UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA:

Cómo Utilizar el Cifrado en Móviles

PRESENTADO POR:

Hernández Miranda Rafael Francisco

GRUPO:

10B

MATERIA:

Gestión del Proceso de Desarrollo de Software

PROFESOR:

Ray Brunett Parra Galaviz

FECHA:

27/01/2025.

Introducción

En la era digital, los dispositivos móviles almacenan y transmiten una gran cantidad de información sensible, como credenciales de usuario, datos financieros y archivos privados. Debido al aumento de ciberataques y vulnerabilidades en las aplicaciones móviles, garantizar la seguridad de estos datos se ha convertido en una prioridad.

¿Cómo Utilizar el Cifrado en Móviles?

El cifrado es una técnica esencial para proteger la información en dispositivos móviles contra accesos no autorizados. En el contexto de la seguridad móvil, se aplica en diferentes niveles, como el almacenamiento de datos, la comunicación y la autenticación.

1. **Cifrado de Almacenamiento**
    - Full-Disk Encryption (FDE): Protege todo el sistema de archivos del dispositivo (usado en Android y iOS).
    - File-Based Encryption (FBE): Cifra archivos individuales, permitiendo que algunos archivos sean accesibles antes de que el usuario desbloquee el dispositivo.
2. **Cifrado de Comunicación**
    - TLS (Transport Layer Security): Protege la comunicación entre el dispositivo y los servidores web (HTTPS).
    - End-to-End Encryption (E2EE): Aplicado en mensajería (ej. WhatsApp, Signal).
    - VPN (Virtual Private Network): Protege el tráfico de red en conexiones públicas.
3. **Cifrado en Bases de Datos y Almacenamiento Local**
    - SQLCipher (SQLite cifrado para Android e iOS).
    - Encriptación de SharedPreferences en Android con EncryptedSharedPreferences.
    - Keychain en iOS para almacenar credenciales de forma segura.
4. **Cifrado de Contraseñas y Tokens de Autenticación**
    - Uso de bcrypt o Argon2 para almacenar contraseñas de usuarios.
    - Uso de HMAC para proteger tokens en la autenticación.

¿Cuándo Utilizar el Cifrado en Móviles?

El cifrado debe implementarse en situaciones donde la seguridad de los datos es crítica. Algunos casos incluyen:

1. **Cuando se manejan datos sensibles del usuario**
    - Información personal (nombres, direcciones, números de teléfono).
    - Datos financieros (números de tarjetas, cuentas bancarias).
    - Credenciales de inicio de sesión y tokens de autenticación.
2. **Cuando se almacenan datos en el dispositivo**
    - Se recomienda cifrar archivos en dispositivos móviles para evitar accesos en caso de robo o pérdida del dispositivo.
3. **Cuando se transmiten datos entre la app y el servidor**
    - Usar TLS 1.2 o superior para evitar ataques de interceptación de datos.
4. **Cuando se requiere autenticación biométrica**
    - Uso de Android BiometricPrompt o iOS Face ID/Touch ID con cifrado de claves para acceso seguro.

Conclusión

El cifrado es una medida de seguridad indispensable en el desarrollo móvil para proteger los datos de los usuarios contra accesos no autorizados. Su uso debe aplicarse en almacenamiento, transmisión de datos y autenticación para evitar vulnerabilidades en las aplicaciones móviles.

Bibliografía

Cifrado de la información. (s/f). Incibe.es. Recuperado el 5 de febrero de 2025, de https://www.incibe.es/ciudadania/tematicas/cifrado

Criptografía. (s/f). Android Developers. Recuperado el 5 de febrero de 2025, de https://developer.android.com/privacy-and-security/cryptography?hl=es-419

ManageEngine. (s/f). *Cifrado de dispositivos para Android*. Manageengine.com. Recuperado el 5 de febrero de 2025, de https://www.manageengine.com/latam/mobile-device-management/cifrado-de-dispositivos-android.html