
– Insecure APIs
– Data breaches
– Misconfigured cloud storage
– Insider threats at cloud provider
– DDoS attacks
– Ransomware targeting cloud workloads
Cloud environments interact with many third-party services, increasing attack surface.

---

3. Vulnerability Assessment

Typical cloud vulnerabilities:
– Weak access controls
– Missing encryption for data at rest or in transit
– Misconfigured S3 buckets / public storage
– Inadequate logging or monitoring
– Poor key management
– Lack of MFA
– Unpatched virtual machines
Because cloud uses shared responsibility, misconfigurations by the client are extremely common.

---

4. Risk Evaluation

Risk = Threat × Vulnerability × Impact

High-risk examples:
– Publicly accessible storage → major data breach
– Weak IAM permissions → privilege escalation
– Insecure API → remote code execution
– No backup strategy → service outage

Medium-risk examples:
– Unoptimized firewall rules
– Dependence on single cloud provider

Low-risk examples:
– Minor configuration issues with low-impact assets

This ranking helps management prioritize remediation steps.

---

5. Control Recommendation (Mitigation)

To manage risks, apply:
– **Encryption** for data at rest and in transit
– **Strong IAM policies** (least privilege, MFA)
– **Cloud logging & monitoring** (CloudTrail, CloudWatch)
– **Network segmentation** using VPC, subnets, security groups
– **Regular vulnerability scanning**
– **Secure API gateways** with authentication and rate limiting
– **Backup and disaster recovery plan**
– **Compliance checks** (ISO 27017, NIST, SOC 2)
– **Shared Responsibility Model awareness training**

---

6. Documentation and Review

All risks, controls, decisions, and responsibilities are documented.
Assessments are repeated after changes like new cloud services, new users, or new applications.

13(a)(ii) Discuss the relationship between cybercrime and information security.
Cybercrime refers to illegal activities performed using computers or networks, such as hacking, phishing, identity theft, ransomware, and data breaches.

Information Security focuses on protecting the confidentiality, integrity, and availability of data.

Relationship

1. **Cybercrime creates the need for Information Security**
   Cybercriminals exploit vulnerabilities, which forces organizations to implement stronger security controls.
2. **Information Security minimizes impact of cybercrime**
   Security measures such as encryption, access control, firewalls, IDS, and authentication help defend against cybercrime.
3. **Both evolve together**
   As cybercriminals develop advanced attacks (ransomware-as-a-service, polymorphic malware), information security adapts through new defenses like zero-trust, AI-based threat detection, and multi-factor authentication.
4. **Legal and organizational connection**
   Cybercrime laws (IT Act 2000, GDPR, DPA) require organizations to maintain adequate information security.
   Failure leads to legal penalties and reputational damage.
5. **Objective alignment**
   Cybercrime aims to exploit information.
   Information Security aims to protect information.

Thus, cybercrime acts as the *driving force*, and information security acts as the *protective shield*.

13(b)(i) Illustrate with examples how passive and active security attacks work. Apply this understanding to explain why active attacks pose a greater risk to network security.

Security attacks are broadly classified into **passive** and **active**, based on whether the attacker only observes or also modifies data. Understanding the difference is crucial for designing defense mechanisms.

---

1. Passive Attacks

A passive attack **does not alter** data or system state.
The attacker only **eavesdrops, monitors, or collects information**.

Examples:

a. Eavesdropping / Sniffing:
An attacker capturing unencrypted network traffic to read usernames, passwords, or messages.

b. Traffic Analysis:
Even if data is encrypted, the attacker studies communication patterns (frequency, timing, size) to infer sensitive information.

Characteristics:

– Silent and undetectable
– No data modification
– Aim is information gathering
– Hard to notice without encryption and monitoring tools

Passive attacks threaten **confidentiality**.

2. Active Attacks

An active attack **modifies**, **injects**, **deletes**, or **disrupts** data or system operations.

Examples:

a. Man-in-the-Middle (MITM):
Attacker intercepts communication, alters messages, and forwards them.

b. Denial of Service (DoS):
Flooding a server with traffic to shut it down.

c. Spoofing / Masquerading:
Attacker impersonates a legitimate user by forging identity information.

d. SQL Injection:
Attacker inserts malicious SQL queries to modify database content.

Characteristics:

– Direct interaction with victim
– Changes system behavior
– Detectable but more damaging
– Threatens confidentiality, integrity, and availability

3. Why Active Attacks Pose a Greater Risk

1. **Cause immediate and visible damage**
   – Data corruption, system downtime, service unavailability.

2. **Break integrity & availability**
   Passive attacks only steal data; active attacks can destroy it.
3. **Can lead to complete system compromise**
   Example: a single SQL injection can wipe databases or steal all records.
4. **Can be chained with other attacks**
   MITM + session hijacking → full account takeover.
5. **Financial & operational impact is higher**
   Organizations lose revenue, reputation, and uptime.

13(b)(ii) Describe the Indian legal framework for cybercrime prevention, focusing on the IT Act 2000 and its amendments.

India's primary law for regulating cyber activities and preventing cybercrime is the **Information Technology (IT) Act, 2000**. It defines offenses, penalties, and responsibilities for electronic communication, digital signatures, and data protection.

---

1. Key Provisions of the IT Act 2000

– **Section 43:** Penalties for unauthorized access, damage to computer systems, malware insertion, and data theft.
– **Section 66:** Cyber offenses done dishonestly or fraudulently (hacking).
– **Section 67:** Punishment for publishing obscene content online.
– **Section 69:** Powers to intercept, monitor, and decrypt information.
– **Legal recognition of electronic documents and digital signatures.**

---

2. IT (Amendment) Act 2008 – Major Improvements

– Introduced **Section 66A** (offensive messages — later struck down by Supreme Court).
– Added **Section 66C/66D** for identity theft and online cheating.
– Defined **cyber terrorism** under Section 66F.
– Improved protection for **sensitive personal data**.
– Strengthened digital signature and electronic authentication systems.
– Provided legal recognition for **electronic contracts**.

---

3. Effectiveness and Role in Cybercrime Prevention

– Establishes penalties and punishments for cyber offenses.
– Empowers law enforcement to investigate digital crimes.
– Governs data protection, intermediaries, and digital transactions.
– Ensures digital signatures, e-governance, and electronic records are legally valid.

14(a)(i) Explain the concept of cyber security. Why is it considered a crucial aspect in the digital age, especially with the rise of cybercrime?

Cyber security refers to the practices, technologies, and processes designed to protect networks, systems, data, and digital infrastructure from unauthorized access, attacks, damage, or misuse. It ensures the **confidentiality, integrity, and availability (CIA)** of information.

1. Why Cyber Security Matters Today

Modern society depends heavily on digital systems — banking, healthcare, e-commerce, education, transportation, governance, and communication. Because everything is online, the attack surface becomes massive.

2. Rising Cybercrime

Hackers now use sophisticated methods:
– Ransomware-as-a-service
– Phishing kits
– Zero-day exploits
– Social engineering
– Deepfake scams
– Supply chain attacks

These attacks target businesses, government bodies, and individuals. Without cybersecurity, any digital system is exposed to theft, data loss, and financial damage.

3. Increased Online Data

People store personal information online: Aadhaar details, bank accounts, passwords, photos, confidential documents.
Organizations store customer data, business strategies, intellectual property, and financial records.
More data online = more targets = more risk.

4. Dependency on Cloud & Remote Work

The shift to cloud services and remote work environments increases vulnerability:
– Unsecured home networks
– Misconfigured cloud storage
– Inconsistent device security
Cybersecurity becomes essential to enforce secure access, encryption, and monitoring.

5. Financial & Operational Impact

Cyberattacks can shut down entire operations.
Examples:
– Ransomware freezing servers
– DDoS attacks blocking websites
– Data breaches causing lawsuits and penalties
Cybersecurity protects business continuity and prevents costly downtime.

14(a)(ii) Discuss the techniques used in phishing attacks and their potential consequences.

Phishing is a social engineering attack where attackers trick users into revealing sensitive information by masquerading as a trusted entity.

---

1. Techniques Used in Phishing

a. Email Phishing
Fake emails mimic banks, companies, or government bodies and contain malicious links/forms.

b. Spear Phishing
Highly targeted emails sent to specific individuals using personal information to appear legitimate.

c. Clone Phishing
A real email is copied and resent with a malicious attachment or link.

d. SMS Phishing (Smishing)
Fraudulent text messages asking users to click malicious links or share OTPs.

e. Voice Phishing (Vishing)
Attackers call victims pretending to be bank officers, police, or support staff.

f. Website Spoofing
Attackers create fake websites identical to real sites to steal credentials.

g. Social Media Phishing
Fake accounts impersonate celebrities, support teams, or friends to extract information.

---

2. Consequences of Phishing

– **Credential theft** (passwords, banking logins)
– **Financial loss** due to fraudulent transactions
– **Identity theft**
– **Malware infection** (ransomware, spyware)
– **Unauthorized access to enterprise systems**
– **Data breaches** exposing confidential records
– **Reputation damage** for both individuals and organizations

Phishing attacks exploit human trust, making them one of the most successful cybercrimes.

14(b)(i) Define key-loggers and spywares. How do they function to compromise the security of a system, and what are the implications for user privacy?

Keyloggers and **Spyware** are malicious programs designed to secretly monitor user activity. They are widely used in credential theft, surveillance, and financial fraud.

1. Keyloggers

A **keylogger** records every keystroke typed on a keyboard.
This includes:
– Usernames and passwords
– Banking credentials
– Private messages
– Emails
– Personal information

Working Mechanism

Keyloggers operate as:
a. Software Keyloggers: Installed programs that intercept keyboard events at OS level (API hooking, kernel drivers).
b. Hardware Keyloggers: Physical devices placed between the keyboard and CPU.
c. Browser-based Keyloggers: Malicious scripts capturing form inputs.

Impact on Security

– Immediate credential theft
– Full compromise of email, social media, and banking accounts
– Can bypass encryption because they capture input before encryption happens

2. Spyware

Spyware secretly monitors user activity and gathers information without consent.
It collects browsing history, login information, device details, screenshots, and sometimes video/audio via webcam/mic.

Working Mechanism

– Hidden background processes
– Malicious browser extensions
– Bundled with free software
– Exploits vulnerabilities to install silently
– Communicates collected data to attacker’s server

Impact on Security

– Password theft
– Session hijacking
– Network intrusion via stolen credentials
– Manipulation of browser traffic
– Installation of additional malware (trojans, ransomware)

3. Privacy Implications

Both keyloggers and spyware invade user privacy at the deepest level:
– Steal private conversations and personal photos
– Track location and online behavior
– Record search habits and financial activities
– Enable blackmail, stalking, and identity theft
– Remove any sense of digital confidentiality

14(b)(ii) Explain the concept of SQL injection and how it can exploit database vulnerabilities.

SQL Injection is a code-injection attack where an attacker inserts malicious SQL commands into input fields (such as login forms or search boxes) to manipulate the backend database.

1. How SQL Injection Works

An application fails to validate or sanitize user input.
Example vulnerable query:

```
SELECT * FROM users WHERE username = ' " + input + " ' AND password = ' " + input2 + " ';
```

If attacker inputs:

```
' OR '1'='1
```

The query becomes always true.

2. What Attackers Can Do

– Bypass login authentication
– Read sensitive data (users, passwords, financial info)
– Modify or delete database records
– Dump entire database tables
– Execute administrative operations (DROP TABLE, UPDATE, INSERT)
– Gain shell access in advanced cases (e.g., SQLi → RCE)

3. Why SQL Injection Happens

– No input validation
– Concatenating user input directly into SQL queries
– Weak config of database privileges
– Missing prepared statements or ORM protections

4. Database Vulnerabilities Exploited

– Lack of parameterized queries
– Poor access control (admin rights for app users)
– Detailed error messages revealing SQL structure
– Outdated DBMS with known exploits

Part C

15(i) Explain the role of Intrusion Detection Systems (IDS) in network security, including its importance and types.

An **Intrusion Detection System (IDS)** monitors network or system activities to detect malicious behavior, policy violations, or security breaches. It acts like a security camera for digital infrastructure.

Role of IDS

– Continuously examines traffic, logs, and system activity.
– Identifies suspicious patterns such as port scans, brute-force attempts, malware signatures, or abnormal traffic spikes.
– Alerts administrators immediately so they can react before damage spreads.
– Provides early warning to reduce impact of attacks like ransomware, DDoS, unauthorized access, and privilege escalation.

Importance

– Helps detect attacks that bypass firewalls or antivirus.
– Reduces mean time to detect (MTTD) and respond (MTTR).
– Essential for compliance (ISO 27001, SOC2) requiring monitoring.
– Supports forensic investigation by storing attack logs.
– Improves overall situational awareness in a network.

Types of IDS

1. Network-based IDS (NIDS)

Monitors network packets flowing across segments.
Useful for detecting worms, scanning, MITM, DDoS.

2. Host-based IDS (HIDS)

Runs on individual machines.
Monitors system calls, logs, file changes, rootkits.

3. Signature-based IDS

Detects known attack patterns.
Fast but cannot detect new threats.

4. Anomaly-based IDS

Learns normal behavior and flags deviations.
Can detect zero-day attacks but may generate false alarms.

15(ii) Describe the ElGamal encryption scheme and its advantages over RSA.

ElGamal encryption is an asymmetric key cryptosystem based on the difficulty of the **Discrete Logarithm Problem** in modular arithmetic. It provides encryption and digital signatures.

Working of ElGamal Encryption

1. Key Generation

– Select a large prime number **p** and generator **g**.
– Choose private key **x**.
– Compute public key $y = g^x \bmod p$.

2. Encryption

To encrypt message **m**:
– Choose random number **k**.
– Compute:

$C1 = g^k \bmod p$
$C2 = m \times y^k \bmod p$

Ciphertext = (C1, C2)

3. Decryption

Receiver computes:

$m = C2 \times (C1^x)^{-1} \bmod p$

This retrieves the original message.

Advantages Over RSA:

1. **Higher Security Per Bit**
   ElGamal relies on discrete logarithms, which are harder mathematically than RSA's factoring problem.
2. **Semantic Security (Randomness)**
   Each encryption uses a new random value **k**, making ciphertext unpredictable.
   RSA is deterministic unless padding is added.
3. **Better Resistance to Certain Cryptanalytic Attacks**
   ElGamal's probabilistic nature avoids many pattern-based attacks.
4. **Preferred in Modern Cryptosystems**
   Used in PGP, GnuPG, and several secure communication protocols.

ElGamal provides strong confidentiality and is considered safer for many modern cryptographic applications.

15(iii) Compare quantitative and qualitative risk control practices and their applicability in different scenarios.

Risk control practices decide how an organization handles identified risks. They can be **quantitative** or **qualitative** depending on how risk is measured.

Quantitative Risk Control:

Uses **numerical and financial values** to measure risk.

Features:

– Assigns monetary value to assets, impact, and probability
– Uses metrics like Annual Loss Expectancy (ALE)
– Helps calculate Return on Security Investment (ROSI)
– Requires statistical data and historical attack patterns

When applicable:

– Large organizations with measurable data
– Financial planning, insurance decisions
– Cost–benefit analysis of security controls

Qualitative Risk Control:

Uses **descriptive scales** (high/medium/low) instead of numeric values.

Features:

– Based on expert judgment, experience, and interviews
– Faster and easier to perform
– Good for identifying areas needing immediate attention
– Useful when data is insufficient for mathematical analysis

When applicable:

– Startups, SMEs, or new systems
– Early-stage risk assessments
– Situations where probability/impact cannot be quantified precisely

---

15(iv) Describe how proxy servers and anonymizers work to provide online privacy

Proxy servers and **anonymizers** act as intermediaries between a user and the internet to hide identity, location, and browsing activity.

1. Proxy Servers

A proxy forwards user requests to websites on their behalf.

How they provide privacy:

– **Hide IP address** from websites
– Filter, block, or allow traffic based on rules

– Cache pages to reduce tracking
– Prevent direct communication between user and destination server

Uses:

– Bypassing geographic restrictions
– Corporate content filtering
– Basic identity masking

---

2. Anonymizers

More privacy-focused than standard proxies.

How they work:

– Route traffic through multiple anonymous servers
– Strip identifying information (cookies, headers, metadata)
– Prevent tracking and profiling
– Encrypt communications when paired with tools like VPN/Tor

Uses:

– Avoiding surveillance
– Protecting journalists, activists, whistleblowers
– Preventing behavioral tracking by advertisers
