P-4

Group: 7, Members: Peter Gifford, Kyle Brekke, Ren Wall, Madison Hanson

Due: November 18, 2019

1 Algorithm Description - Double Ratchet Algorithm

The double ratchet algorithm is creating a very secure way for two people to exchange messages through the use of a shared secret key. With many encryption algorithms once the key is discovered the encryption is compromised because a third party can decrypt all the messages being sent. The double ratchet algorithm solves this problem by consistently generating new keys. Every message generates a new one of these keys which can be used to decrypt the message meaning that having any single key will only give access to a singular message and cannot be used to retrieve any other keys making this extremely secure.

Citation

"The Double Ratchet Algorithm." RSS, https://signal.org/dogs/specifications/doubleratchet/