Important Questions with Answers for MID – 1 (Sep 2025)
WDS

1. **What is the significance of cryptography in view of web security and what are the legal restrictions on cryptography?**
2. **Discuss in detail about privacy-protecting techniques.**
3. **Describe and Differentiate Security vulnerability, threat and Risk?**
4. **Explain different cryptographic protocols.**
5. **What are the different types of backups.**
6. **Discuss the strategies for managing multiple usernames and passwords.**
7. **What points to be considered in choosing an Internet service Provider**
8. **Explain in detail how Kerberos and Diffie-Hellman Alg can be used for authentication?**
9. **Explain the mechanisms used for protecting database server.**
10. **Explain in detail about the different types of Access Control Models.**

Answers

1. Significance of Cryptography in Web Security & Legal Restrictions

Importance in Web Security

Cryptography is the backbone of secure communication on the internet. It ensures:

- **Confidentiality**: Data is encrypted so only authorized parties can read it.
- **Integrity**: Hashing ensures data hasn't been tampered with.
- **Authentication**: Digital signatures and certificates verify identities.
- **Non-repudiation**: Prevents denial of actions (e.g., signed transactions).

Applications:

- HTTPS (SSL/TLS)
- Secure email (PGP, S/MIME)
- VPNs
- Blockchain and digital currencies

Legal Restrictions

Cryptography is regulated to balance privacy and national security:

- **Export Controls**: Many countries restrict exporting strong encryption (e.g., U.S. EAR regulations).
- **Government Access**: Some laws mandate backdoors or key escrow (e.g., India's IT Act).
- **Use Restrictions**: In some regions, using certain encryption tools without registration is illegal.

2. Privacy-Protecting Techniques

Key Techniques

- **End-to-End Encryption**: Ensures only sender and receiver can read messages (e.g., Signal, WhatsApp).
- **Anonymous Browsing**: Tools like Tor or VPNs mask IP addresses.
- **Secure Search Engines**: DuckDuckGo, Startpage avoid tracking.
- **Cookie Management**: Blocking third-party cookies reduces tracking.
- **Browser Extensions**: Privacy Badger, Ghostery block trackers.
- **Data Minimization**: Collect only necessary user data.
- **Differential Privacy**: Adds noise to datasets to protect individual identities.

3. Vulnerability vs Threat vs Risk

Term	Definition	Example
Vulnerability	Weakness in a system that can be exploited	Unpatched software
Threat	Potential cause of harm exploiting a vulnerability	Malware, phishing
Risk	Likelihood and impact of a threat exploiting a vulnerability	Data breach due to weak password

Formula: Risk = Threat × Vulnerability

4. Cryptographic Protocols

Common Protocols

- **SSL/TLS**: Secures web traffic (HTTPS)
- **IPSec**: Secures IP communications (VPNs)
- **SSH**: Secure remote login
- **PGP**: Encrypts emails
- **Kerberos**: Network authentication using tickets
- **Diffie-Hellman**: Secure key exchange
- **OAuth**: Authorization for APIs
- **S/MIME**: Secure email messaging

5. Types of Backups

Type	Description
Full Backup	Entire data copied
Incremental Backup	Only changes since last backup

Type	Description
Differential Backup	Changes since last full backup
Mirror Backup	Exact replica; deletes files if removed from source
Local Backup	Stored on physical devices (e.g., HDD, NAS)
Offsite Backup	Stored in remote locations or cloud
Cloud Backup	Online backup services (e.g., Google Drive, AWS)

6. Managing Multiple Usernames and Passwords

Strategies

- **Password Managers**: Tools like Bitwarden, LastPass store and generate strong passwords.
- **Multi-Factor Authentication (MFA)**: Adds extra layer (OTP, biometrics).
- **Single Sign-On (SSO)**: One login for multiple services.
- **Unique Passwords**: Avoid reuse across platforms.
- **Regular Updates**: Change passwords periodically.
- **Avoid Browser Storage**: Use encrypted vaults instead.

7. Choosing an Internet Service Provider (ISP)

Key Considerations

- **Availability**: Coverage in your area
- **Speed**: Download/upload rates
- **Reliability**: Uptime and performance
- **Cost**: Monthly fees, installation charges
- **Contract Terms**: Lock-in periods, cancellation fees
- **Customer Support**: Responsiveness and service quality
- **Security**: Protection against malware, firewalls
- **Bundled Services**: TV, phone, cloud storage

8. Kerberos & Diffie-Hellman for Authentication

Kerberos

- Uses a **Key Distribution Center (KDC)** with:
  - Authentication Server (AS)
  - Ticket Granting Server (TGS)
- Process:
  1. User logs in → gets Ticket Granting Ticket (TGT)
  2. TGT used to request service ticket
  3. Service ticket used to access resources

Diffie-Hellman

- Enables secure key exchange over insecure channels.
- Each party generates a private and public key.
- Shared secret is computed using: $$ \text{Shared Key} = g^{ab} \mod p $$
- Used in VPNs, TLS, and secure messaging.

9. Protecting Database Servers

Mechanisms

- **Authentication & Authorization**: Role-based access
- **Encryption**: At rest and in transit
- **Firewalls**: Restrict unauthorized access
- **Regular Updates**: Patch vulnerabilities
- **Database Activity Monitoring (DAM)**: Logs and alerts
- **Backup & Recovery**: Regular backups
- **Segmentation**: Separate production and test environments
- **Least Privilege Principle**: Minimal access rights

10. Access Control Models

Model	Description
DAC	Owner decides access (flexible but less secure)
MAC	Central authority assigns access based on classification
RBAC	Access based on user roles (e.g., admin, HR)
ABAC	Access based on attributes (e.g., time, location, device)
RuBAC	Access based on rules (e.g., time-based restrictions)
OrBAC	Organization-level policies independent of implementation
IBAC	Identity-based access (individual user control)

********** *Wish you all the best* **********