UTT

UNIVERSIDAD TECNOLÓGICA DE TIJUANA

GOBIERNO DE BAJA CALIFORNIA

TEMA: Data encryption mechanisms in mobile apps

PRESENTADO POR: Ramírez Aispuro Juan José

GRUPO: 10-B

MATERIA: Desarrollo Móvil Integral

PROFESOR: Ray Brunett Parra Galaviz

Tijuana, Baja California, 01/24/2024

Data encryption is a critical component of mobile application security, ensuring the confidentiality and integrity of sensitive information. By converting readable data into an unreadable format, encryption protects it from unauthorized access.

Types of Data Encryption in Mobile Applications:

1. **Data at Rest Encryption:** Protects data stored on the device, such as databases and files. Both Android and iOS offer built-in encryption features to secure stored data.
2. **Data in Transit Encryption:** Secures data transmitted over networks, including cellular and Wi-Fi connections. Protocols like TLS (Transport Layer Security) are commonly used to encrypt data during transmission.

Best Practices for Implementing Data Encryption:

- **Use Strong Encryption Algorithms:** Employ robust algorithms like AES (Advanced Encryption Standard) to ensure high security levels.
- **Manage Encryption Keys Securely:** Implement secure key management practices to protect encryption keys from unauthorized access.
- **Regularly Update and Patch Applications:** Keep applications updated to address known vulnerabilities and enhance security measures.
- **Educate Users on Security Practices:** Inform users about the importance of using strong passwords and enabling two-factor authentication to further protect their data.

By adhering to these practices, developers can significantly enhance the security of mobile applications, safeguarding user data against potential threats.