P-4

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

Due: November 18, 2019

1   Algorithm Description - Double Ratchet Algorithm

In communications sometimes it is useful to have that conversation be encrypted, whether it is employees communicating with each other, a whistleblower providing information about something, or people who are concerned about their privacy. The double ratchet algorithm is an algorithm that is used by the encrypted messaging platform Signal and is the focus of our project. The double ratchet algorithm creates a 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 that can not be derived from prior 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 of the other keys making this more secure than algorithms that just use one secret key throughout the conversation.

Citation

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