UTT

UNIVERSIDAD TECNOLÓGICA DE TIJUANA

GOBIERNO DE BAJA CALIFORNIA

**TOPIC:**

Data encryption mechanisms in mobile applications

**STUDENT:**

Paredes Nevarez Alexis Omar

**GROUP:**

10B

**SUBJECT:**

Comprehensive Mobile Development

**PROFESSOR:**

Ray Brunett Parra Galaviz

Tijuana, Baja California, 24 de Enero de 2025

## DATA ENCRYPTION MECHANISMS IN MOBILE APPLICATIONS

Data encryption is a security mechanism that converts information into an unreadable format for unauthorized users. It uses mathematical algorithms to transform the data into ciphertext, which can only be decrypted with a specific key.

## IMPORTANCE OF ENCRYPTION IN MOBILE APPLICATIONS

Encryption is critical in mobile applications because:

- Protects sensitive data: Applications handle passwords, financial information, private messages, etc.
- Compliance with regulations: Laws like GDPR, HIPAA, or PCI DSS require encryption to safeguard user privacy.
- Prevents unauthorized access: Minimizes the impact of attacks like network interception or physical access to devices.

## COMMON TYPES OF ENCRYPTION

### a) Symmetric encryption

- Features: Uses the same key for encryption and decryption.
- Algorithm example: AES (Advanced Encryption Standard).
- Uses: Storing sensitive data locally in the app or databases.

### b) Asymmetric encryption

- Features: Uses a pair of keys: a public key for encryption and a private key for decryption.
- Algorithm example: RSA (Rivest-Shamir-Adleman).
- Uses: Securing data transmission, such as authentication or key exchanges.

### c) Hashing

- Features: A one-way encryption method used to ensure data integrity.
- Algorithm example: SHA-256 (Secure Hash Algorithm).
- Uses: Storing passwords or verifying file integrity.

## ENCRYPTION MECHANISMS IN MOBILE APPLICATIONS

### a) Database encryption

- Use libraries like SQLCipher to encrypt SQLite databases locally.

### b) Local storage encryption

- Android: Use Keystore to securely store cryptographic keys.
- iOS: Use Keychain Services to protect sensitive data.

### c) Data-in-transit encryption

- Implement TLS (Transport Layer Security) to encrypt communication between the app and server.

### d) Message encryption

- Use libraries like Signal Protocol (used by WhatsApp) for end-to-end encryption (E2EE).

### e) Tokenization

- Replace sensitive data like credit card numbers with non-sensitive tokens.

## BEST PRACTICES

1. **Secure key storage**
   - Never store keys in plaintext or within the source code.
   - Use secure storage like Android Keystore or iOS Secure Enclave.

2. **Use secure algorithms**
   - Avoid outdated algorithms like DES or MD5. Use AES and SHA-256 instead.

3. **Encrypt sensitive data**
   - Always encrypt personal data, whether in transit or at rest.

4. **Implement access controls**
   - Restrict access to encrypted data to authenticated users only.

5. **Perform security testing**
   - Identify encryption vulnerabilities using tools like the OWASP Mobile Security Testing Guide.