Exam Cram Notes: Cryptographic Solutions

Cryptography secures data through encryption, hashing, and key management to ensure **confidentiality, integrity, and authenticity** in security systems.

---

1. Encryption

Encryption converts plaintext into **ciphertext** using an algorithm and a key.

Types of Encryption

1. **Symmetric Encryption (Secret Key)**
    - Uses a **single key** for encryption and decryption.
    - Fast and efficient, but **key distribution** is a challenge.
    - Example Algorithms:
        - **AES (Advanced Encryption Standard) – Strongest, used in WPA3, SSL/TLS**
        - **DES (Data Encryption Standard) – Weak, replaced by AES**
        - **3DES – Stronger than DES, but outdated**
        - **RC4 – Stream cipher, insecure**
2. **Asymmetric Encryption (Public/Private Key)**
    - Uses a **key pair (public and private keys)**.
    - Public key encrypts, private key decrypts.
    - Slower but **used for secure key exchange**.
    - Example Algorithms:
        - **RSA – Used in SSL/TLS, digital signatures**
        - **ECC (Elliptic Curve Cryptography) – More efficient than RSA**
        - **Diffie-Hellman – Secure key exchange**

---

2. Hashing

A one-way function that generates a unique fixed-size hash from input data.

- Used for **integrity checking**, password storage, and digital signatures.
- Example Algorithms:
    - **SHA-256 (Secure Hash Algorithm) – Common in blockchain & digital signatures**
    - **MD5 – Weak, vulnerable to collisions**
    - **HMAC (Hashed Message Authentication Code) – Adds authentication to hashing**

Example:
🔷 **Password hashing –** Hashing passwords before storing them in a database (**bcrypt, PBKDF2, Argon2** are best practices).

---

3. Digital Signatures

- Provides **authentication, integrity, and non-repudiation**.
- Uses **asymmetric encryption**:
  - The sender signs with their **private key**.
  - The receiver verifies with the **public key**.
- Example: Used in **email security (PGP), software signing, and digital certificates**.

---

4. Public Key Infrastructure (PKI)

- A framework that manages **digital certificates and encryption keys**.
- Components:
  - **Certificate Authority (CA)** – Issues and revokes digital certificates.
  - **Registration Authority (RA) –** Verifies user identity.
  - **Certificate Revocation List (CRL) & Online Certificate Status Protocol (OCSP) –** Tracks revoked certificates.

Example: **SSL/TLS certificates** for secure web browsing.

---

5. Transport Encryption (Data in Transit Security)

- Secures communication over networks.
- **Protocols:**
  - **TLS (Transport Layer Security) –** Secures HTTPS, email, VPNs.
  - **SSL (Secure Sockets Layer) – Deprecated, replaced by TLS.**
  - **IPsec (Internet Protocol Security) –** Secures VPN connections.

Example: TLS encrypts **HTTPS traffic** for secure browsing.

---

6. Data at Rest Encryption

- Protects stored data from unauthorized access.
- **Examples:**
  - **BitLocker (Windows) & FileVault (macOS) –** Full disk encryption.

- **Database Encryption –** AES-encrypted data storage.
- **Hardware Security Module (HSM) –** Secure key storage.

---

7. Email and File Encryption

- **PGP (Pretty Good Privacy) –** Encrypts emails and files.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions) –** Uses PKI for email encryption.

Key Exam Tips

✅ Know the difference between **symmetric vs. asymmetric encryption** and their use cases.
✅ Understand **hashing vs. encryption** and when to use each.
✅ Be familiar with **digital signatures, TLS, PKI, and data encryption methods**.
✅ Expect scenario-based questions on **choosing the right cryptographic solution**.