

# Signal

## La crittografia a portata di tua nonna

*Matteo Martinelli 24/02/21*



[www.luccalug.it](http://www.luccalug.it)



# Bad models create bad products

## Fondazione no-profit

- Signal Foundation
- Supporto attraverso donazioni di utenti ed entità interessate al progetto

## Sviluppo aperto

- Ricerca e sviluppo di nuove soluzioni
- Software libero
- Codice e discussioni pubbliche su Github e Forum degli utenti
- Audit pubblici da parte di università e entità private

# Information security not Computer security

## Computer security

Mettere informazioni importanti in un computer e fare in modo che altre persone non possano accedervi

Strategia perdente DA SEMPRE

## NEWS

[Home](#) | [Coronavirus](#) | [Video](#) | [World](#) | [UK](#) | [Business](#) | [Tech](#) | [Science](#) | [Stories](#) | [Entertainment](#)

[Tech](#)

## Adobe hack: At least 38 million accounts breached

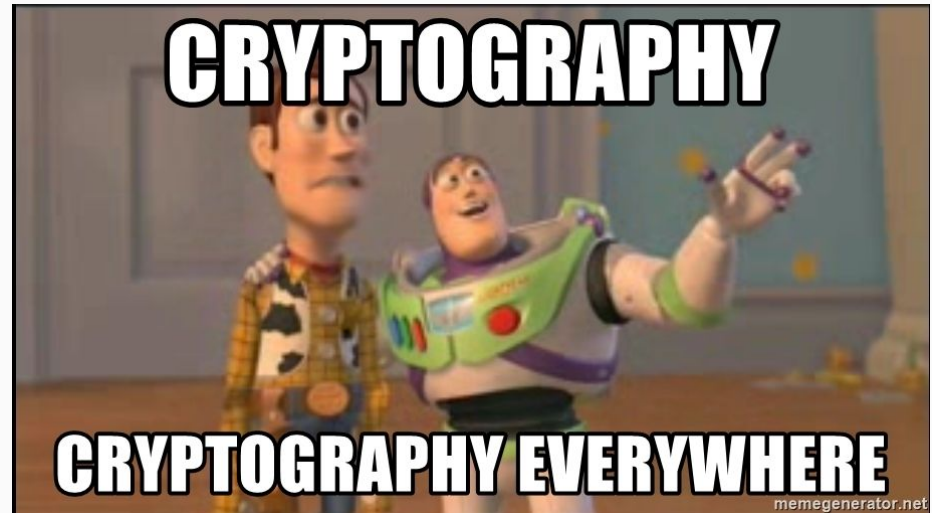
🕒 30 October 2013

# Information security not Computer security

## Information security

Mettere in sicurezza l'informazione stessa in modo da non doversi preoccupare del computer

Il computer può essere compromesso ma le informazioni rimarranno comunque al sicuro perché crittografate



Non un sistema in cui ti devi fidare di chi detiene i tuoi dati, ma un sistema in cui non devi fidarti affatto

# Signal protocol

Protocollo di crittografia End-to-End che garantisce:

- Confidenzialità
- Integrità
- Autenticazione
- Consistenza partecipanti
- Segretezza passata
- Segretezza futura (concetto ideato da Signal protocol)
- Irriconducibilità dei messaggi
- Diniego dei messaggi
- Diniego dei partecipanti
- Asincronia

# Probabilmente lo stai già usando ma non lo sai

- Whatsapp
- Skype
- Google Allo
- RCS (Android message)
- Facebook messenger
- Wire
- ...



# Non è tutto oro quel che luccica

## Signal

**None.**

(The only personal data Signal stores is your phone number, and it makes no attempt to link that to your identity.)



## Telegram

Contact Info  
Contacts  
User ID



## Whatsapp

Device ID  
User ID  
Advertising Data  
Purchase History  
Coarse Location  
Phone Number  
Email Address  
Contacts  
Product Interaction  
Crash Data  
Performance Data  
Other Diagnostic Data  
Payment Info  
Customer Support  
Product Interaction  
Other User Content



## Facebook

Purchase History	Advertising Data
Other Financial Info	Other Usage Data
Precise Location	Crash Data
Coarse Location	Performance Data
Physical Address	Other Diagnostic Data
Email Address	Other Data Types
Name	Browsing History
Phone Number	Health
Other User Contact Info	Fitness
Contacts	Payment Info
Photos or Videos	Photos or Videos
Gameplay Content	Audio Data
Other User Content	Gameplay Content
Search History	Customer Support
Browsing History	Other User Content
User ID	Search History
Device ID	Sensitive Info
Product Interaction	iMessage
Device ID	Email address
Signal	Phone number Search history





# Let's get technical

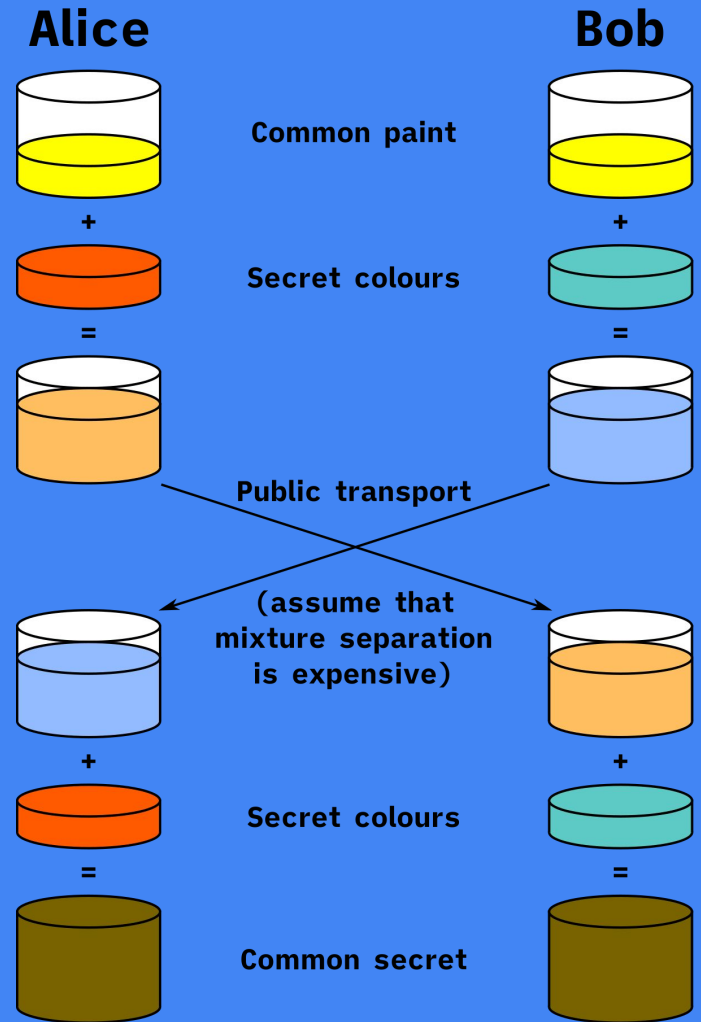
## Signal amalgama in un unico protocollo

- Extended Triple Diffie-Hellman
- Double Ratchet
- Curve25519, AES256, HMAC-SHA256 come primitive crittografiche

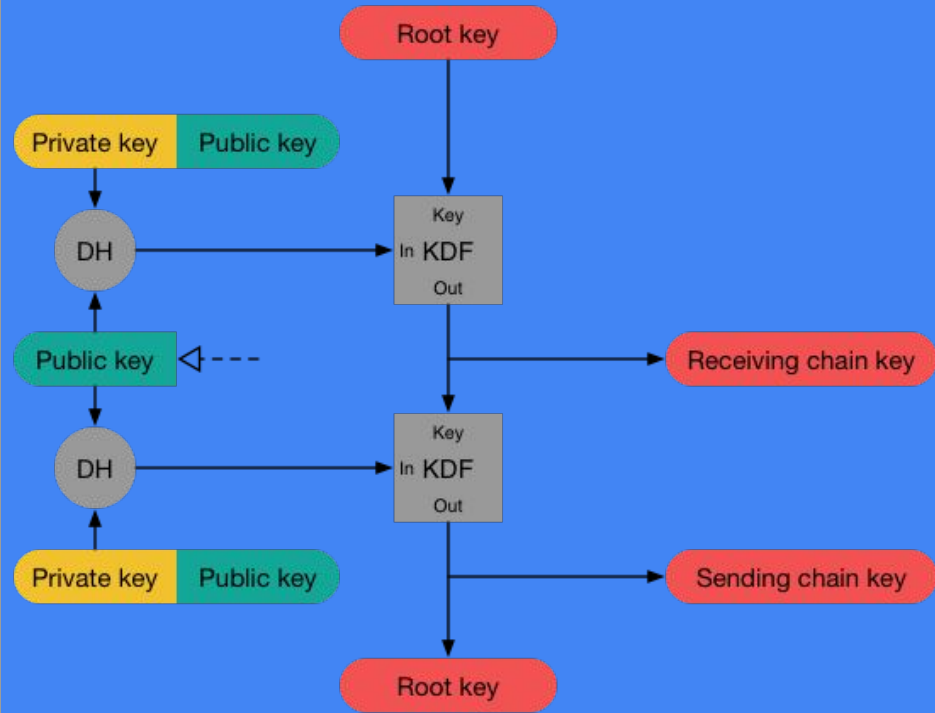
Vediamo questi componenti singolarmente

# X3DH

eXtended Triple Diffie-Hellman



# Double Ratchet algorithm



# Primitive crittografiche utilizzate

## Curve25519

Curva ellittica per la generazione della chiavi

## AES-256

L'effettivo algoritmo che cripta il testo in chiaro con le chiavi generate precedentemente

## HMAC-SHA256

Algoritmo che verifica l'integrità dei dati e l'autenticazione dei messaggi

# ...e tutto questo solo per lo scambio di messaggi

Ci sono molte altre soluzioni che Signal ha progettato per rendere l'applicazione il più moderna e comoda possibile

- Private contact discovery
- Private groups
- Private profiles
- Secure value recovery
- ...

# Facile da usare

Anche la migliore crittografia è inutile se utilizzata da nessuno

Offrire la migliore esperienza possibile grazie a

- Attenzione per la UX (per gli utenti non tecnici)
- Protocollo centralizzato

Domande?