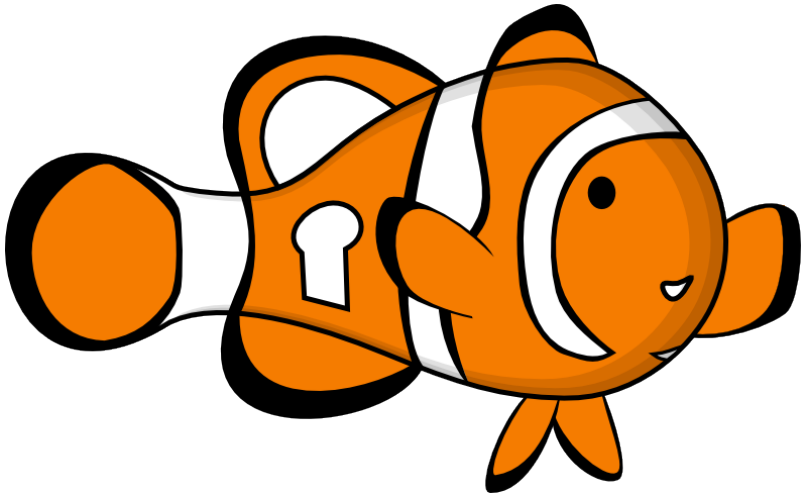
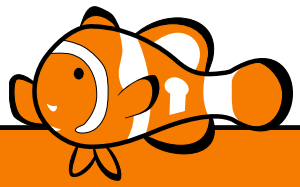
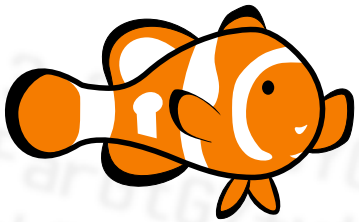
OMEMO

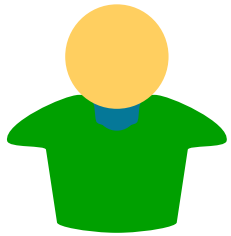
encryption made usable

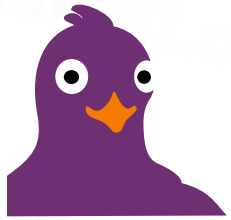


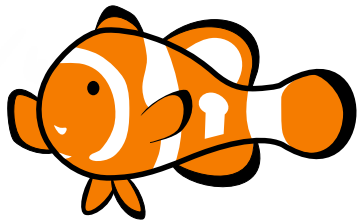
every hero needs an origin story

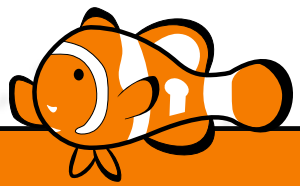


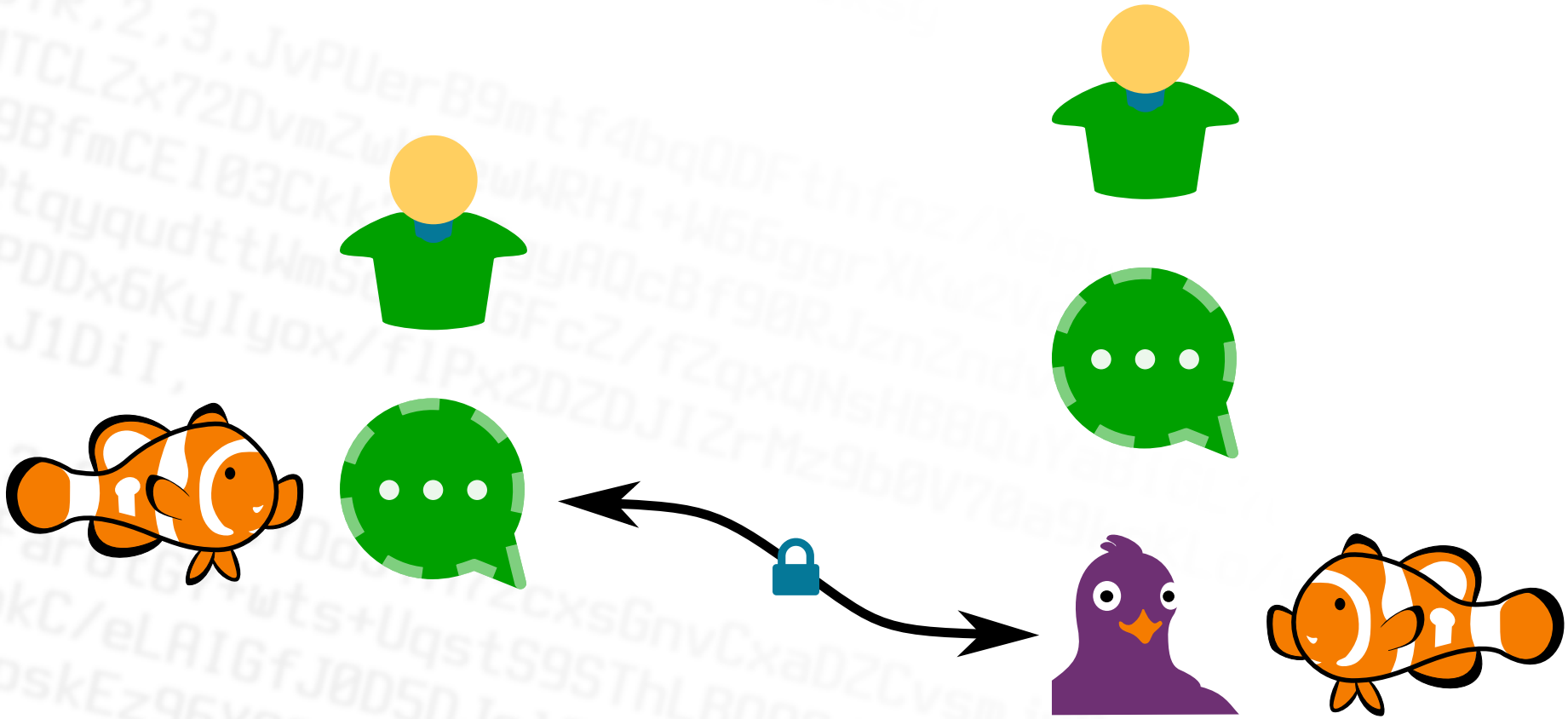


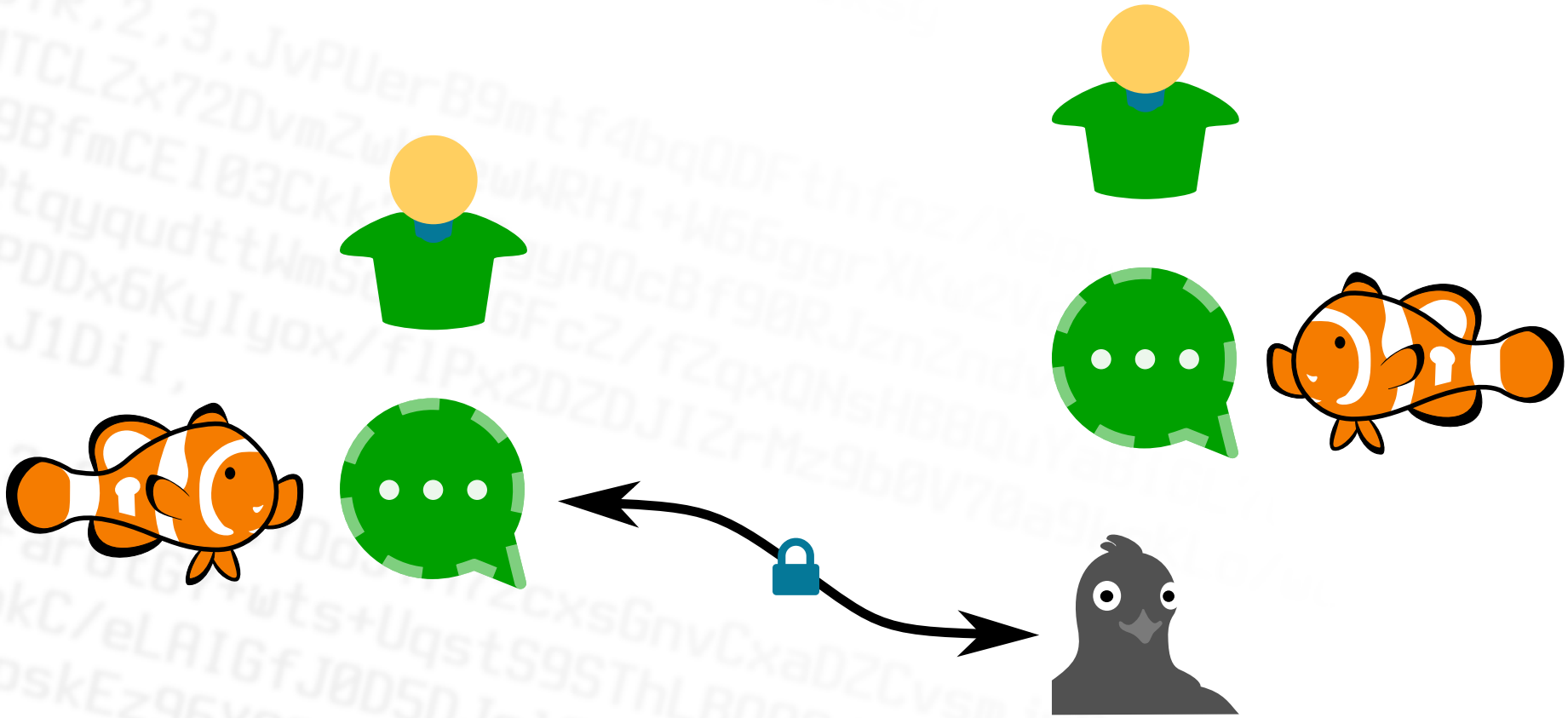


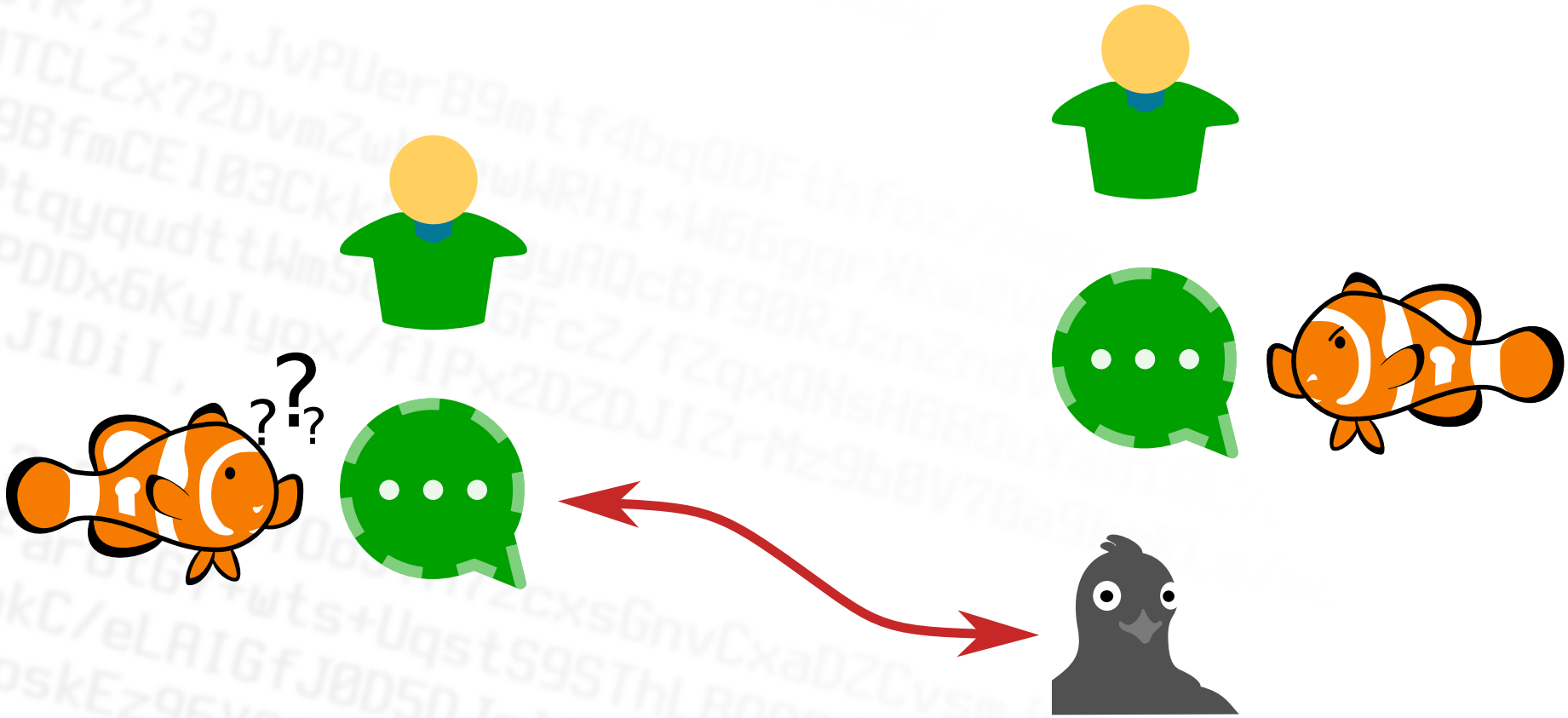




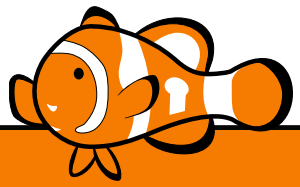








Google
SUMMER
of
CODE
2015

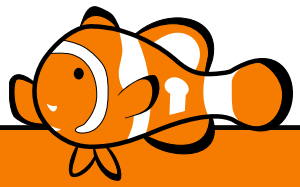


easy
to use

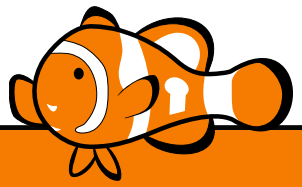
history
synchronization

forward
secrecy

reach offline
contacts

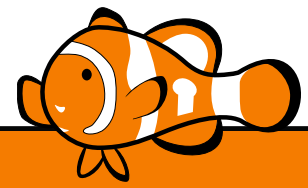


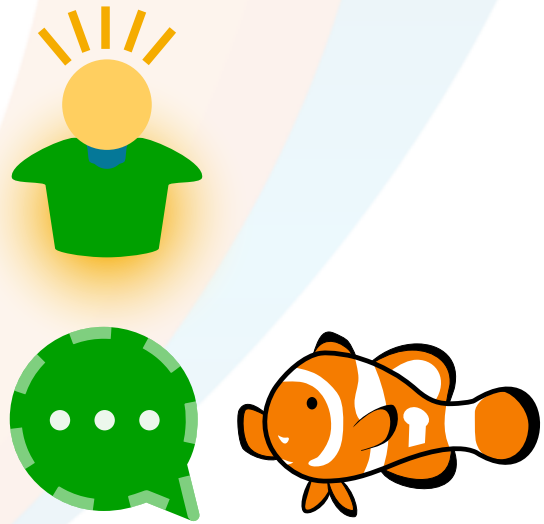
it should just work™

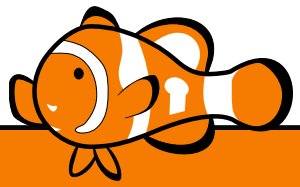


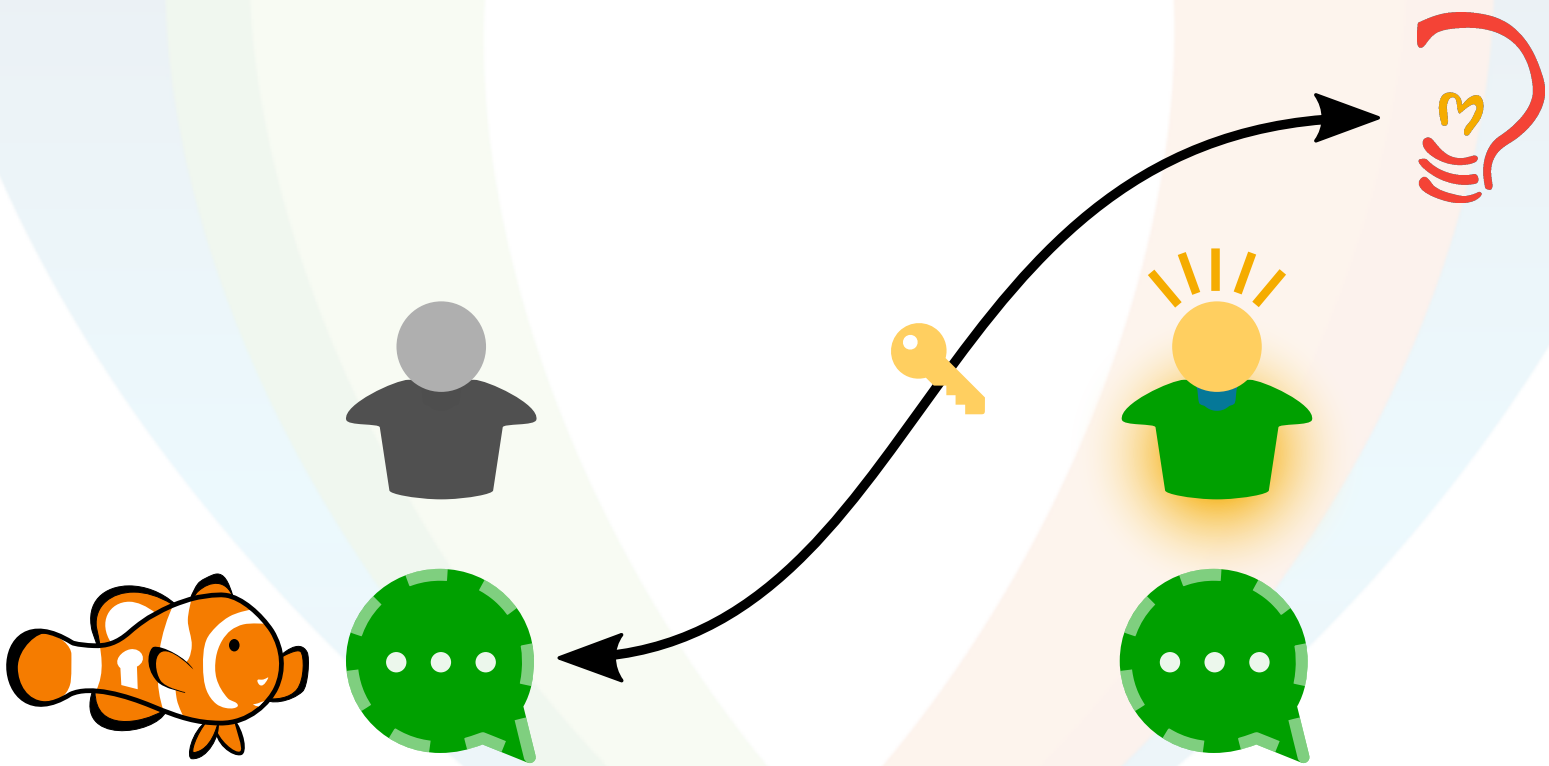
“crypto is hard”

– *Sun Tzu*

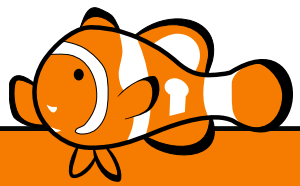


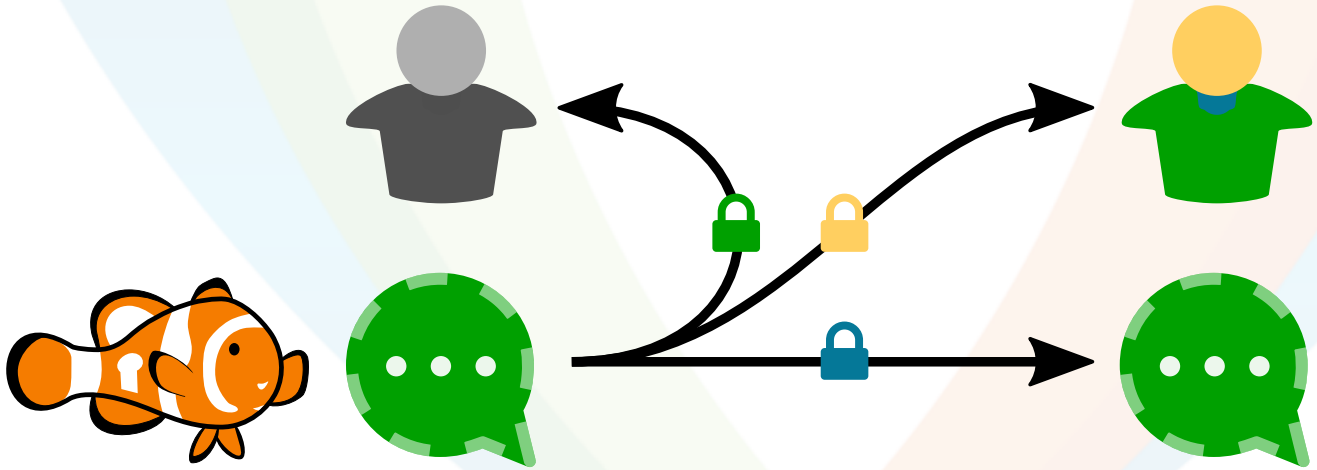




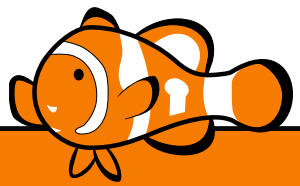


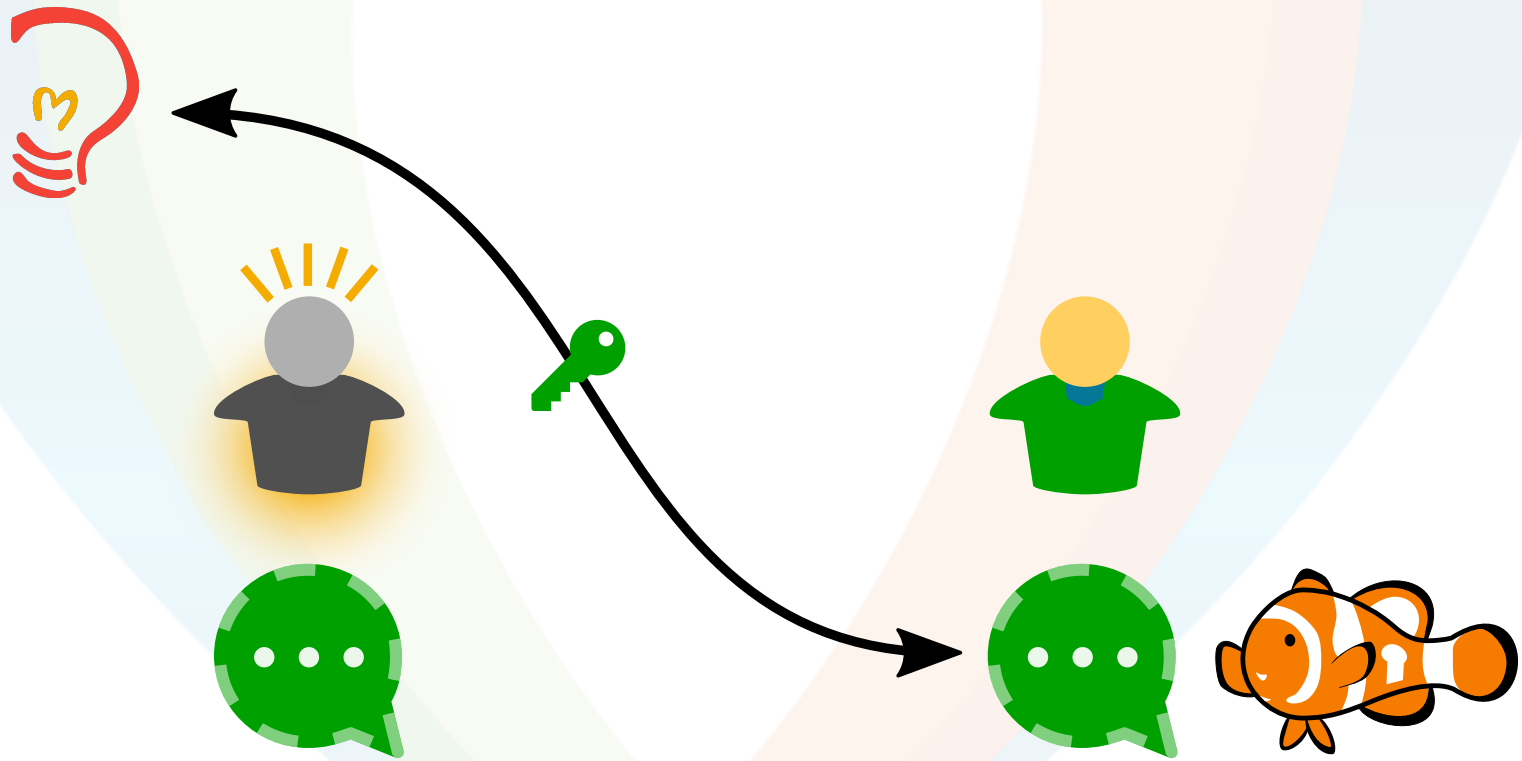
fetch PreKey from server



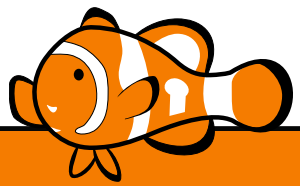


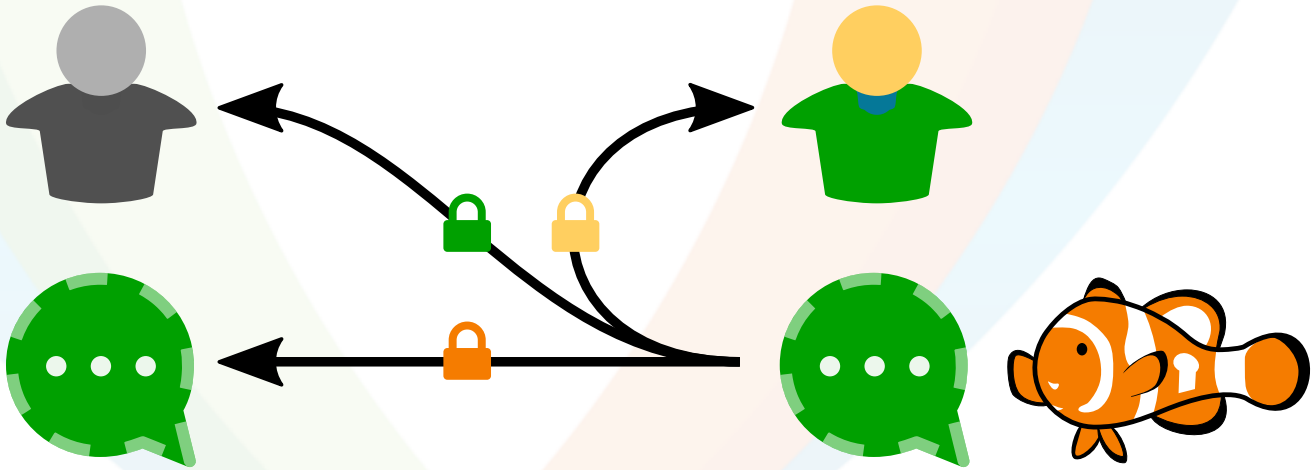
one message, three headers



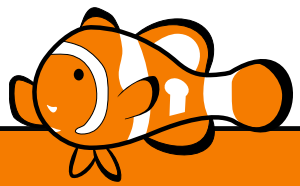


fetch PreKey from server





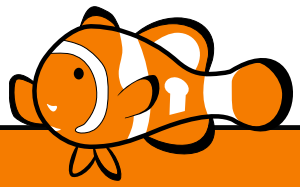
one message, three headers



Try it!

http://conversations.im/omemo

http://play.google.com/store/apps/details?id=eu.siacs.conversations

http://github.com/siacs/Conversations

http://github.com/kalkin/gajim-omemo