

Double Ratchet Protocol

- The root key k_{root} **does not encrypt messages**
 - Use **for deriving a series of keys** $k_1, k_2, k_3 \dots$ that will be used to encrypt (send) and decrypt (receive) each message m_1, m_2, m_3
- ➔ **Double Ratchet Key Derivation Protocol**
(more details in bonus challenge)

Conclusion