UNIT WISE Sample Question and Answers

UNIT - I: Web Security

1. What are the common web security risks?

   Common web security risks include SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and man-in-the-middle attacks.

2. Explain the best practices for web security.

   Best practices for web security include using HTTPS, validating and sanitizing user inputs, using secure cookies, and regular security audits.

3. How does cryptography enhance web security?

   Cryptography enhances web security by ensuring data confidentiality, integrity, and authentication through encryption, digital signatures, and hashing algorithms.

4. Discuss the legal restrictions on cryptography.

   Legal restrictions on cryptography vary by country; for instance, some countries have laws limiting the use or export of strong encryption technologies.

5. What is digital identification and how is it used in web security?

   Digital identification involves using digital certificates and public key infrastructure (PKI) to authenticate and verify the identities of users and devices on the web.

UNIT - II: Privacy and Web Server Security

1. How can web users protect their privacy online?

   Web users can protect their privacy by using VPNs, enabling two-factor authentication, using strong passwords, and being cautious with the information they share online.

2. What are the techniques for ensuring physical security of servers?

   Techniques for physical security of servers include controlled access to server rooms, surveillance cameras, and secure rack enclosures.

3. Describe the methods for securing web applications.

   Methods for securing web applications involve input validation, secure coding practices, regular security testing, and using application firewalls.

4. What are the best practices for web server security?

   Best practices for web server security include keeping software up-to-date, using firewalls, disabling unnecessary services, and monitoring server logs.

5. How do backups and anti-theft measures contribute to web security?

   Backups ensure that data can be recovered in case of data loss, while **anti-theft measures** protect the physical hardware from being stolen or tampered with.

UNIT - III: Database Security

1. What are the recent advances in access control for databases?

   Recent advances in access control include role-based access control (RBAC), attribute-based access control (ABAC), and fine-grained access control mechanisms.

2. Explain access control models for XML databases.

   Access control models for XML databases include element-level access control, XML security labels, and XPath-based access control.

3. Discuss trust management and trust negotiation in database security.

   Trust management and trust negotiation involve establishing and verifying trust relationships between parties in a database system, often using digital certificates and policies.

4. How is security maintained in data warehouses and OLAP systems?

   Security in data warehouses and OLAP systems is maintained through encryption, access control, and secure data transmission protocols.

5. What are the common database issues in trust management?

   Common database issues in trust management include establishing trust relationships, ensuring data integrity, and protecting sensitive information.

UNIT - IV: Security Re-engineering for Databases

1. What is database watermarking and how is it used for copyright protection?

   Database watermarking is a technique used to embed a unique identifier in a database to protect intellectual property and detect unauthorized copying.

2. Explain the concepts and techniques of security re-engineering for databases.

   Security re-engineering for databases involves redesigning and improving database security measures to address new threats and vulnerabilities.

3. How do trustworthy records retention practices contribute to database security?

   Trustworthy records retention practices ensure that data is stored securely, complies with legal requirements, and can be retrieved reliably when needed.

4. Describe damage quarantine and recovery in data processing systems.

   Damage quarantine and recovery involves isolating and mitigating the effects of security breaches to prevent further damage and restoring affected data to its original state.

5. What are Hippocratic databases and their capabilities?

   Hippocratic databases are designed to ensure privacy protection by embedding privacy policies within the database and enforcing them during data access.

UNIT - V: Privacy in Database Publishing

1. What is the Bayesian perspective on privacy in database publishing?

   The Bayesian perspective on privacy involves using Bayesian inference methods to manage and protect privacy in data publishing.

2. How is privacy-enhanced location-based access control implemented?

   Privacy-enhanced location-based access control uses techniques like anonymization, pseudonymization, and encryption to protect user location data while allowing controlled access.

3. Explain the methods for efficiently enforcing security and privacy policies in a mobile environment.

   Efficient enforcement of security and privacy policies in a mobile environment involves using lightweight cryptographic protocols, context-aware access control, and secure communication channels.

4. Discuss the future trends in privacy and database publishing.

   Future trends in privacy and database publishing may include advancements in homomorphic encryption, differential privacy, and secure multi-party computation.

5. What challenges are associated with privacy in database publishing?

   Challenges in privacy and database publishing include balancing data utility and privacy, protecting against re-identification attacks, and ensuring compliance with privacy regulations.