Secure Messaging with Double Ratchet
A requirement for the Signal Protocol

Avery Keuben (CPSC)
Joshua Liu (CPSC)
Aritra DE (MATH)

March 14, 2025

1 Overview

2 AES-256

2.1 Implementation

2.2 Mode Of Operation

2.3 AEAD

3 SHA-256

3.1 Implementation

3.2 HMAC SHA-256

3.2.1 Use as a KDF

3.3 HKDF

4 Double Ratchet

4.1 Implementation

4.2 Effectiveness

4.2.1 Forward Secrecy

Def: Output keys from the past appear random to an adversary who learns the KDF key at some point in time.

4.2.2 Break-in Recovery

Def: Future output keys appear random to an adversary who learns the KDF key at some point in time, provided that future inputs have added sufficient entropy.

5 X3DH - Triple-extended Diffie-Hellman

5.1 Implementation

5.2 Effectiveness