Cryptography & Web Security Exam Preparation Notes

1. Overview of Cryptography

Cryptography is the science of securing information using mathematical techniques. It ensures:

- Confidentiality

- Integrity

- Authentication

- Non-repudiation

Historical Milestones:

- Ancient civilizations: Egypt, Rome (Caesar cipher)

- 1970s: DES by IBM, public adoption of secure encryption

- 1976: Diffie-Hellman key exchange (start of public-key cryptography)

- 1978: RSA algorithm

2. Information Security Goals

Main goals of cryptography:

1. Confidentiality: Prevent unauthorized data access.

2. Integrity: Ensure data is unaltered.

3. Authentication: Verify identity.

4. Non-repudiation: Prevent denial of sent messages.

Other terms include: authorization, access control, timestamping, ownership, anonymity, etc.

3. Cryptographic Primitives

Building blocks:

- Encryption (symmetric & public-key)

- Digital signatures

- Hash functions

- MACs

- Random & pseudorandom generators

Evaluation based on: security, functionality, performance, implementation ease.

4. Symmetric-Key Encryption

Same key used for encryption and decryption. Fast but needs secure key sharing.

Types:

- Block ciphers: Encrypt data in blocks (e.g., AES, DES)

- Stream ciphers: Encrypt data bit-by-bit (e.g., Vernam cipher)

Classic Techniques:

- Substitution (monoalphabetic, polyalphabetic)

- Transposition

- Product ciphers (multiple rounds of substitution + transposition)

5. Public-Key Cryptography

Asymmetric key system: Public key encrypts, private key decrypts.

Applications:

- RSA: Based on factoring large integers

- Diffie-Hellman: Secure key exchange

- ElGamal: Based on discrete log problem

Uses:

- Secure key distribution

- Digital signatures

- Email and communication encryption

6. Digital Signatures

Ensure authenticity and non-repudiation of messages.

Process:

1. Signer generates a signature using private key.

2. Receiver verifies it using public key.

Must be unique, message-dependent, and hard to forge.

7. Hash Functions

Used for integrity and authentication.

Properties:

- Preimage resistance

- Second preimage resistance

- Collision resistance

Common uses: password storage, digital signatures, checksums.

8. Key Management

Managing cryptographic keys is critical:

- Generation

- Exchange (e.g., via PKI)

- Storage

- Revocation

Includes certificate authorities, trust models, and secure transport.

9. Attacks & Security Models

Common attack models:

- Ciphertext-only

- Known-plaintext

- Chosen-plaintext

- Chosen-ciphertext

Security must withstand worst-case scenarios to be considered robust.