End-To-End Encryption in Mobile Apps

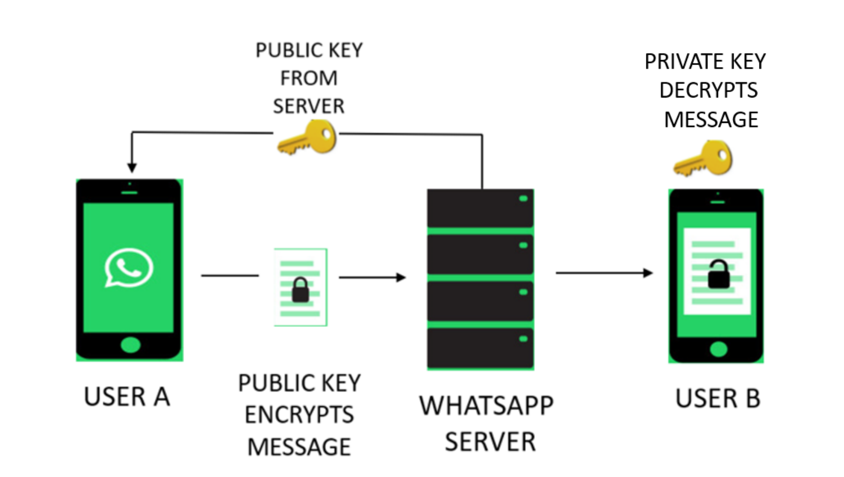
Messages transmitted to be read only by users and not by any third party

→

Implemented using asymmetric cryptography or public key systems

→

Servers not involved in the key generation process



How It Works?

Step1: Start Chatting!
Step2: Key1=Public Key & Key2=Secret Key
Step 3: E2E encryption apps exchange Key1
Step 4: Key 2 doesn’t leave the device!
Step 5: Encrypt using public key & decrypt using Secret Key

Background Story? Open Whisper Systems' Signal Protocol - Application Layer.

Examples: WhatsApp, Allo, Signal & FB Messenger

Non-federated cryptographic protocol used to provide end-to-end encryption

Double Ratchet Algorithm, prekeys, a triple Diffie–Hellman (3-DH) handshake, and Curve25519, AES-256 and HMAC-SHA256

REFERENCES: [Diffie-Helman key exchange]
https://faq.whatsapp.com/en/android/28030015/
https://xbsoftware.com/blog/video-messaging-apps-with-end-to-end-encryption-and-all-about-encrypted-text-messages/
http://resources.infosecinstitute.com/basics-of-cryptography-the-practical-application-and-use-of-cryptography/#gref
https://en.wikipedia.org/wiki/Open_Whisper_Systems