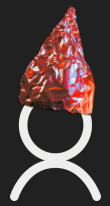
Slides with notes/references:
https://docs.google.com/presentation/d/13kL9VlYb4149weCgwV5NiTw2xlQwyTcVjo_w2Zwuucs/edit?usp=sharing

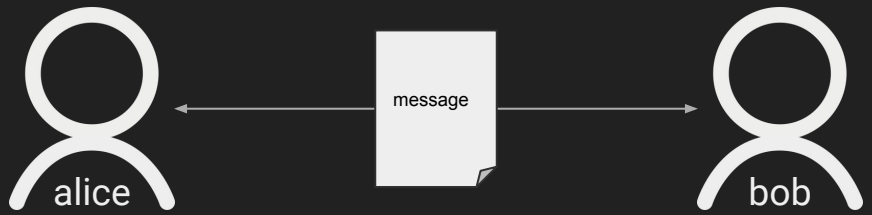
Secure Messaging Deep Dive

Stian Kristoffersen @ oslohack:22



Background & Concepts

Scope: text messages



Messaging Service	Number of users (approx)
WhatsApp (Meta)	2 billion
WeChat	1.3 billion
iMessage (Apple)	1.3 billion
Messenger (Meta)	1 billion
Telegram	700 million
Tencent QQ	560 million
Snapchat	560 million
Google Chat	500 million
…	
Signal	40 million

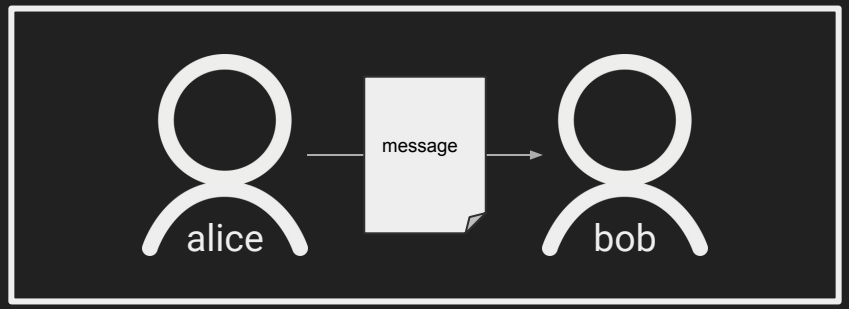
Disclaimers and security levels

Baseline for private messaging in 2022

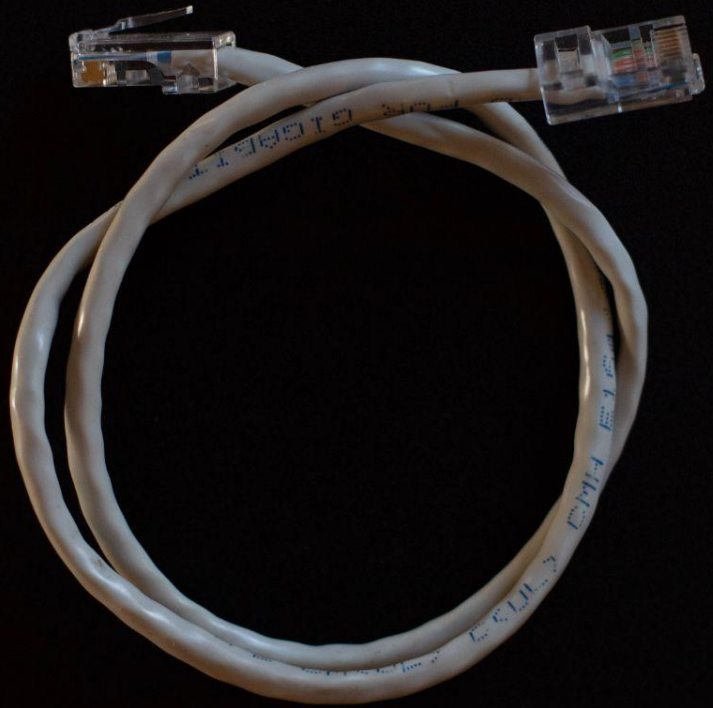
Beyond the baseline

Ridiculous territory

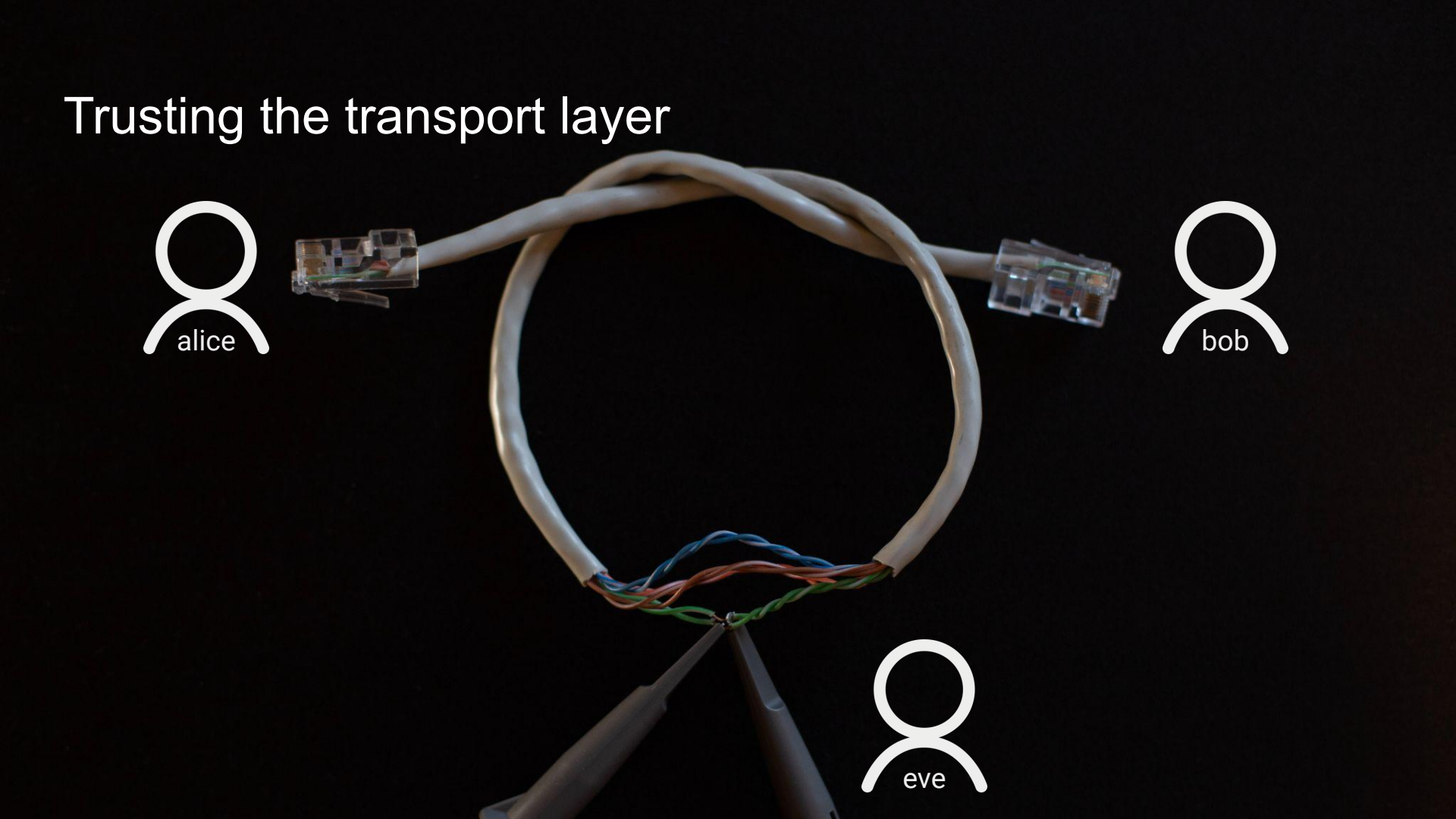
Concept: Secure Messaging



Trusting the transport layer



Trusting the transport layer



Concept: Secure Messaging

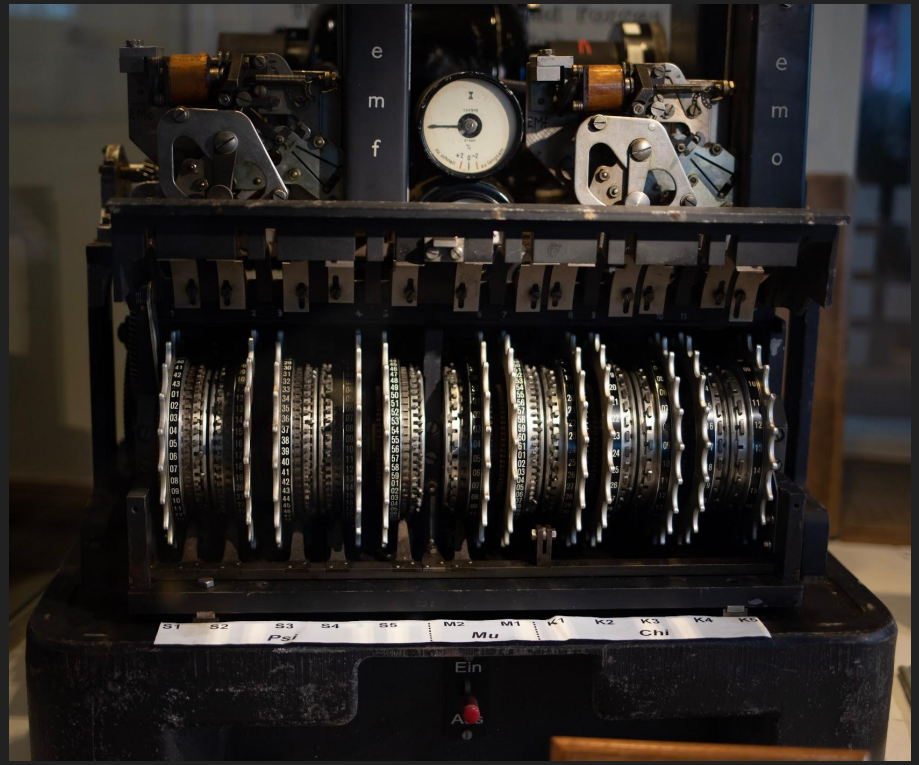
1. Confidentiality
2. Integrity

WWII: The Enigma and the Bombe

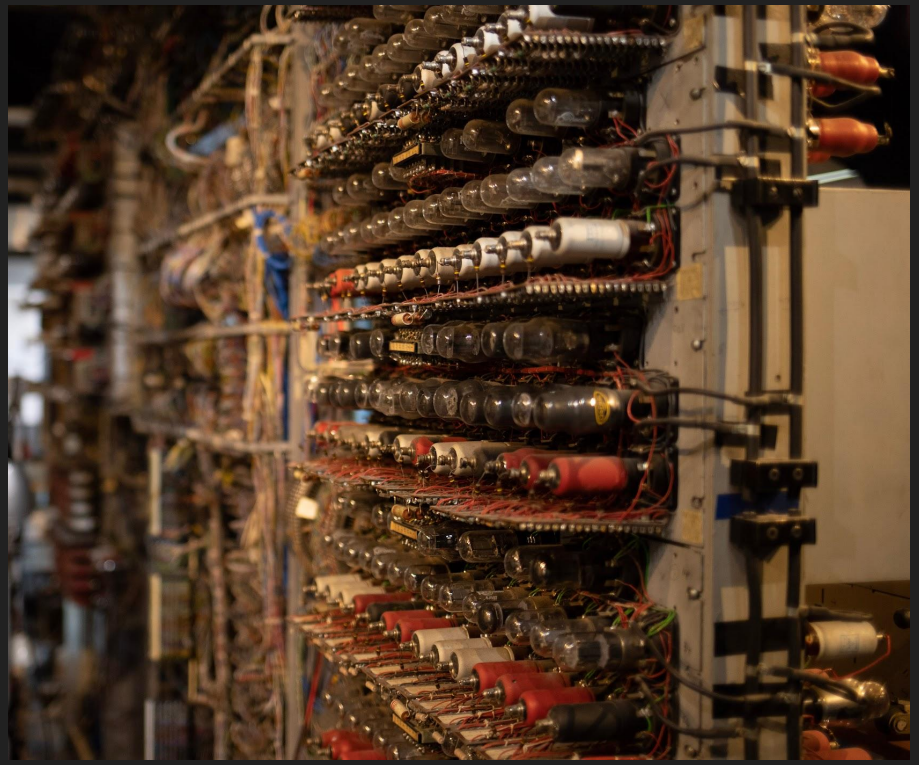
Enigma displayed at Bletchley Park, U.K.

Bombe replica displayed at the
National Museum of Computing, U.K.

WWII: The Lorenz and the Colossus



Lorenz cipher machine displayed at the National Museum of Computing, U.K.

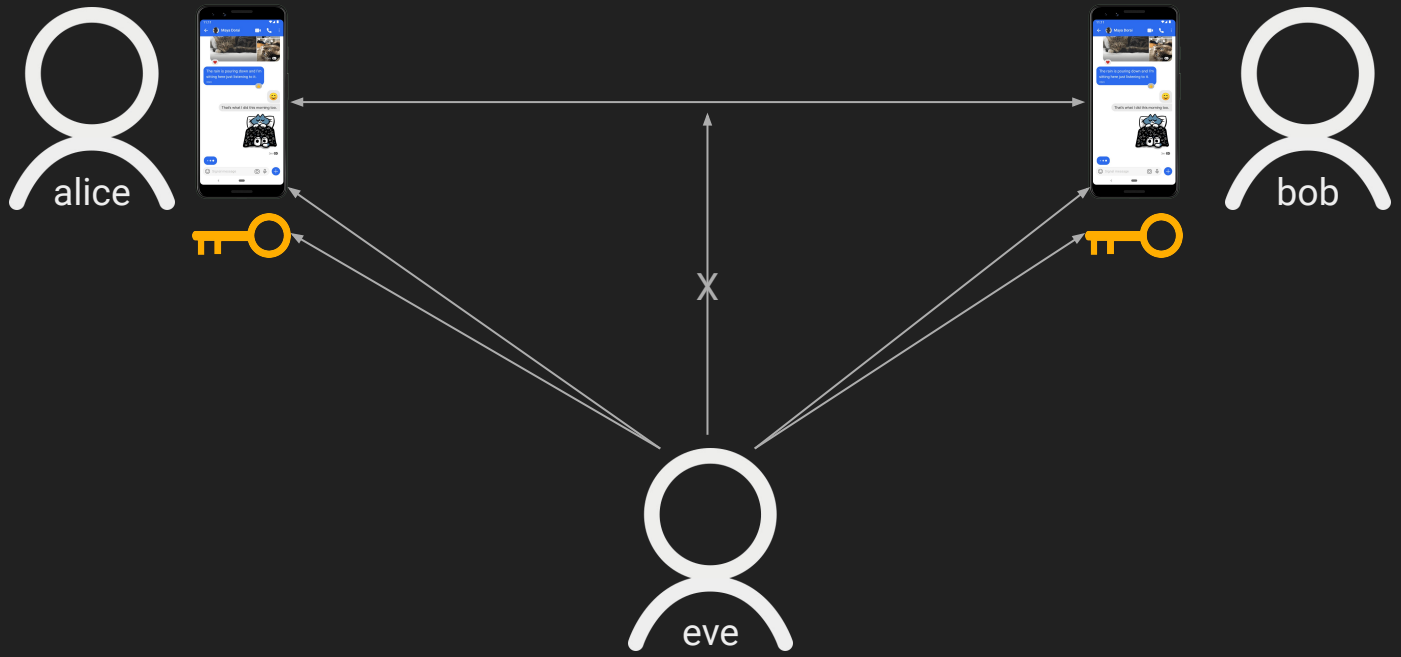


Colossus replica displayed at the National Museum of Computing, U.K.

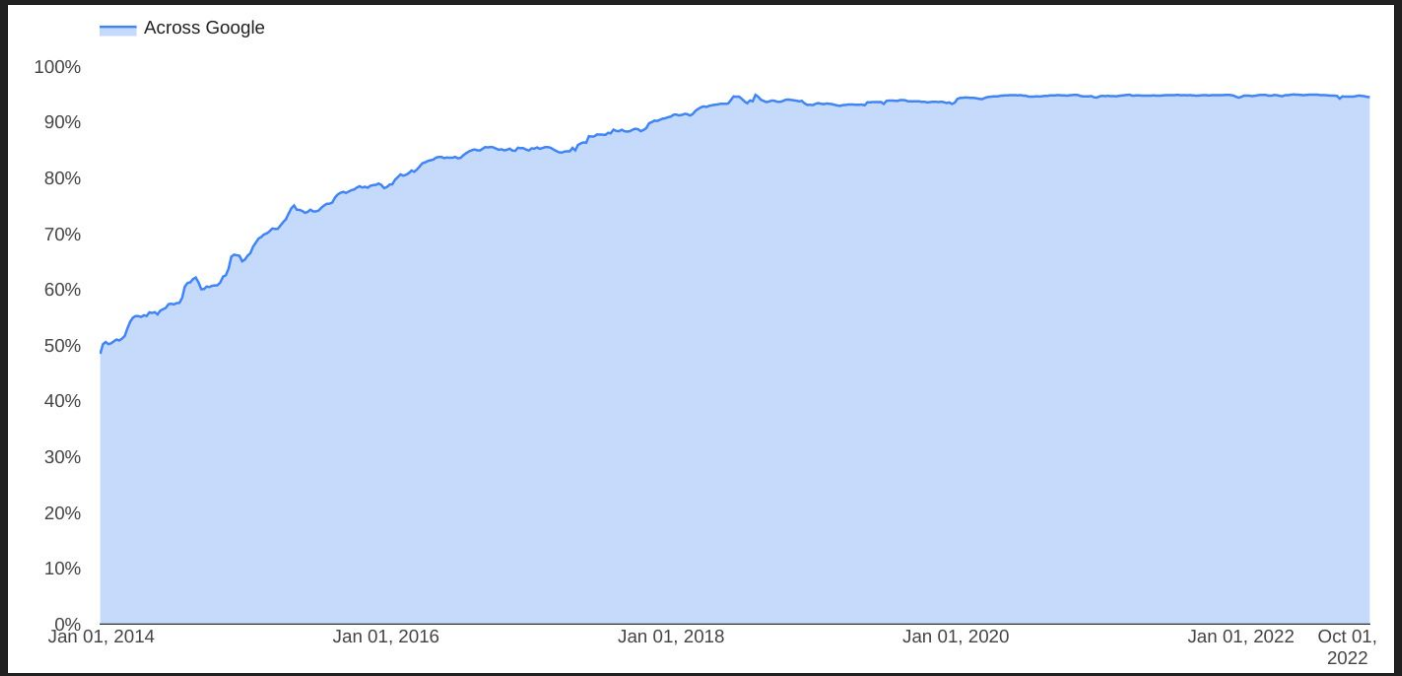
1970: Spy satellite without encryption

The Hubble Space Telescope, NASA

1990s: Crypto Wars

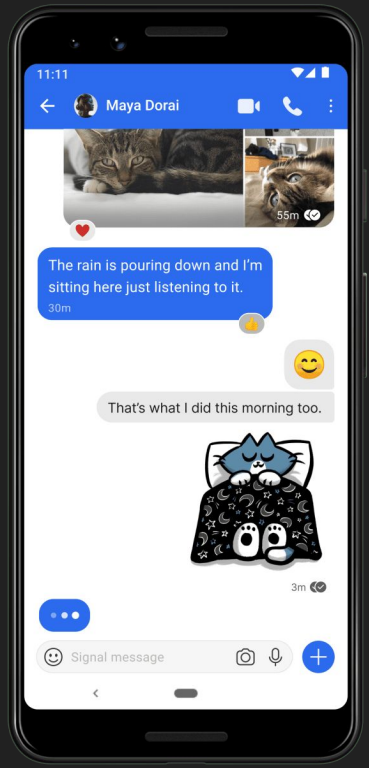


Post-Snowden leak: TLS Adoption



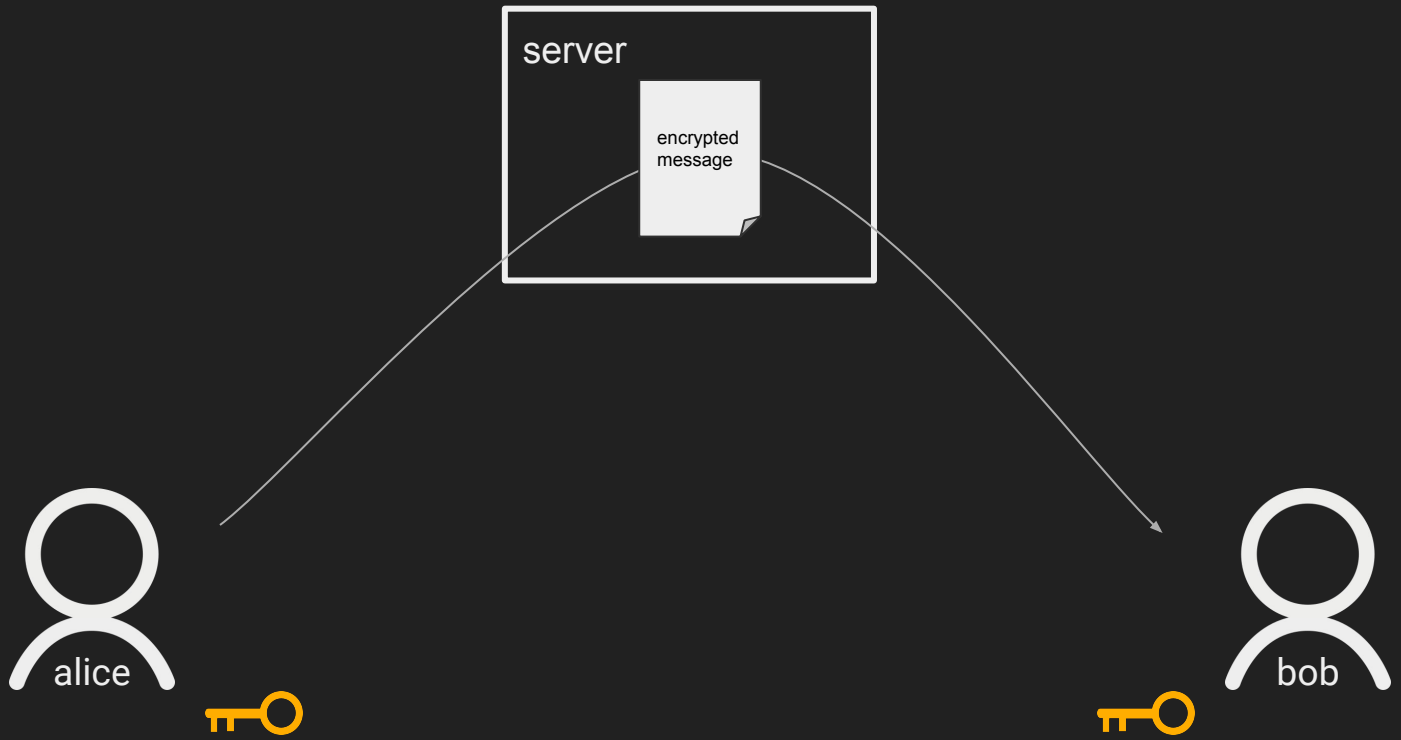
https://transparencyreport.google.com/https/overview

2022: Great* crypto in your pocket!

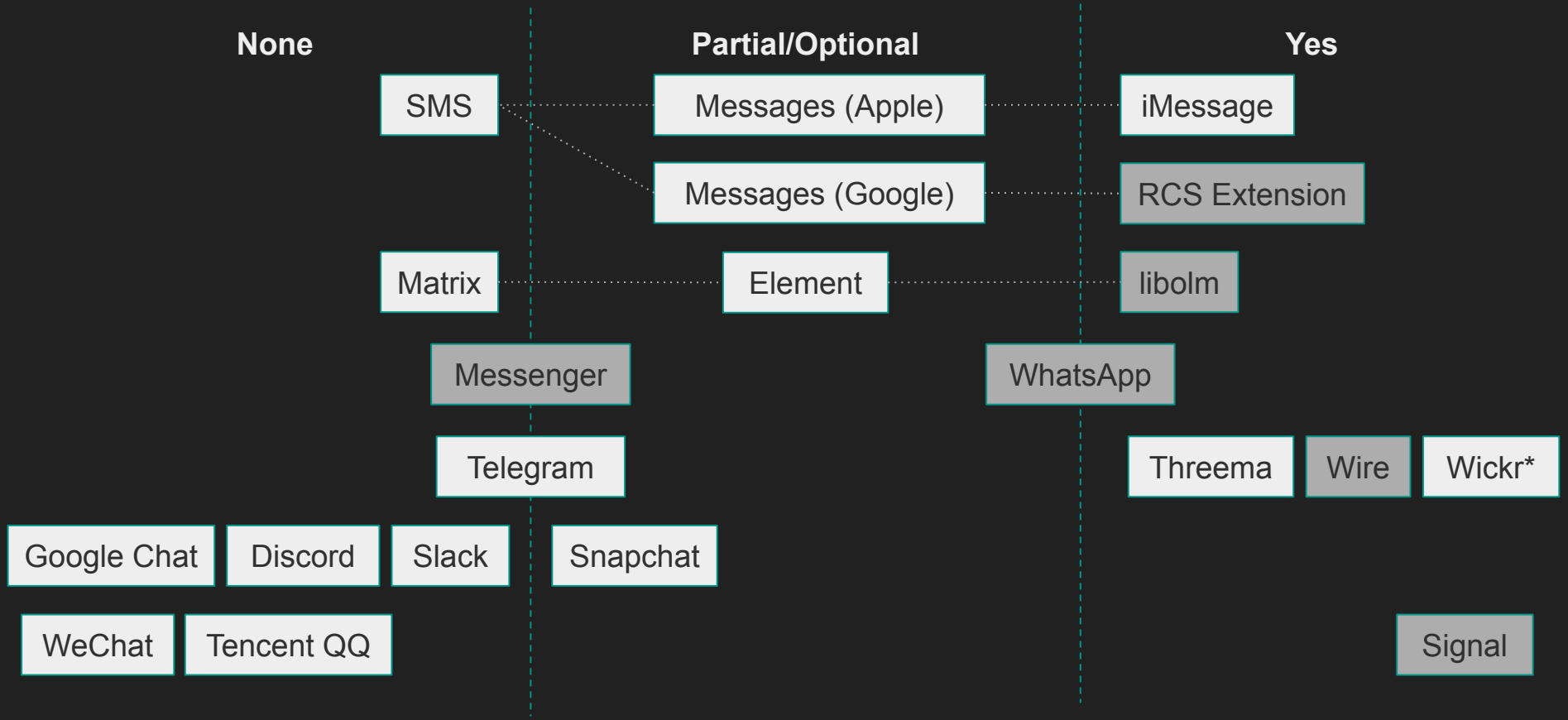


*caveats apply
also crypto: means cryptography

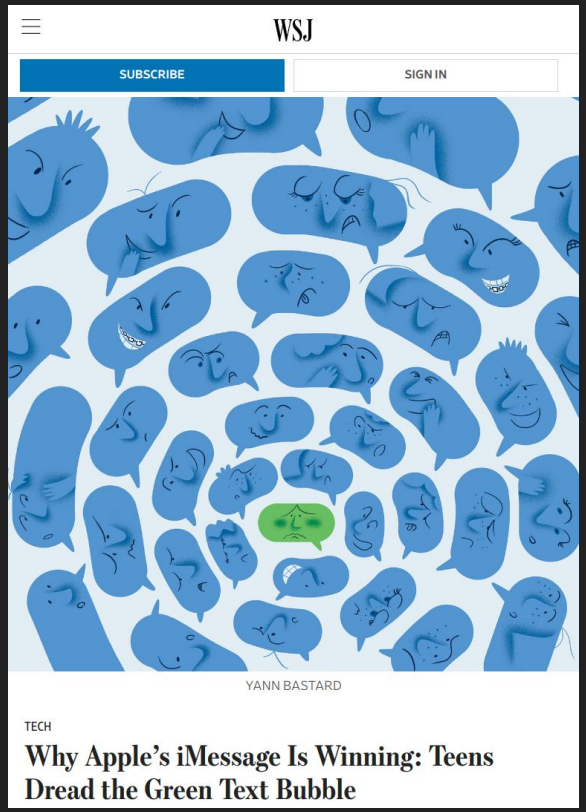
Concept: End-to-End Encryption

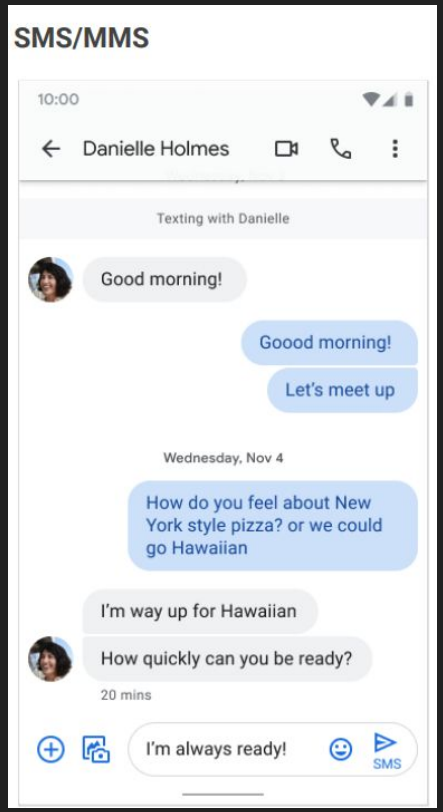


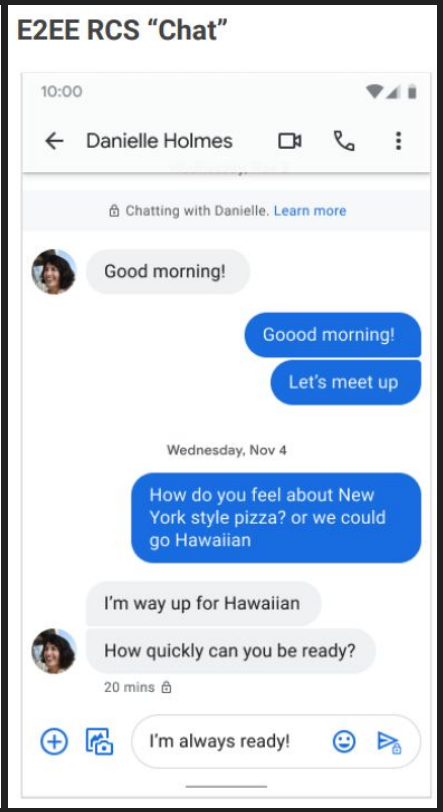
Comparison: End-to-End Encryption



SMS vs E2E for Apple and Google Messages

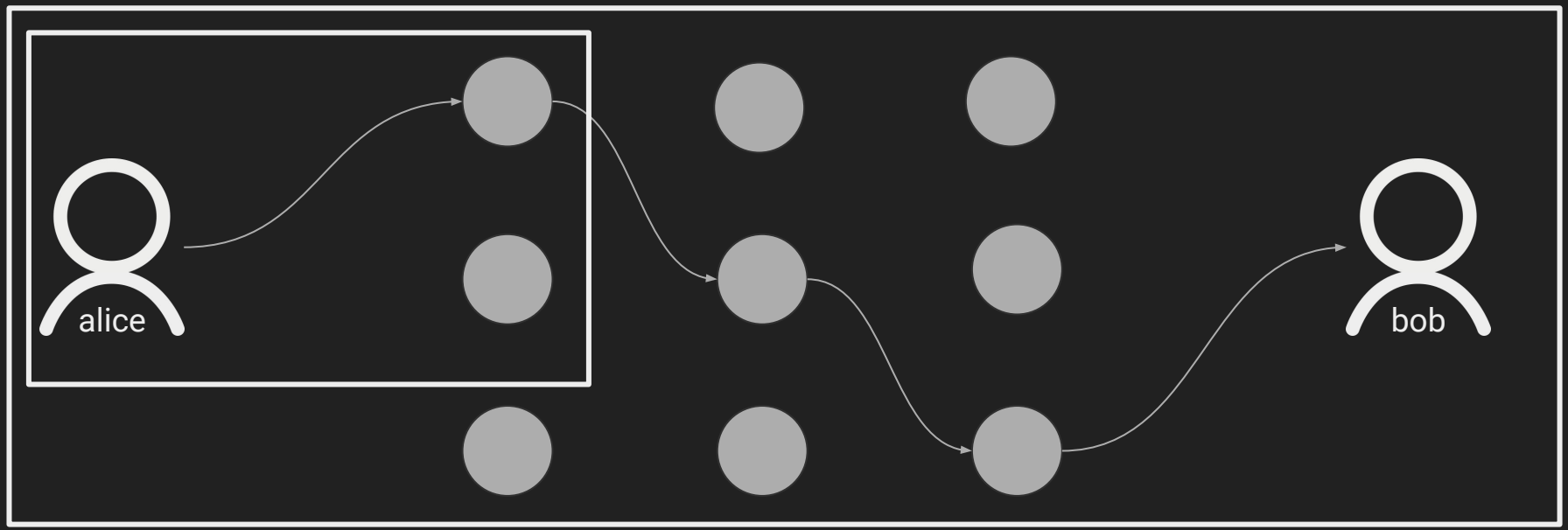






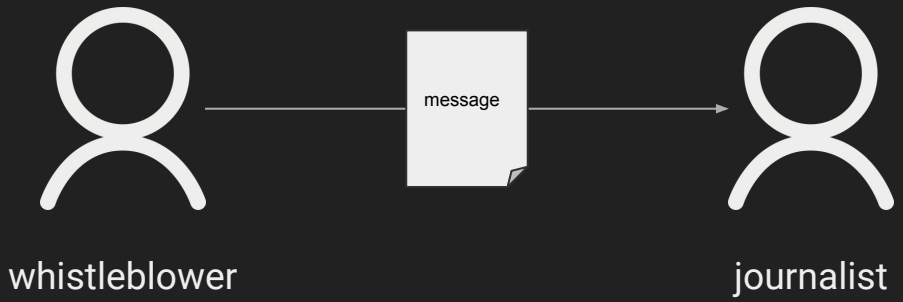
Concept: Metadata

Concept: Traffic Analysis



Traffic obfuscation, e.g. Tor

Concept: Deniability (repudiation)



Concept: Secure Messaging

1. Key Exchange
2. Encryption
3. Key Update
4. Metadata

Signal

Signal

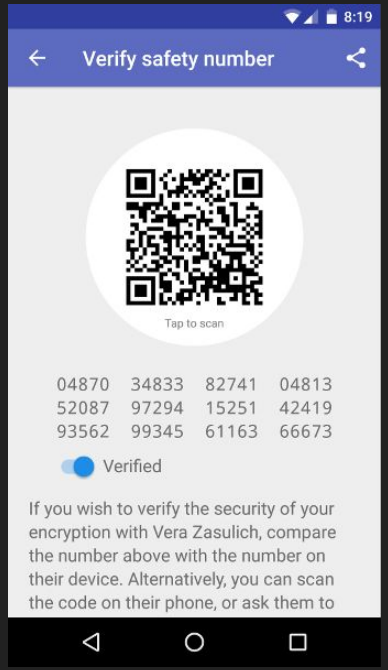
Key Exchange	X3DH
Cryptography	• Curve25519 • AES-256 • SHA-256
Key Update	Double Ratchet
Metadata	• Phone number • Last connection timestamp • Account creation timestamp

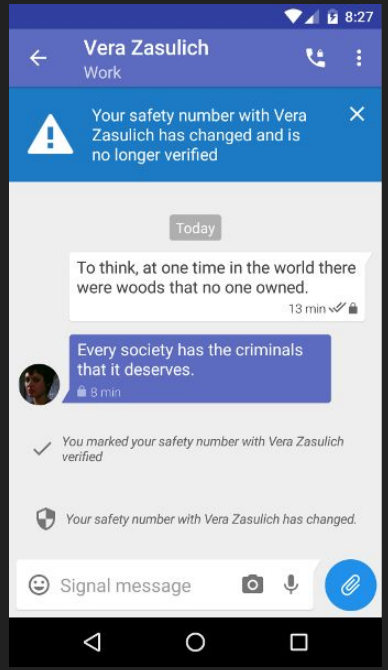
Key Exchange: X3DH

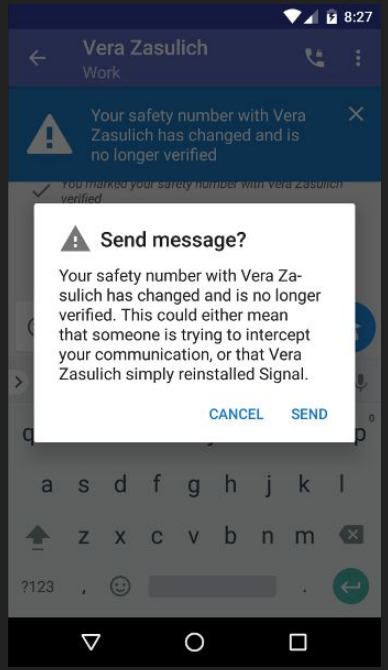
- Establish a shared secret key between two identities
- Extended Triple Diffie-Hellman
- Async
- Forward secrecy
- Deniability

https://signal.org/docs/specifications/x3dh/

Verify safety number in Signal





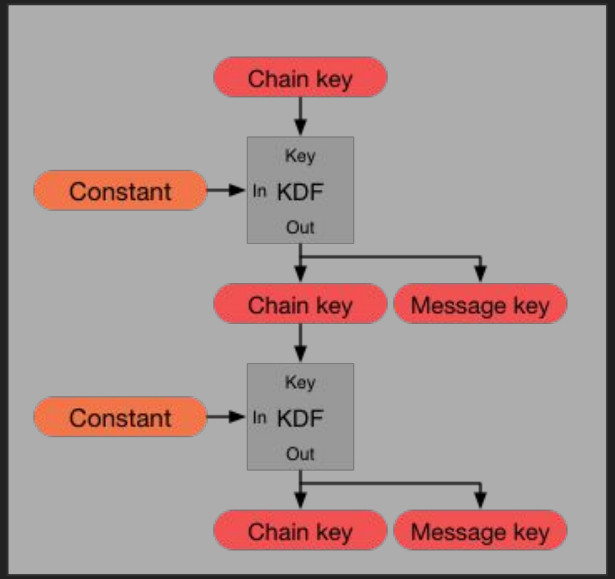


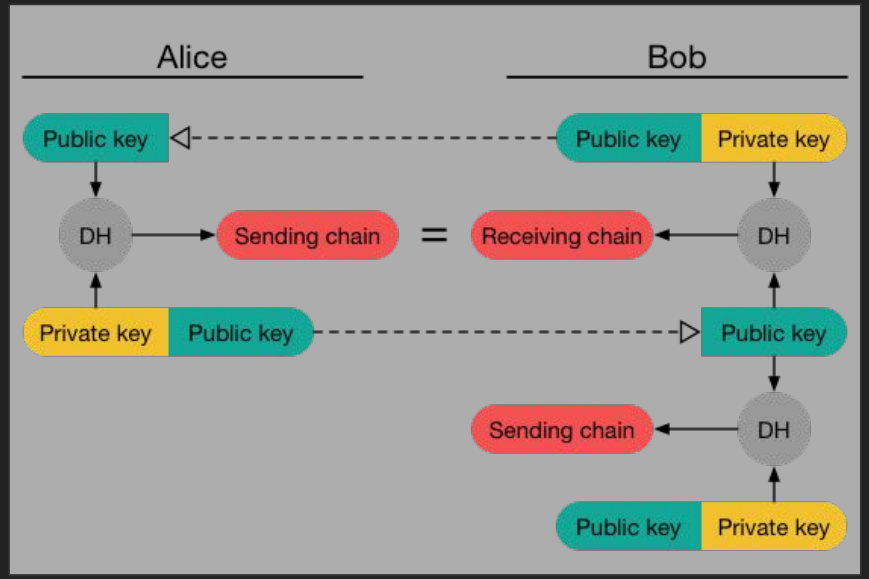
https://signal.org/blog/verified-safety-number-updates/

Cryptography: Signal

- End-to-end encryption
- Curve25519
- AES-256
- HMAC-SHA256

Key Update: The Double Ratchet Algorithm





Forward secrecy

Post-compromise security

https://signal.org/docs/specifications/doubleratchet/

Implementers of the Signal Protocol

- Signal
- WhatsApp (Meta)
- Messenger (Meta)
- Messages (Google)
- Skype (Microsoft)

Based on parts of it:

- Wire
- Matrix (libolm)

Shortcomings* to note compared to Signal

End-to-end encryption	See other slide
Key Exchange	iMessage, Threema (minor), Wire (minor)
Cryptography	iMessage, Telegram
Key Update	iMessage (none), Threema (optional), Telegram (minor)
Deniability	iMessage, Matrix

*might be inaccurate


METADATA
METADATA EVERYWHERE
LIGHTYEAR
Meme based on Pixar's Toy Story

Signal Metadata

- Phone number
- Last connection timestamp
- Account creation timestamp

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS

(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed									
Legal Process & Additional Details	• **Message Content: Limited** • **Subpoena:** can render basic subscriber information • **18 U.S.C. §2709(d):** can render 25 days of iMessage lookups to and from a target number[1] • **Pen Register:** no capability • **Search Warrant:** can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud	• **Message Content: Limited*** • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage *Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applies and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• **No Message Content** • Date and time a user registered • Last date of a user's connectivity to the service	• **No Message Content** • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram *may* disclose IP address and phone number to relevant authorities	• **No Message Content** • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• **No Message Content:** • Provides account (i.e. phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number	• **No Message Content** • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• **Message Content: Limited*** • **Subpoena:** can render basic subscriber records • **Court Order:** Subpoena return as well as information like blocked users • **Search Warrant:** Provides address book contacts and WhatsApp users who have the target in their address book contacts • **Pen Register:** Sent every 15 minutes, provides source and destination for each message *If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• **No Message Content** • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

 SUBSCRIBER DATA

 MESSAGE SENDER-RECEIVER DATA

 DEVICE BACKUP

 IP ADDRESS

 ENCRYPTION KEY(S)

 DATE/TIME INFORMATION

 REGISTRATION TIME DATA

 USER'S CONTACTS

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

1 (U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry between parties does not indicate a conversation took place. These query logs have also contained errors.

https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/

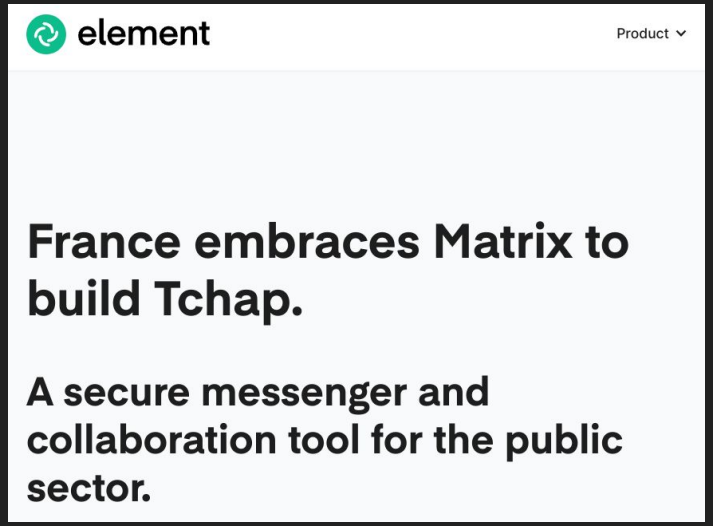
Signal: trusting the creators?

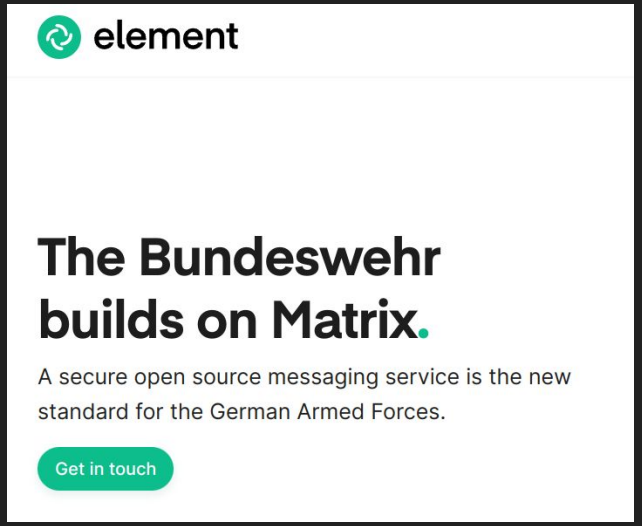
- Nonprofit foundation
- Track record of being privacy focused
- Work in a way (open source) trust does not need to be absolute

1970-2018: Crypto AG

- Swiss company, secretly controlled by the U.S. and Germany, selling backdoored secure communication equipment

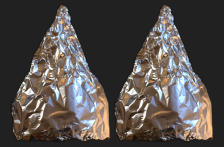
Tchap and BwMessenger





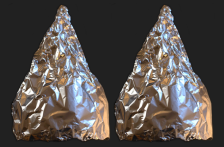
Beyond Signal

Beyond Signal: Key Exchange



- Ensure always unique initial keys
- Enforce identity verification
- Meet in person

Conventional vs quantum computer security level

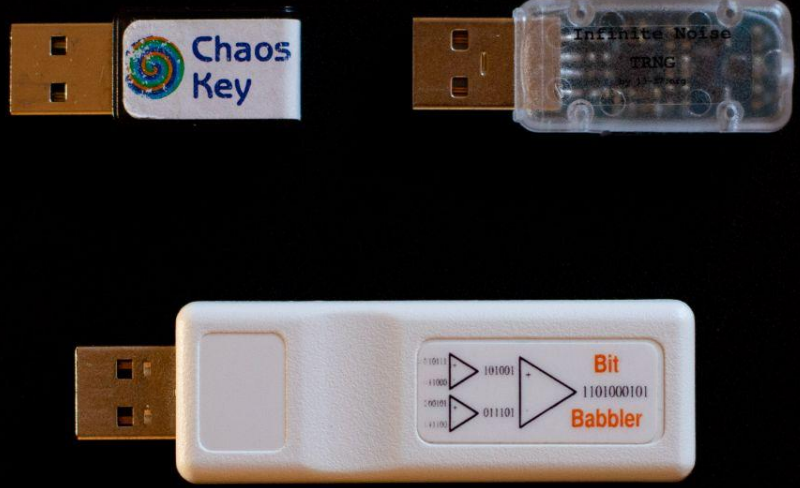


Algorithm	Effective Key Strength	
	Conventional	Quantum Computers
RSA-2048	112 bits	0 bits
ECC-384	256 bits	0 bits
AES-128	128 bits	64 bits
AES-256	256 bits	128 bits
SHA3-256	256 bits (preimage)	128 bits (preimage)

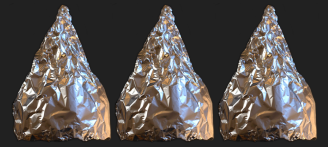
WWII: 5-UCO

From “Top Secret: From ciphers to cyber security” at the Science Museum, U.K.

True Random Number Generators (TRNG)

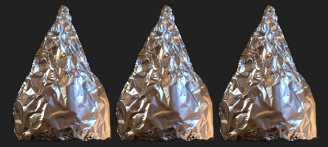


Concept: Robust Combiners



- Combine crypto primitives in a way that is as secure as the primitives individually

Beyond Signal: Key Update

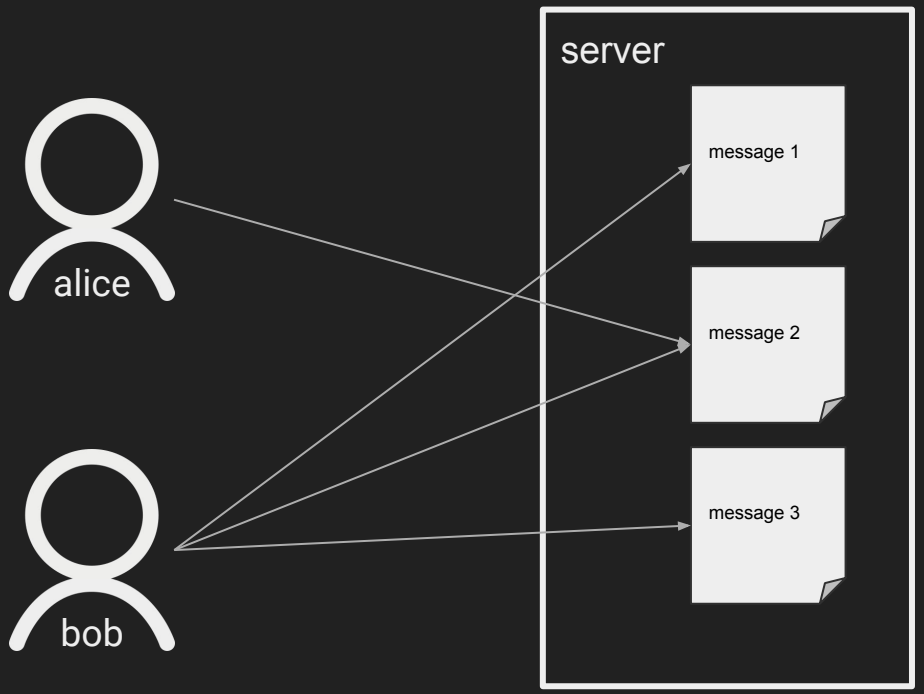


- A small security issue have been found in the Double Ratchet algorithm, with a proposed solution called the Triple Ratchet
- Add requirements to send/receive
  - Biometrics
  - Yubikeys
  - Interaction with other participants in conversation

Beyond Signal: Metadata

- Don’t require any personal information like phone numbers
  - Might make preventing abuse harder

Concept: Private Information Retrieval



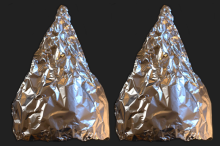
1800s: Encrypted newspaper ads

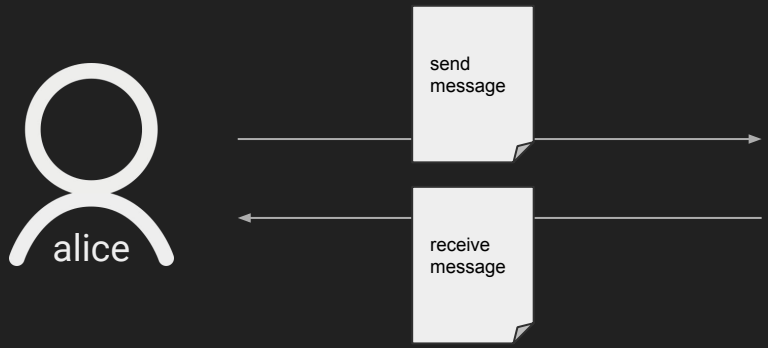
ONE OF THE ENCRYPTED ADS PUBLISHED IN *THE TIMES*. (IMAGE: ELONKA DUNIN, A.J. JACOBS, KLAUS SCHMEH.)

https://www.vice.com/en/article/4axwz3/codebreakers-find-sexts-arctic-dispatches-in-200-year-old-encrypted-newspaper-ads

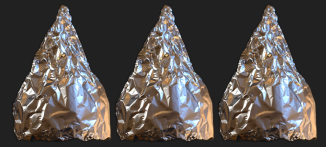
WWI, onwards: Numbers station

Beyond Signal: Appear like other traffic



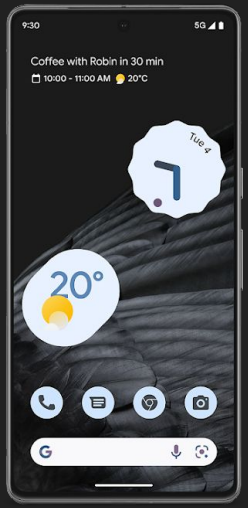


My hobby project



Cryptography

Protocol



Colossus replica displayed at the National Museum of Computing, U.K.