MÁSTER INTERUNIVERSITARIO EN CIBERSEGURIDAD

Information Security
Lab assignment IV: my WhatsApp

1 Double ratchet

The Double Ratchet encryption algorithm is widely used in messaging systems like WhatsApp, Signal, Facebook Messenger or Matrix for protecting the messages exchanged in a session between two parties. It makes use of many cryptographic primitives (public-key encryption, symmetric encryption, key derivation) covered in the course, so it forms a good exercise in learning these in a real application.

The Double Ratchet algorithm first establishes a secret shared key between the parties, using some key agreement protocol like X3DH. After that, the parties derive new keys for every message exchanged so that earlier keys cannot be calculated from the new ones. Diffie-Hellman public values are also calculated and attached to the messages. The main concept for understanding Double Ratchet is that of KDF chains.

The following Sections are a brief excerpt from the Double Ratchet public specification. Reading the specification is highly recommended before going through these notes.

2 Implementation

2.1 Initialization

We will skip the key agreement protocol that Double Ratchet stipulates. Instead

- Your client and server will have initially a (`PublicKey`, `PrivateKey`) key pair created with the Diffie-Hellman scheme.
- Your client and server will have initially the same `RootKey` (128 bits). Set the value directly in the code.

2.2 Double ratchet

- Diffie-Hellman ratchet
  - Use Diffie-Hellman for generating the (`PublicKey`, `PrivateKey`) key pairs.
  - Use HKDF to ratchet the Diffie-Hellman keys (see Section 5.2 in the specification).
  - The policy for generating new Diffie-Hellman keys is open to your decision: after sending n messages, after a timeout, per session, etc.
- Symmetric key ratchet
  - We will not encrypt the message headers.
  - Use HMAC to ratchet the symmetric keys.

– Use AES-GCM with 128 bits to perform encryption and decryption of messages. As we saw, AES-GCM is AEAD secure (authenticated encryption with associated data). AE = CPA + ciphertext integrity

2.3 Communication

Our communication model will not consider dropped messager nor out-of-order delivery. To guarantee such properties

- We will use an open MQTT server running at `mastropiero.det.uvigo.es` for exchanging the encrypted messages between clients.
- Publish and subscribe your messages on the channels `name.in` and `name.out`, where `name` if some name of yours (real or not).
- Use open source software libraries in your programming language for implementing the cryptographic primitives and for communicating through the MQTT server.

3 Task

Develop a chat application that is almost compatible with Whatsapp or Signal by implementing double ratchet as outlined above. You program must read input from the console and present the received and sent messages on screen, correctly decrypted.

There exist several open implementations of Double Ratchet on the Internet. While you can freely get inspiration from these, it's mandatory that you provide **your own implementation**, so as to prove your comprehension of the algorithm.