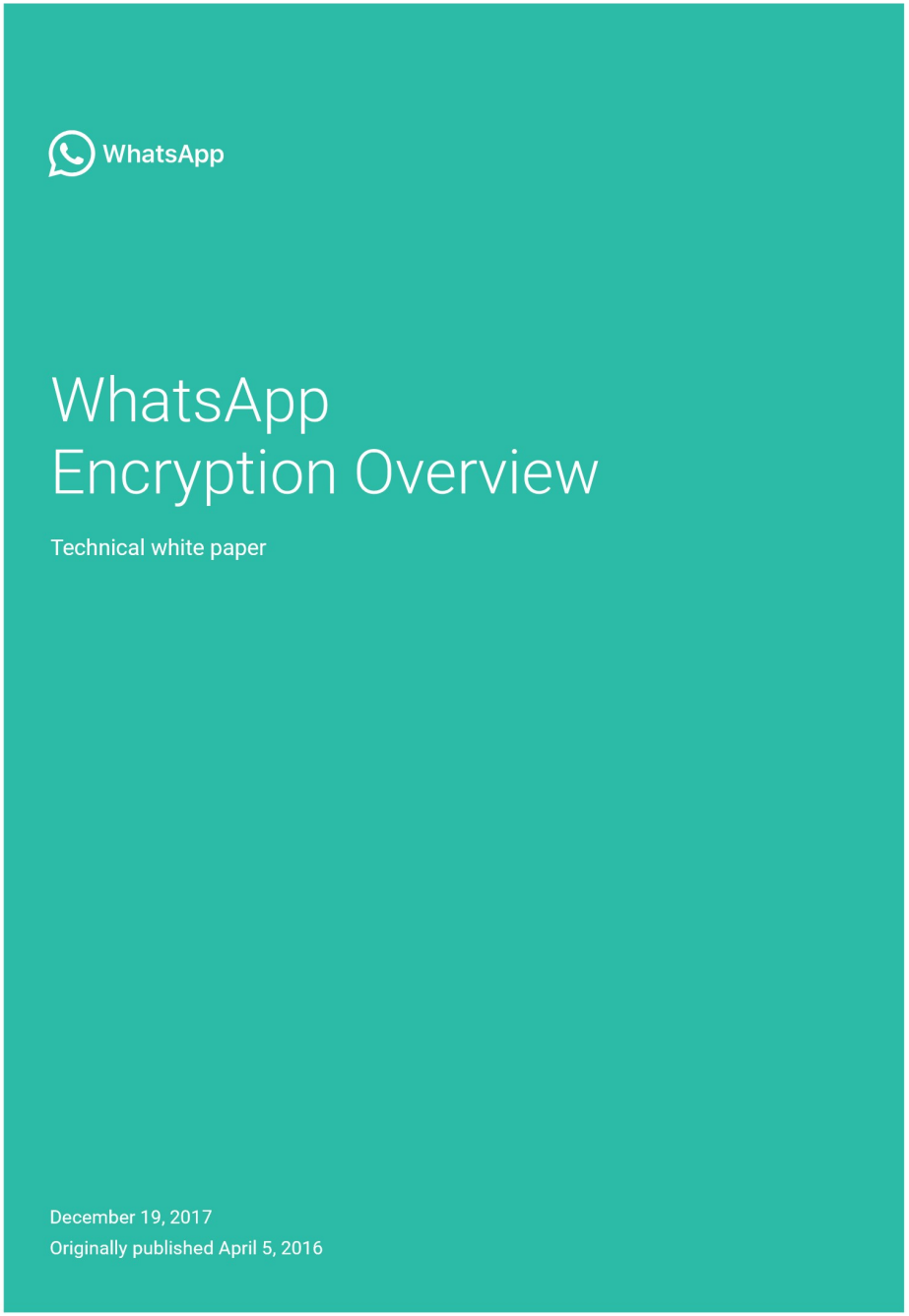
6.3 - Protocolos de comunicación segura

Ejemplo de protocolo de comunicación segura

- Signal Protocol
  - Desarrollado por Open Whisper Systems en 2013
  - Inicialmente para la app open-source ***TextSecure***, que finalmente se llamó ***Signal***.
- Usado por múltiples sistemas de comunicación:
  - WhatsApp
  - Facebook Messenger
  - Google Allo
- El 5 de abril de 2016, WhatsApp publicó un whitepaper explicando su implementación del protocolo.



- Cifrado punto a punto
- Protege las confidencialidad de las comunicaciones de terceras partes y de los servidores de WhatsApp.
- Si las claves de un dispositivo son comprometidas, no pueden ser usadas para descifrar mensajes del pasado.

Cifrado en bloque con clave secreta

Terms

Public Key Types

- `Identity Key Pair` – A long-term Curve25519 key pair, generated at install time.
- `Signed Pre Key` – A medium-term Curve25519 key pair, generated at install time, signed by the `Identity Key`, and rotated on a periodic timed basis.
- `One-Time Pre Keys` – A queue of Curve25519 key pairs for one time use, generated at install time, and replenished as needed.

Session Key Types

- `Root Key` – A 32-byte value that is used to create `Chain Keys`.
- `Chain Key` – A 32-byte value that is used to create `Message Keys`.
- `Message Key` – An 80-byte value that is used to encrypt message contents. 32 bytes are used for an AES-256 key, 32 bytes for a HMAC-SHA256 key, and 16 bytes for an IV.

Client Registration

At registration time, a WhatsApp client transmits its public `Identity Key`, public `Signed Pre Key` (with its signature), and a batch of public `One-Time Pre Keys` to the server. The WhatsApp server stores these public keys associated with the user's identifier. At no time does the WhatsApp server have access to any of the client's private keys.

Initiating Session Setup

To communicate with another WhatsApp user, a WhatsApp client first needs to establish an encrypted session. Once the session is established, clients do not need to rebuild a new session with each other until the existing session state is lost through an external event such as an app reinstall or device change.

To establish a session:

1. The initiating client ("initiator") requests the public `Identity Key`, public `Signed Pre Key`, and a single public `One-Time Pre Key` for the recipient.
2. The server returns the requested public key values. A `One-Time Pre Key` is only used once, so it is removed from server storage after being requested. If the recipient's latest batch of `One-Time Pre Keys` has been consumed and the recipient has not replenished them, no `One-Time Pre Key` will be returned.
3. The initiator saves the recipient's `Identity Key` as $I_{recipient}$, the `Signed Pre Key` as $S_{recipient}$, and the `One-Time Pre Key` as $O_{recipient}$.
4. The initiator generates an ephemeral Curve25519 key pair, $E_{initiator}$.
5. The initiator loads its own `Identity Key` as $I_{initiator}$.
6. The initiator calculates a master secret as `master_secret` = $ECDH(I_{initiator}, S_{recipient}) \,||\, ECDH(E_{initiator}, I_{recipient}) \,||\, ECDH(E_{initiator}, S_{recipient}) \,||\, ECDH(E_{initiator}, O_{recipient})$. If there is no `One Time Pre Key`, the final ECDH is omitted.
7. The initiator uses HKDF to create a `Root Key` and `Chain Keys` from the `master_secret`.

- **ECDH:** Elliptic-curve Diffie-Hellman
- **HKDF:** simple key derivation function basado en HMAC
- **HMAC:** hash-based message authentication

Receiving Session Setup

After building a long-running encryption session, the initiator can immediately start sending messages to the recipient, even if the recipient is offline. Until the recipient responds, the initiator includes the information (in the header of all messages sent) that the recipient requires to build a corresponding session. This includes the initiator's $E_{initiator}$ and $I_{initiator}$.

When the recipient receives a message that includes session setup information:

1. The recipient calculates the corresponding `master_secret` using its own private keys and the public keys advertised in the header of the incoming message.
2. The recipient deletes the `One-Time Pre Key` used by the initiator.
3. The initiator uses HKDF to derive a corresponding `Root Key` and `Chain Keys` from the `master_secret`.

Exchanging Messages

Once a session has been established, clients exchange messages that are protected with a `Message Key` using `AES256` in CBC mode for encryption and `HMAC-SHA256` for authentication.

The `Message Key` changes for each message transmitted, and is ephemeral, such that the `Message Key` used to encrypt a message cannot be reconstructed from the session state after a message has been transmitted or received.

The `Message Key` is derived from a sender's `Chain Key` that "ratchets" forward with every message sent. Additionally, a new ECDH agreement is performed with each message roundtrip to create a new `Chain Key`. This provides forward secrecy through the combination of both an immediate "hash ratchet" and a round trip "DH ratchet."

Calculating a `Message Key` from a `Chain Key`

Each time a new `Message Key` is needed by a message sender, it is calculated as:

1. `Message Key = HMAC-SHA256(Chain Key, 0x01).`
2. The `Chain Key` is then updated as `Chain Key = HMAC-SHA256(Chain Key, 0x02).`

This causes the `Chain Key` to "ratchet" forward, and also means that a stored `Message Key` can't be used to derive current or past values of the `Chain Key`.

Calculating a `Chain Key` from a `Root Key`

Each time a message is transmitted, an ephemeral `Curve25519` public key is advertised along with it. Once a response is received, a new `Chain Key` and `Root Key` are calculated as:

1. `ephemeral_secret = ECDH(Ephemeral`$_{sender}$`, Ephemeral`$_{recipient}$`).`

2. `Chain Key, Root Key = HKDF(Root Key, ephemeral_secret).`

A chain is only ever used to send messages from one user, so message keys are not reused. Because of the way `Message Keys` and `Chain Keys` are calculated, messages can arrive delayed, out of order, or can be lost entirely without any problems.

Transmitting Media and Other Attachments

Large attachments of any type (video, audio, images, or files) are also end-to-end encrypted:

1. The WhatsApp user sending a message ("sender") generates an ephemeral 32 byte `AES256` key, and an ephemeral 32 byte `HMAC-SHA256` key.
2. The sender encrypts the attachment with the `AES256` key in CBC mode with a random IV, then appends a MAC of the ciphertext using HMAC-SHA256.
3. The sender uploads the encrypted attachment to a blob store.
4. The sender transmits a normal encrypted message to the recipient that contains the encryption key, the HMAC key, a SHA256 hash of the encrypted blob, and a pointer to the blob in the blob store.
5. The recipient decrypts the message, retrieves the encrypted blob from the blob store, verifies the SHA256 hash of it, verifies the MAC, and decrypts the plaintext.

Group Messages

Traditional unencrypted messenger apps typically employ “server-side fan-out” for group messages. A client wishing to send a message to a group of users transmits a single message, which is then distributed N times to the N different group members by the server.

This is in contrast to “client-side fan-out,” where a client would transmit a single message N times to the N different group members itself.

Messages to WhatsApp groups build on the pairwise encrypted sessions outlined above to achieve efficient server-side fan-out for most messages sent to groups. This is accomplished using the “Sender Keys” component of the Signal Messaging Protocol.

The first time a WhatsApp group member sends a message to a group:

1. The sender generates a random 32-byte `Chain Key`.

2. The sender generates a random Curve25519 `Signature Key` key pair.

3. The sender combines the 32-byte `Chain Key` and the public key from the `Signature Key` into a `Sender Key` message.

1. The sender generates a random 32-byte `Chain Key`.

2. The sender generates a random Curve25519 `Signature Key` key pair.

3. The sender combines the 32-byte `Chain Key` and the public key from the `Signature Key` into a `Sender Key` message.

4. The sender individually encrypts the `Sender Key` to each member of the group, using the pairwise messaging protocol explained previously.

For all subsequent messages to the group:

1. The sender derives a `Message Key` from the `Chain Key`, and updates the `Chain Key`.

2. The sender encrypts the message using `AES256` in CBC mode.

3. The sender signs the ciphertext using the `Signature Key`.

4. The sender transmits the single ciphertext message to the server, which does server-side fan-out to all group participants.

The "hash ratchet" of the message sender's `Chain Key` provides forward secrecy. Whenever a group member leaves, all group participants clear their `Sender Key` and start over.

Call Setup

WhatsApp voice and video calls are also end-to-end encrypted.
When a WhatsApp user initiates a voice or video call:

1. The initiator builds an encrypted session with the recipient (as outlined in Section *Initiating Session Setup*), if one does not already exist.
2. The initiator generates a random 32-byte SRTP master secret.
3. The initiator transmits an encrypted message to the recipient that signals an incoming call, and contains the SRTP master secret.
4. If the responder answers the call, a SRTP encrypted call ensues.

Verifying Keys

WhatsApp users additionally have the option to verify the keys of the other users with whom they are communicating so that they are able to confirm that an unauthorized third party (or WhatsApp) has not initiated a man-in-the-middle attack. This can be done by scanning a QR code, or by comparing a 60-digit number.

The QR code contains:

1. A version.
2. The user identifier for both parties.
3. The full 32-byte public `Identity Key` for both parties.

When either user scans the other's QR code, the keys are compared to ensure that what is in the QR code matches the `Identity Key` as retrieved from the server.

Transport Security

All communication between WhatsApp clients and WhatsApp servers is layered within a separate encrypted channel. On Windows Phone, iPhone, and Android, those end-to-end encryption capable clients use Noise Pipes with Curve25519, AES-GCM, and SHA256 from the Noise Protocol Framework for long running interactive connections.

This provides clients with a few nice properties:

1. Extremely fast lightweight connection setup and resume.
2. Encrypts metadata to hide it from unauthorized network observers. No information about the connecting user's identity is revealed.
3. No client authentication secrets are stored on the server. Clients authenticate themselves using a Curve25519 key pair, so the server only stores a client's public authentication key. If the server's user database is ever compromised, no private authentication credentials will be revealed.