UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA

Mecanismos de cifrado de datos en aplicaciones móviles

PRESENTADO POR

Perez Bello Vanory Esperanza

GRUPO

10° B

MATERIA

Desarrollo Movil Integral

PROFESOR

Ray Brunett Parra Galaviz

Tijuana, Baja California, 24 Enero del 2025

Mecanismos de cifrado de datos en aplicaciones móviles

Introducción

El cifrado de datos es un proceso esencial en el desarrollo de aplicaciones móviles que busca proteger la información sensible contra accesos no autorizados. En un mundo donde las aplicaciones manejan datos confidenciales como contraseñas, información personal y financiera, el uso de mecanismos de cifrado asegura la privacidad y seguridad de los usuarios.

Tipos de cifrado

Existen dos principales enfoques para el cifrado de datos:

1. **Cifrado simétrico**:
    - Utiliza la misma clave para cifrar y descifrar los datos.
    - Ejemplo: Algoritmo AES (Advanced Encryption Standard).
    - Ventaja: Es rápido y eficiente.
    - Desventaja: La gestión de claves puede ser compleja si se necesita compartir la clave.
2. **Cifrado asimétrico**:
    - Utiliza un par de claves: una pública para cifrar y una privada para descifrar.
    - Ejemplo: Algoritmo RSA (Rivest-Shamir-Adleman).
    - Ventaja: Proporciona mayor seguridad en el intercambio de claves.
    - Desventaja: Es más lento comparado con el cifrado simétrico.

Algoritmos populares

1. **AES (Advanced Encryption Standard):**
    - Estándar de cifrado ampliamente utilizado en aplicaciones móviles.
    - Ofrece una combinación de seguridad y eficiencia.
2. **RSA:**
    - Utilizado para la encriptación de pequeñas cantidades de datos o para el intercambio seguro de claves.
3. **ECC (Elliptic Curve Cryptography):**
    - Algoritmo que proporciona alta seguridad con claves más cortas.
    - Ideal para dispositivos móviles con limitaciones de recursos.

Implementación en plataformas móviles

1. **Android**:
    - Proporciona la API de Seguridad (Android Keystore) para generar y almacenar claves de cifrado.
    - Soporte nativo para AES, RSA y ECC.
2. **iOS**:
    - Utiliza el Keychain y el Secure Enclave para manejar claves de manera segura.
    - Ofrece herramientas como CommonCrypto y CryptoKit.

Buenas prácticas

- Utilizar librerías confiables para evitar errores de implementación manual.
- Asegurarse de que las claves nunca se almacenen en texto plano.
- Habilitar el cifrado de extremo a extremo en aplicaciones de comunicación.
- Actualizar regularmente las bibliotecas de cifrado para protegerse contra vulnerabilidades.

Desafíos del cifrado en aplicaciones móviles

- **Rendimiento:** Algunos algoritmos pueden ser lentos y consumir más recursos.
- **Gestión de claves:** Proteger las claves contra accesos no autorizados es un reto constante.
- **Cumplimiento normativo:** Asegurarse de que el cifrado cumpla con estándares legales y de seguridad.

Conclusión

El cifrado de datos en aplicaciones móviles es una herramienta esencial para proteger la información del usuario y garantizar su privacidad. Aunque presenta desafíos técnicos, su correcta implementación reduce significativamente los riesgos asociados a brechas de seguridad y ataques cibernéticos.

Google. (n.d.). Android Developers. Retrieved January 24, 2025, from https://developer.android.com

Apple Inc. (n.d.). Apple Developer. Retrieved January 24, 2025, from https://developer.apple.com

OWASP Foundation. (n.d.). OWASP Mobile Security Project. Retrieved January 24, 2025, from https://owasp.org