



Signal Protocol

Axolotl Ratchet



Pete Hegseth

TEAM UPDATE:

TIME NOW (1144et): Weather is FAVORABLE. Just CONFIRMED w/ CENTCOM we are a GO for mission launch.

1215et: F-18s LAUNCH (1st strike package)


1345: "Trigger Based" F-18 1st Strike Window Starts (Target Terrorist is @ his Known Location so SHOULD BE ON TIME) — also, Strike Drones Launch (MQ-9s)

1410: More F-18s LAUNCH (2nd strike package)

1415: Strike Drones on Target (THIS IS WHEN THE FIRST BOMBS WILL DEFINITELY DROP, pending earlier "Trigger Based" targets)

1536: F-18 2nd Strike Starts — also, first sea-based Tomahawks launched.



Moxie Marlinspike 

@moxie



There are so many great reasons to be on Signal.

Now including the opportunity for the vice president of the United States of America to randomly add you to a group chat for coordination of sensitive military operations.

Don't sleep on this opportunity...

9:36 PM · Mar 24, 2025 · **492.2K** Views



“In the U.S., downloads were up 45%”

“worldwide Signal downloads on iOS and Google Play were up 28%”

“in Yemen, they were up by 42%”



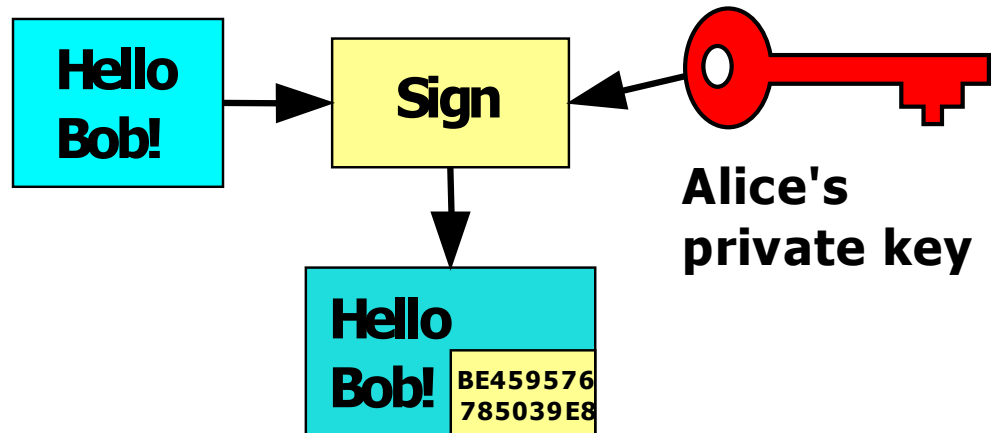
Alice

01101010
11011000
00110101
**Large
random
number**

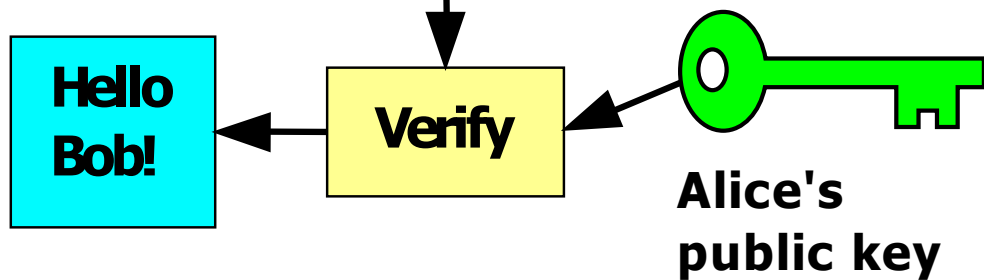
**Key
generation
program**



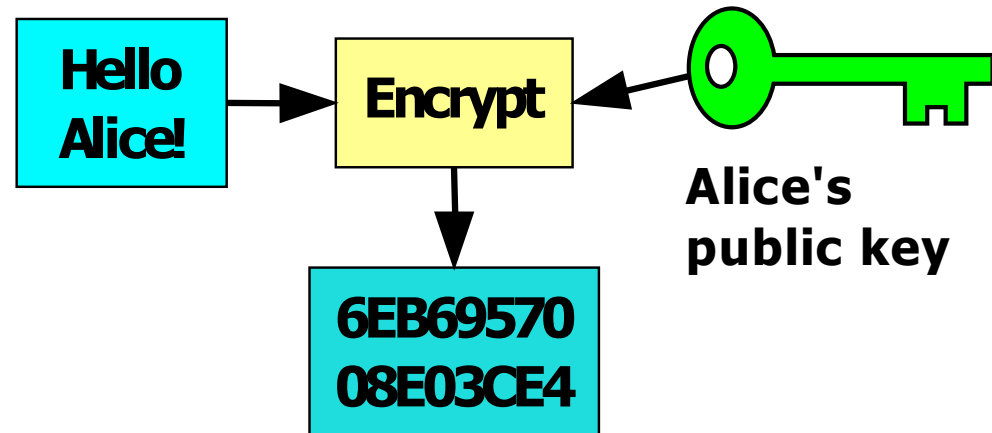
Alice



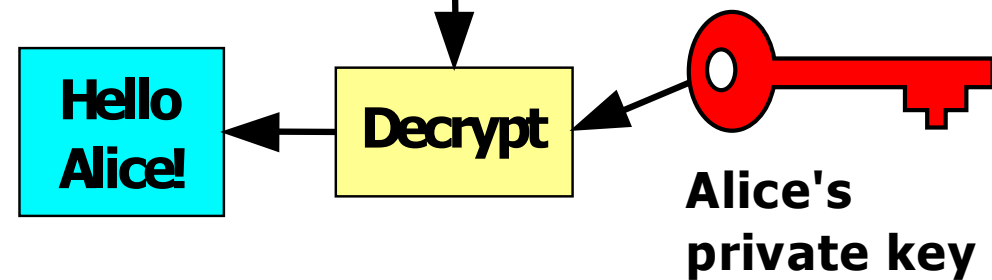
Bob

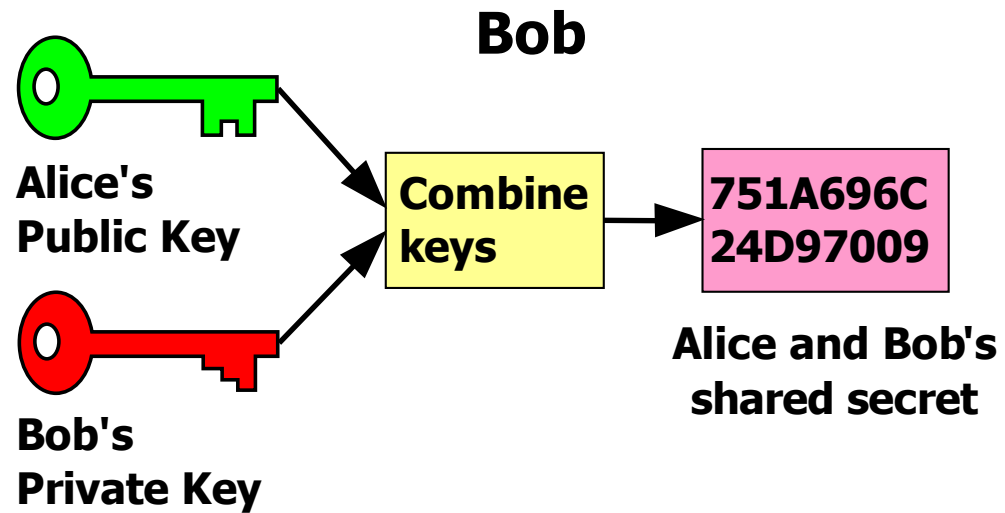
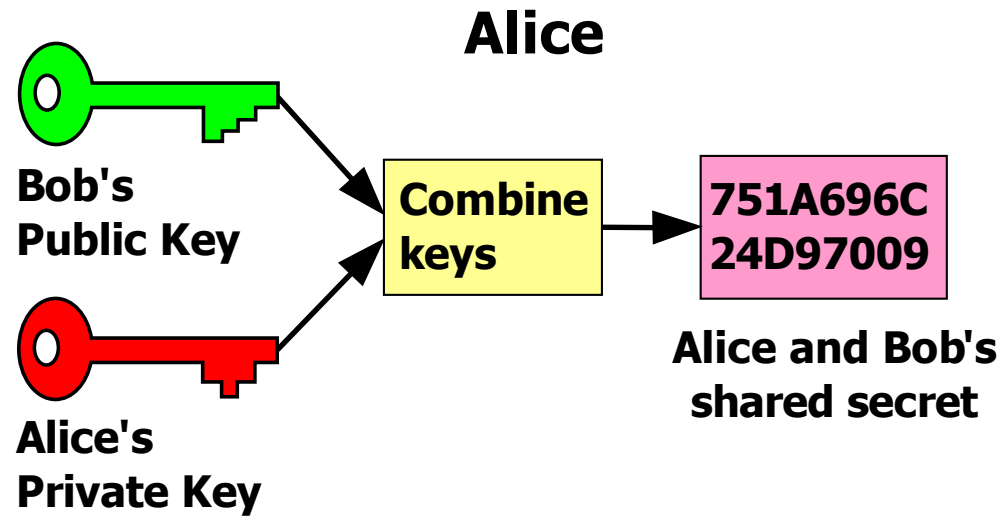


Bob

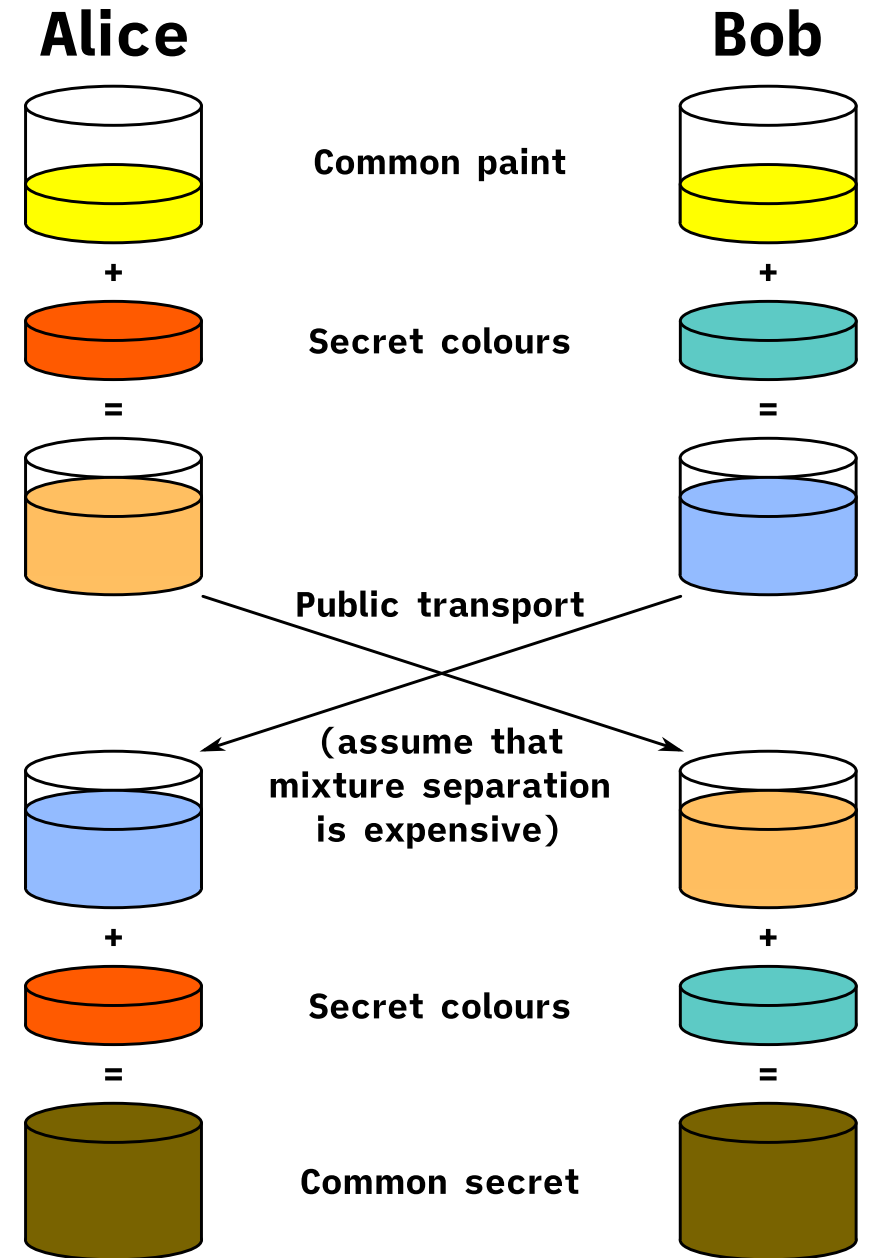


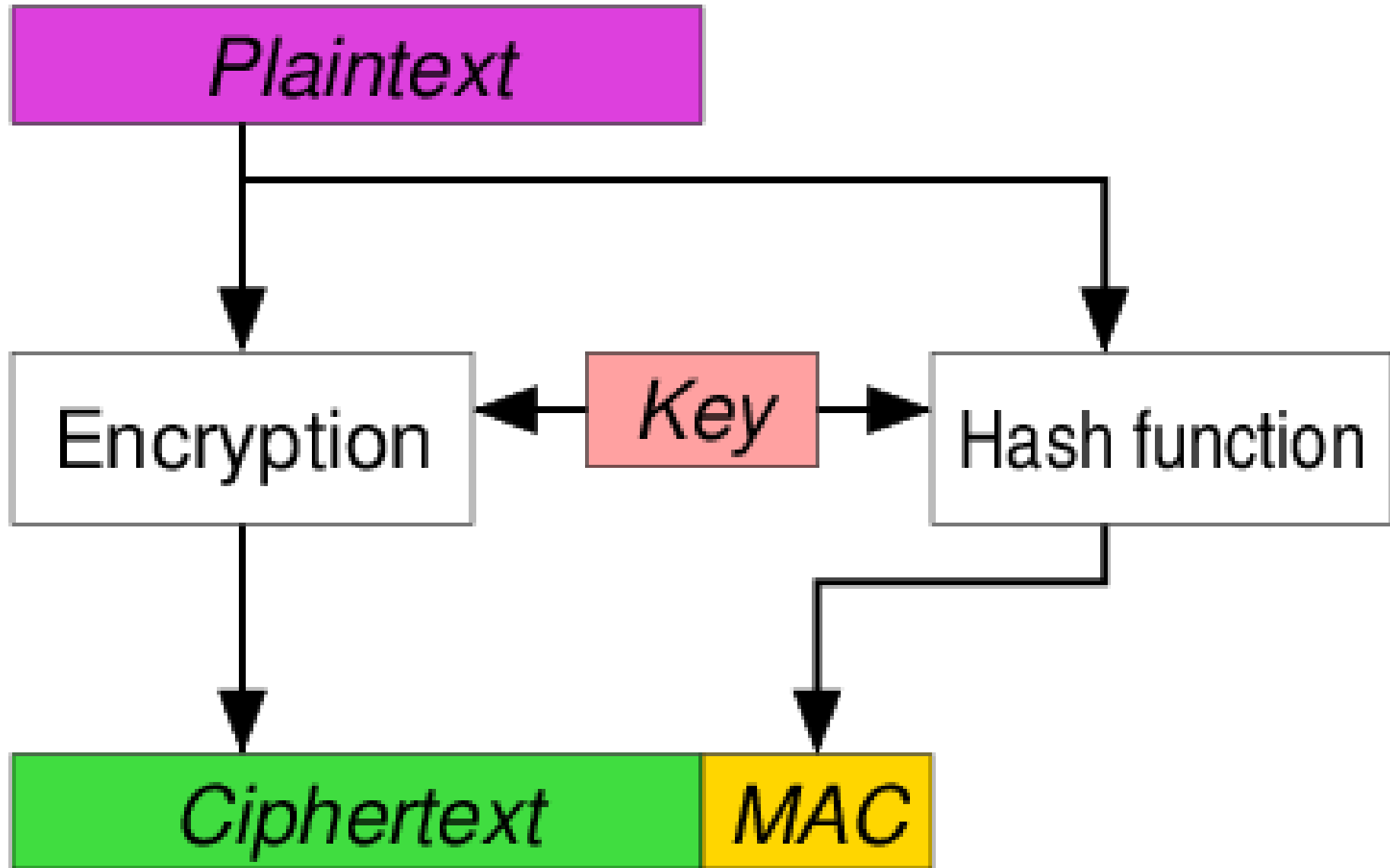
Alice





Diffie-Hellman Key Exchange





(No Model.)

A. E. OSBORN.
RATCHET WRENCH.

No. 295,797.

Patented Mar. 25, 1884.

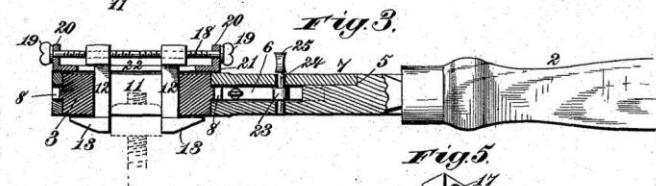
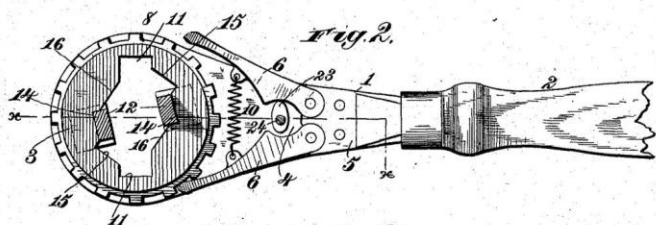
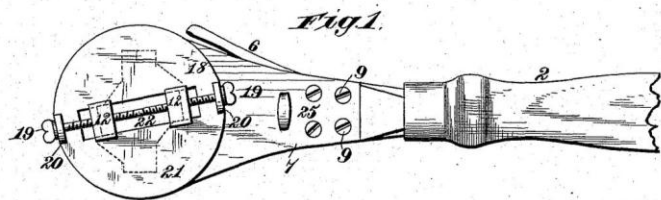


Fig. 4.

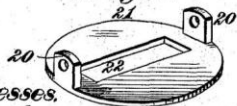
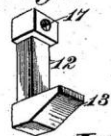


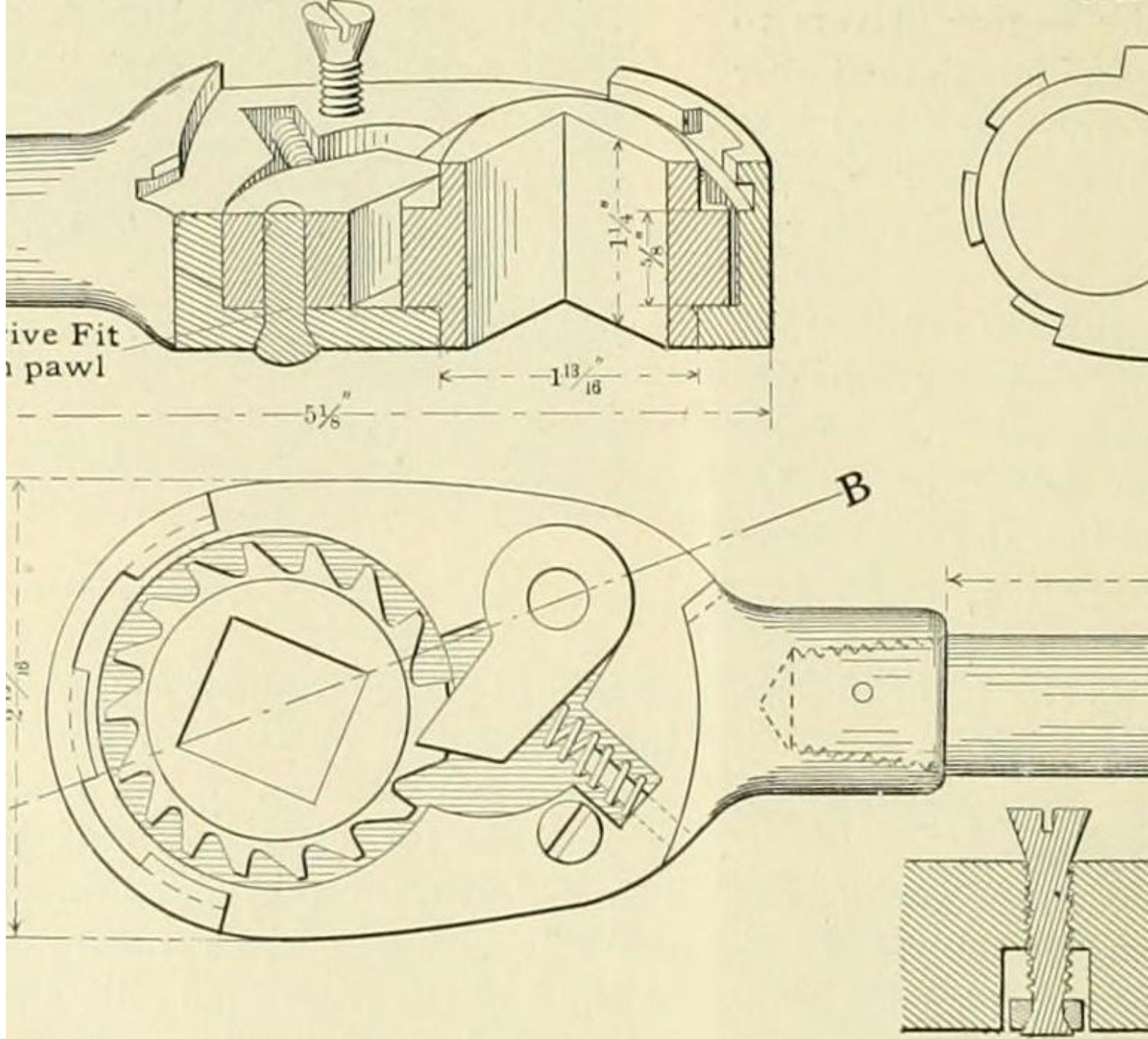
Fig. 5.

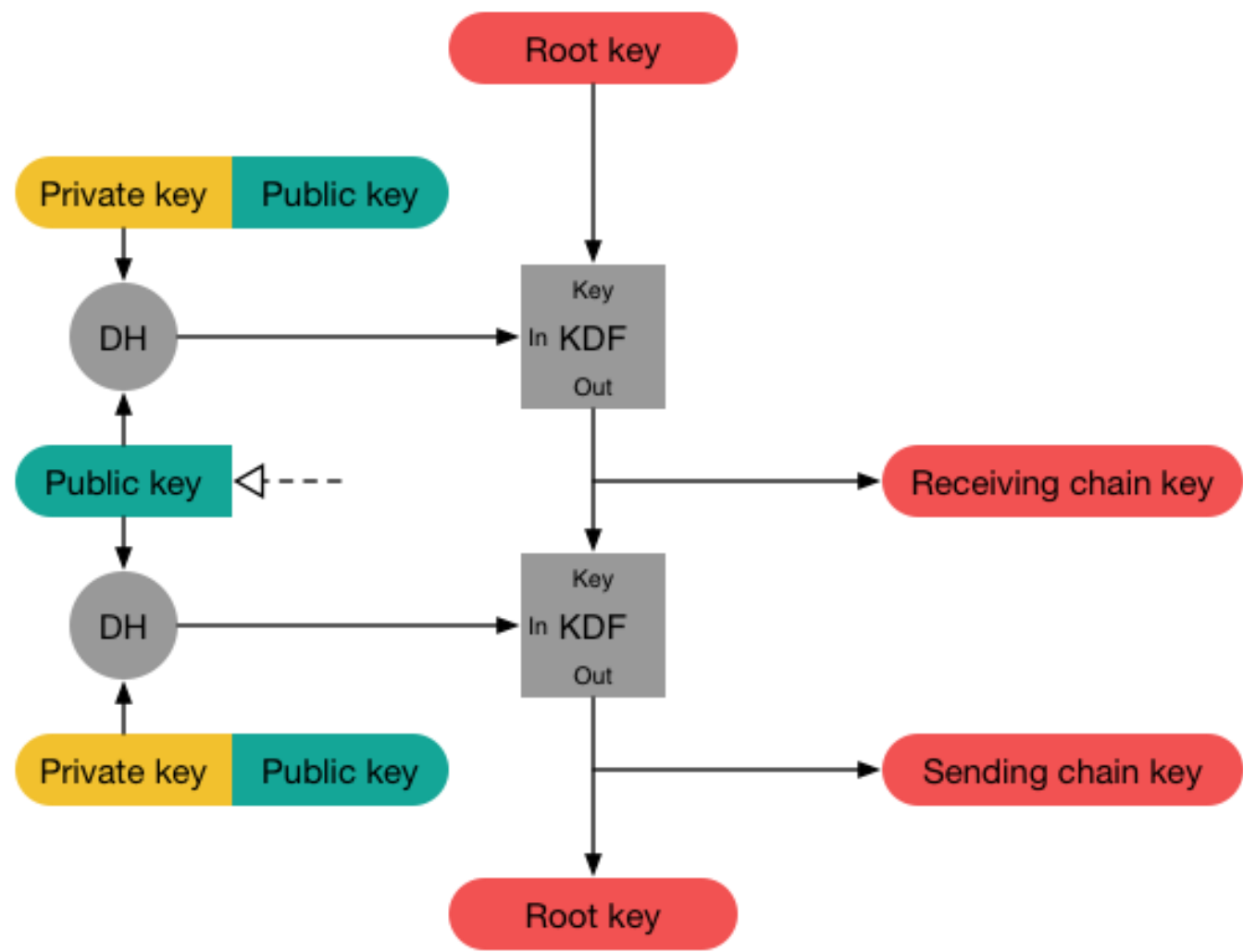


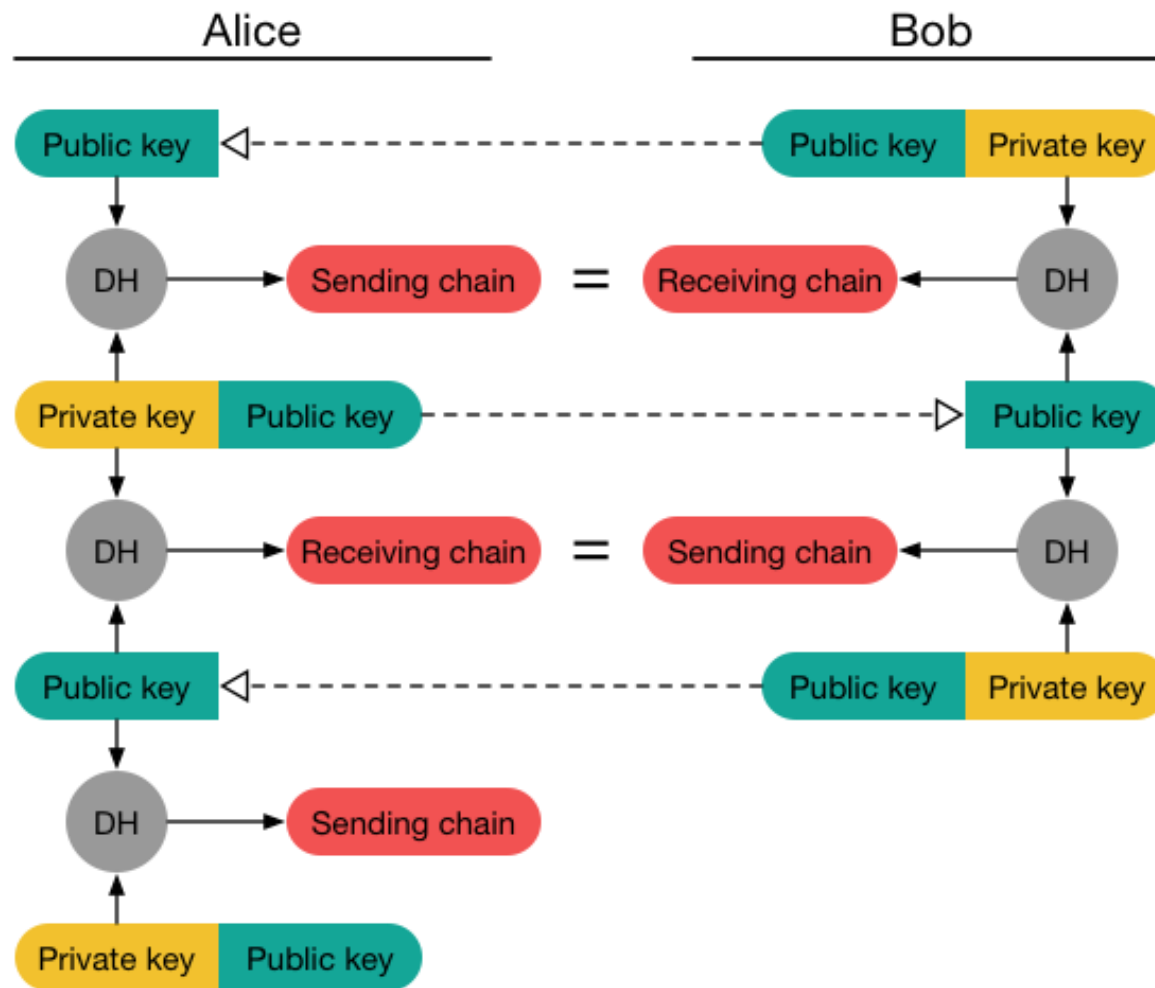
Witnesses:
Robert Smith,
Chas. H. Jones

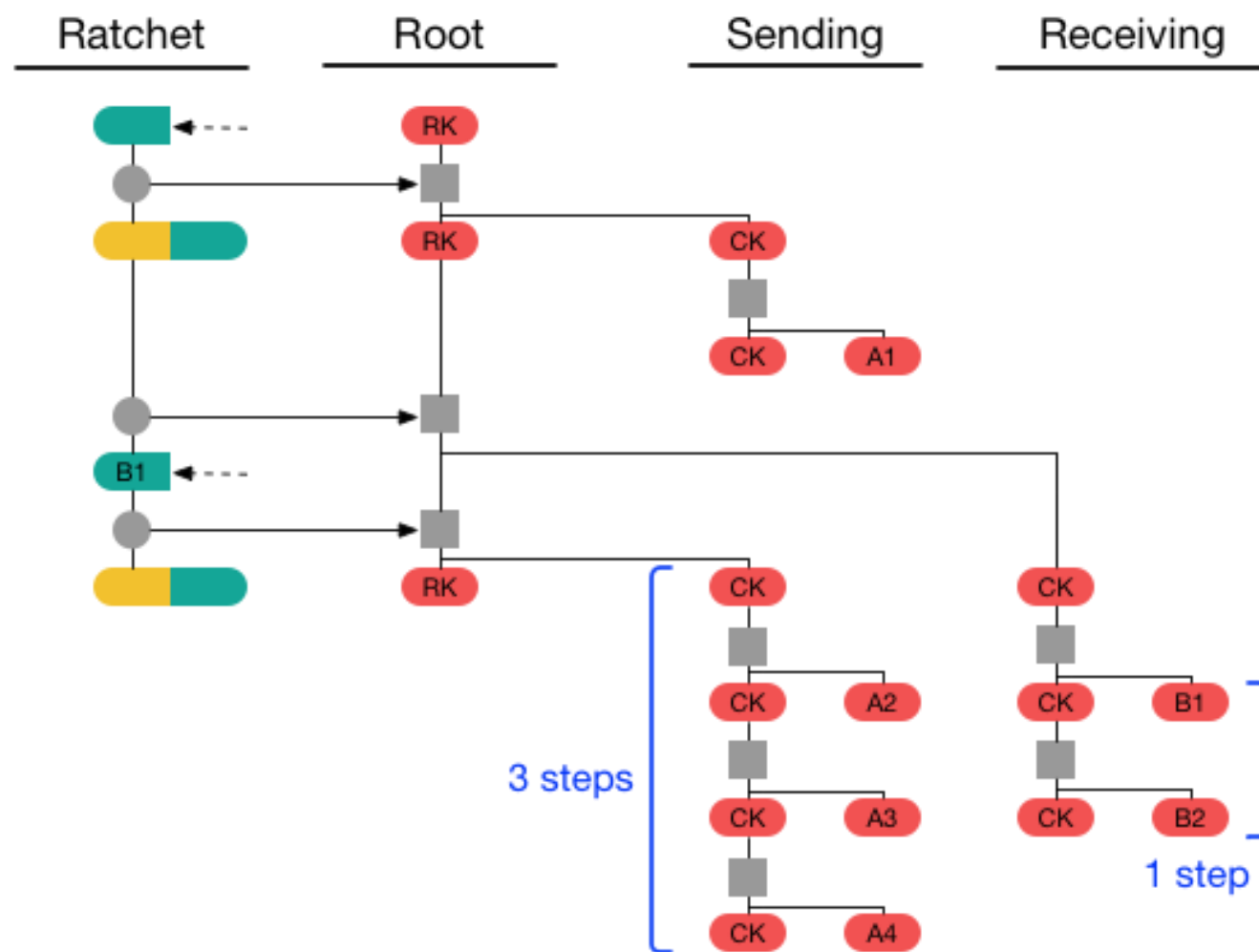
Inventor:
Adelbert E. Osborn
By James L. Norris
Att'y.

H. PETERS, Photo-Lithographer, Washington, D. C.









ephemeral

adjective

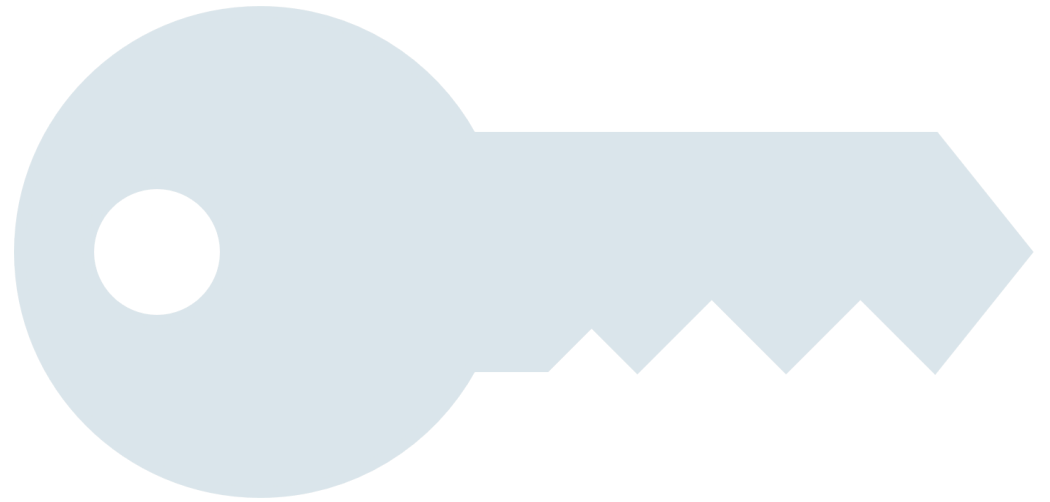
lasting a very short time
lasting one day only

Sesame



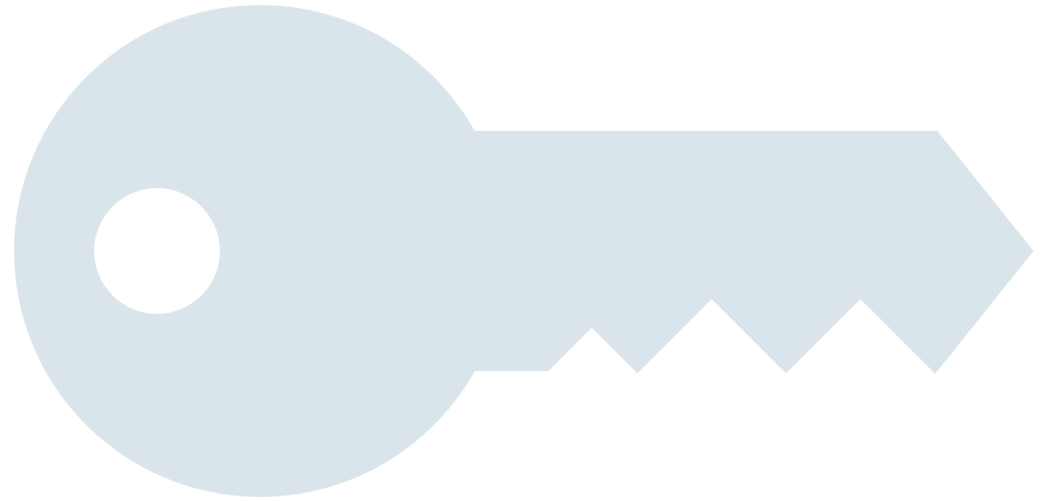
Bob's side

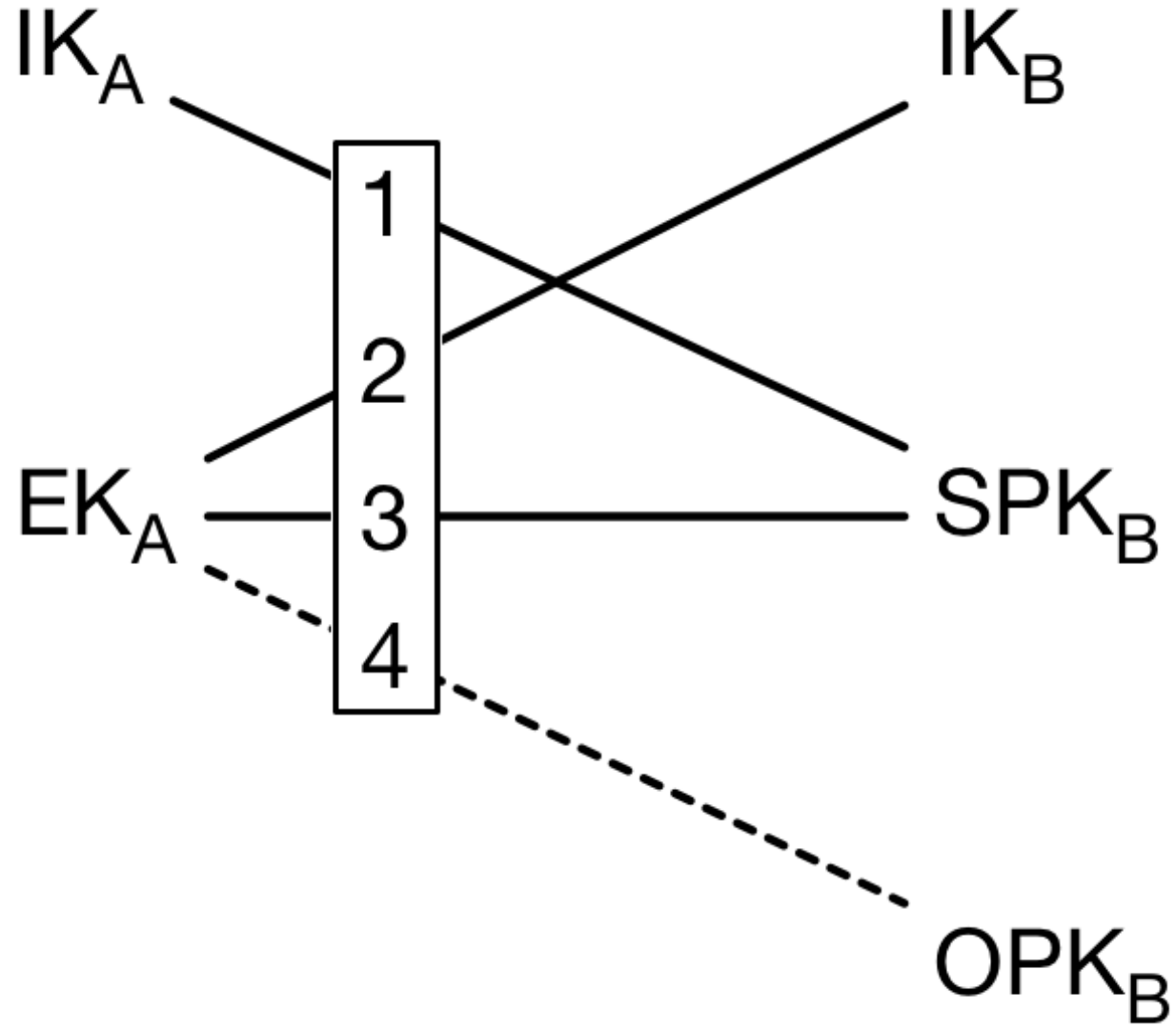
- Public part of identity key
- Signed pre-key
- One-time pre-key 1
- One-time pre-key 2
- One-time pre-key 3
- ...



Alice's side

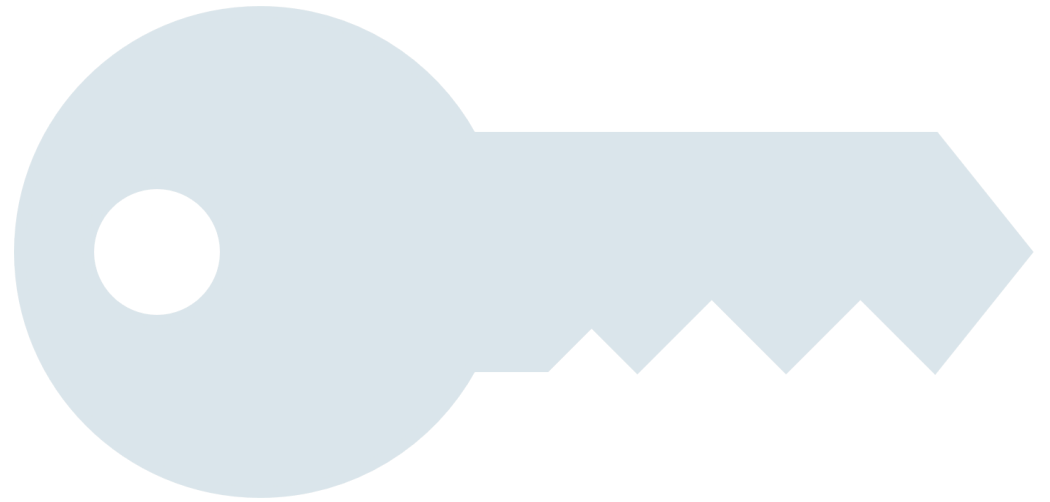
- Takes her private identity key
- Creates ephemeral key
- Asks server for a pre-key package for Bob





Alice sends to Bob

- Public ephemeral key
- Public identity key
- Identifier for Bob's one-time pre-key
- Initial cipher text



Signal Documentation: <https://signal.org/docs/>

Signal Foundation GitHub: <https://github.com/signalapp>

Double Ratchet Messaging Encryption (Computerphile):
<https://youtu.be/9sO2qdTci-s>

Signal Messaging Protocol (Computerphile):
<https://youtu.be/DXv1boalsDI>

