UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

**TOPIC:**

Data Encryption Mechanisms in Mobile Applications continue

**PRESENTED BY:**

Padilla Virgen Jorge Luis

**GRUPO:**

10B

**SUBJECT:**

Desarrollo Movil Integral

**PROFESOR:**

Ray Brunett Parra Galaviz

Tijuana, Baja California, January 24th 2024

## Data Encryption Mechanisms in Mobile Applications

Data encryption in mobile applications is essential for protecting sensitive information from unauthorized access and ensuring user privacy. This process converts readable data into an encoded format that can only be deciphered by authorized entities.

### Encryption in Android:

Android provides the *Keystore* system, which allows applications to securely generate and store cryptographic keys. Recommended algorithms include AES in CBC or GCM modes with 256-bit keys for data encryption. Additionally, the SHA-2 family is advised for hashing and HMAC functions.

### Encryption in iOS:

iOS devices utilize a unique 256-bit key, known as the UID, stored in the device hardware. This key is combined with the user's passcode to generate an additional key that encrypts and protects stored data. A distinctive feature is that the UID cannot be extracted from the device, preventing brute-force attacks.

### Application Layer Encryption:

Beyond the encryption provided by the operating system, applications can implement encryption at the application layer. This approach ensures that data is encrypted before being transmitted over the network using algorithms like AES or RSA. This protects data even if lower network layers are compromised.

### Importance of Encryption:

Encryption protects the confidentiality and integrity of data, preventing unauthorized access and ensuring that information remains unaltered during transmission. It is a critical measure to safeguard user privacy and comply with data protection regulations.

Implementing robust encryption mechanisms is fundamental for developing secure and reliable mobile applications.