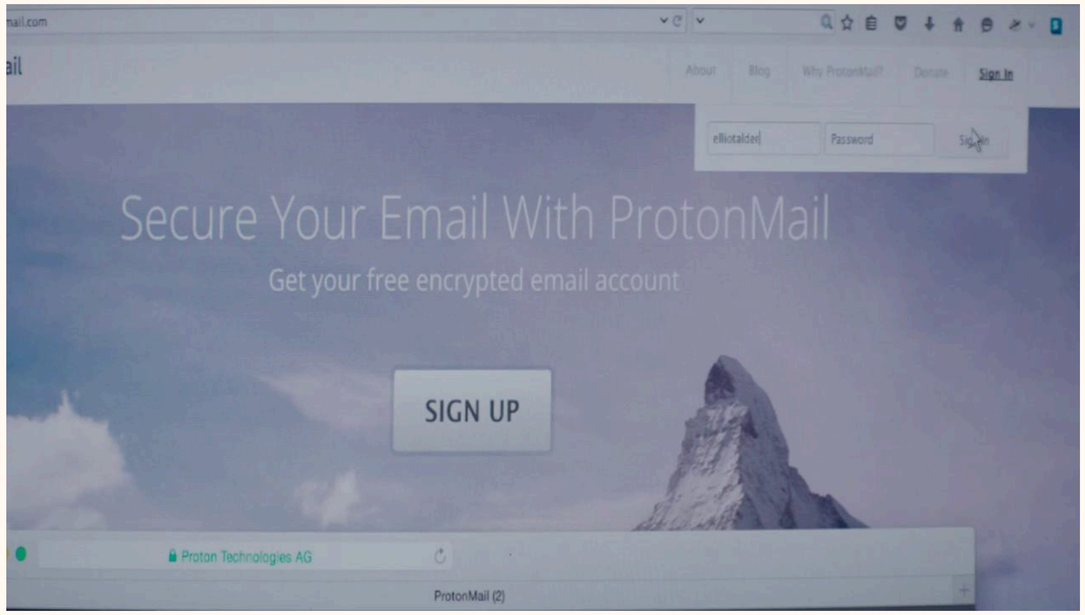
Making end-to-end encryption user friendly

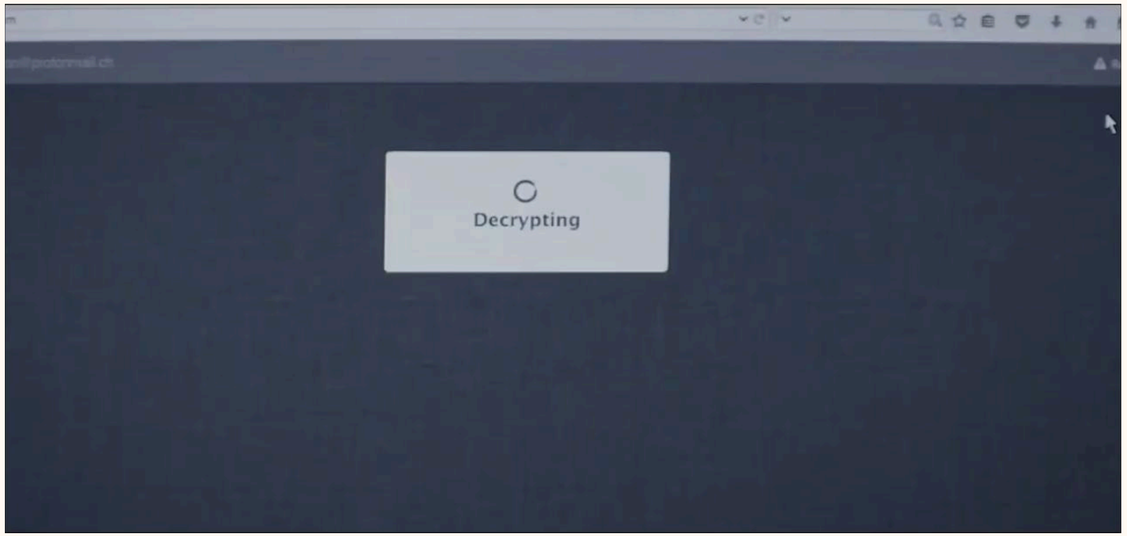
(in distributed systems)

Polycloud 2025 | Tristan-Mihai RADULESCU

Ma série préférée

Ma série préférée





“We cannot read or give anyone else access to your emails [...] no special software or tech skills required. ”

Proton Mail · Security

Nos protagonistes

Alice 🫖

Elle a le main character syndrome. Elle aime trop discuter avec Bob via Le chaton ©

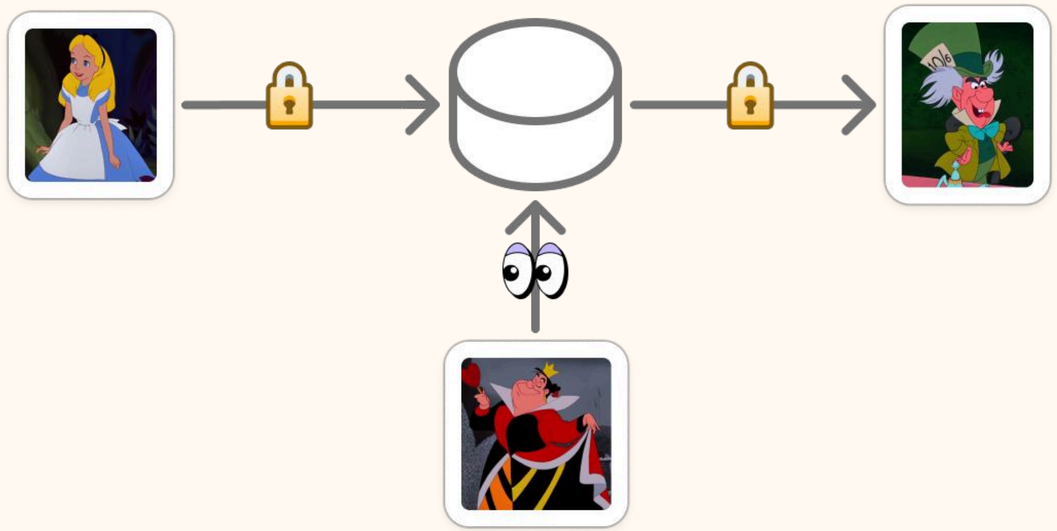
Bob ⏱️

Lui il est juste trop bête. Il raconte toute sa vie à Alice sur Le chaton ©

Malory 🏴‍☠️

Elle, c’est une hackeuse de haute voltige qui cherche à hacker le chaton ©

Chiffrement de bout en bout



Notre objectif

Le chaton©

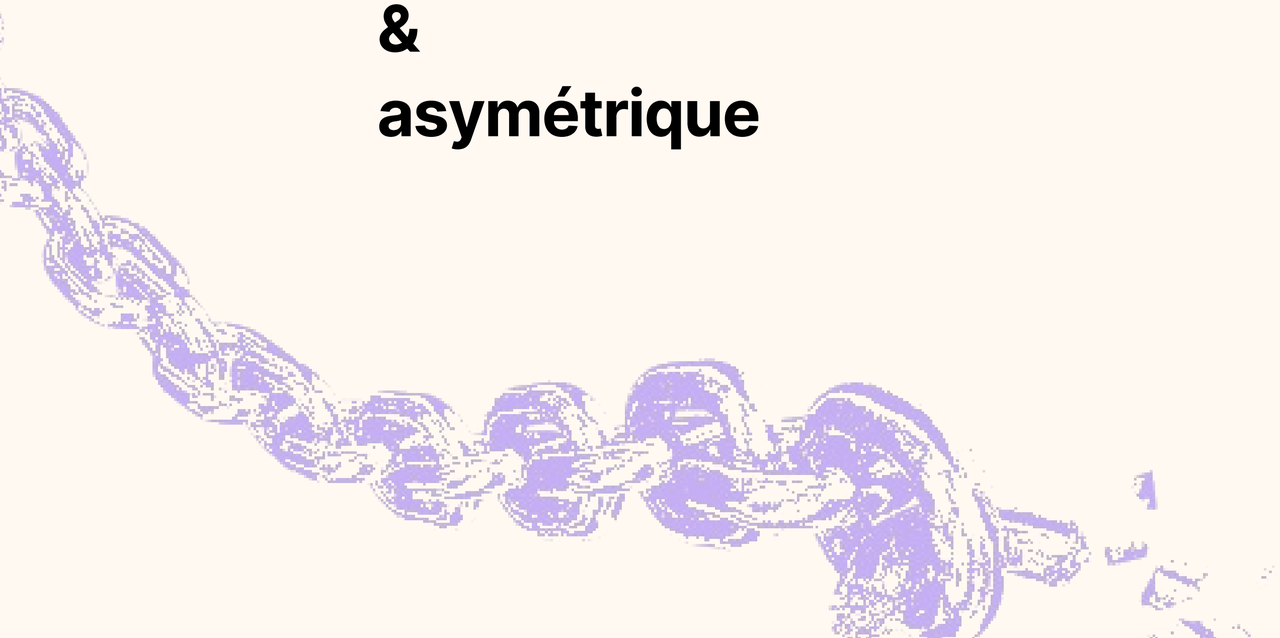
Une messagerie :

- Chiffré de bout en bout
- Et authentifié
- Facile à utiliser

comme le chat t'as vu il peut etre invisible comme toi sur internet avec Le chaton© (vision ?)

Au programme

1. Chiffrement symétrique & asymétrique
2. Diffie Hellman
3. Protocole signal

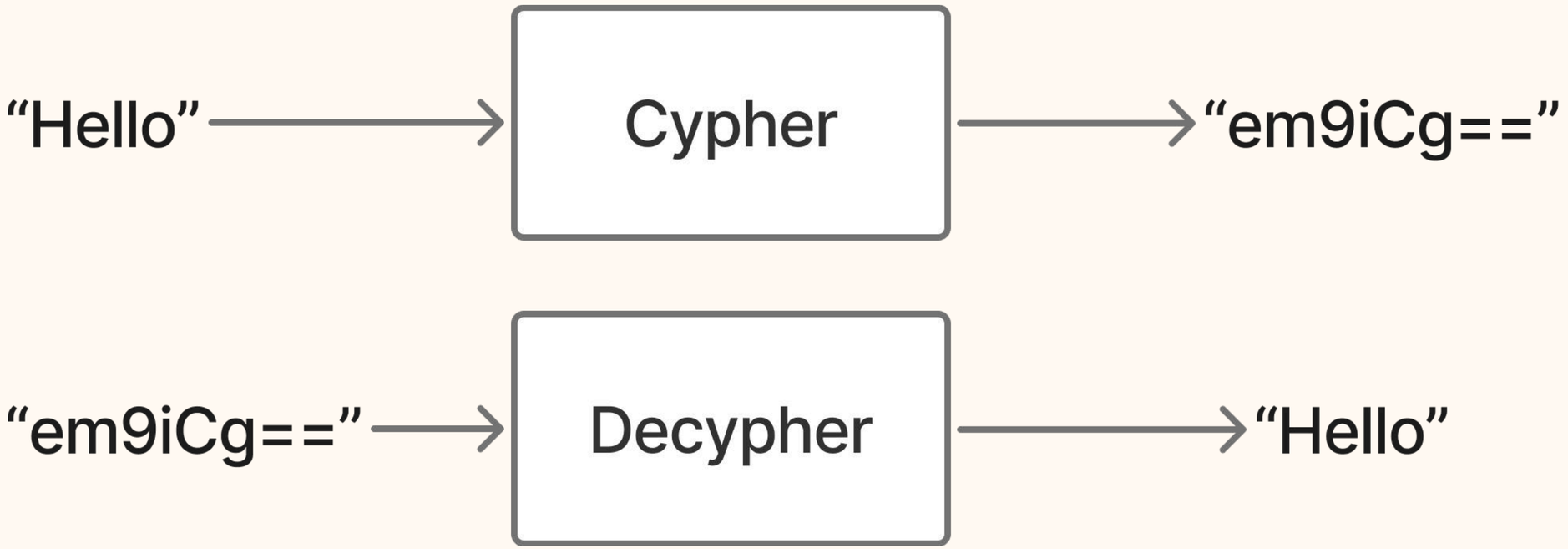


→ $ whoami

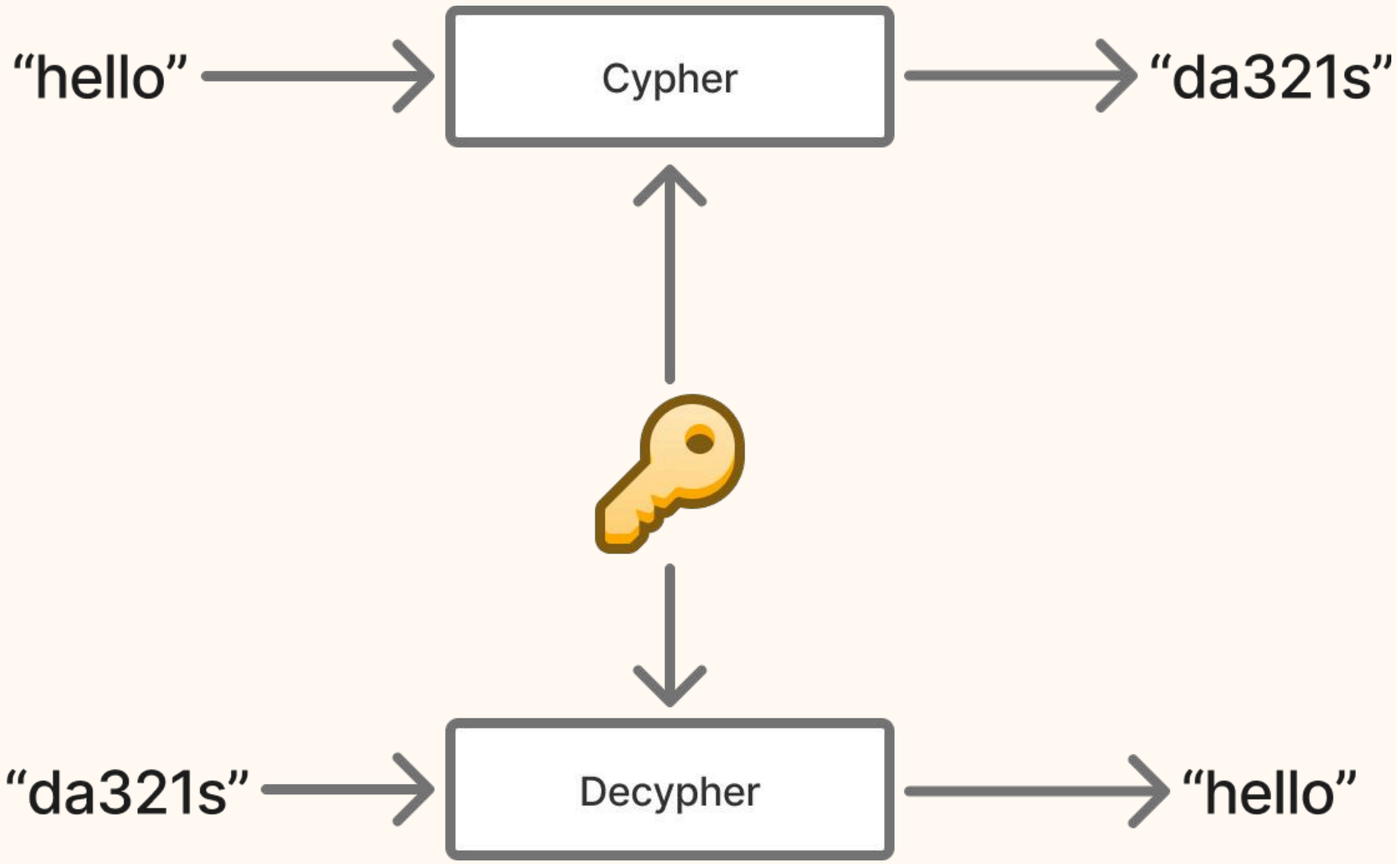
Tristan-Mihai Radulescu (Courtcircuits)

- Apprenti à Polytech Montpellier
- Software eng. à Sweep 🌱
- courtcircuits.xyz
- github.com/Courtcircuits

Comment cacher de l’information

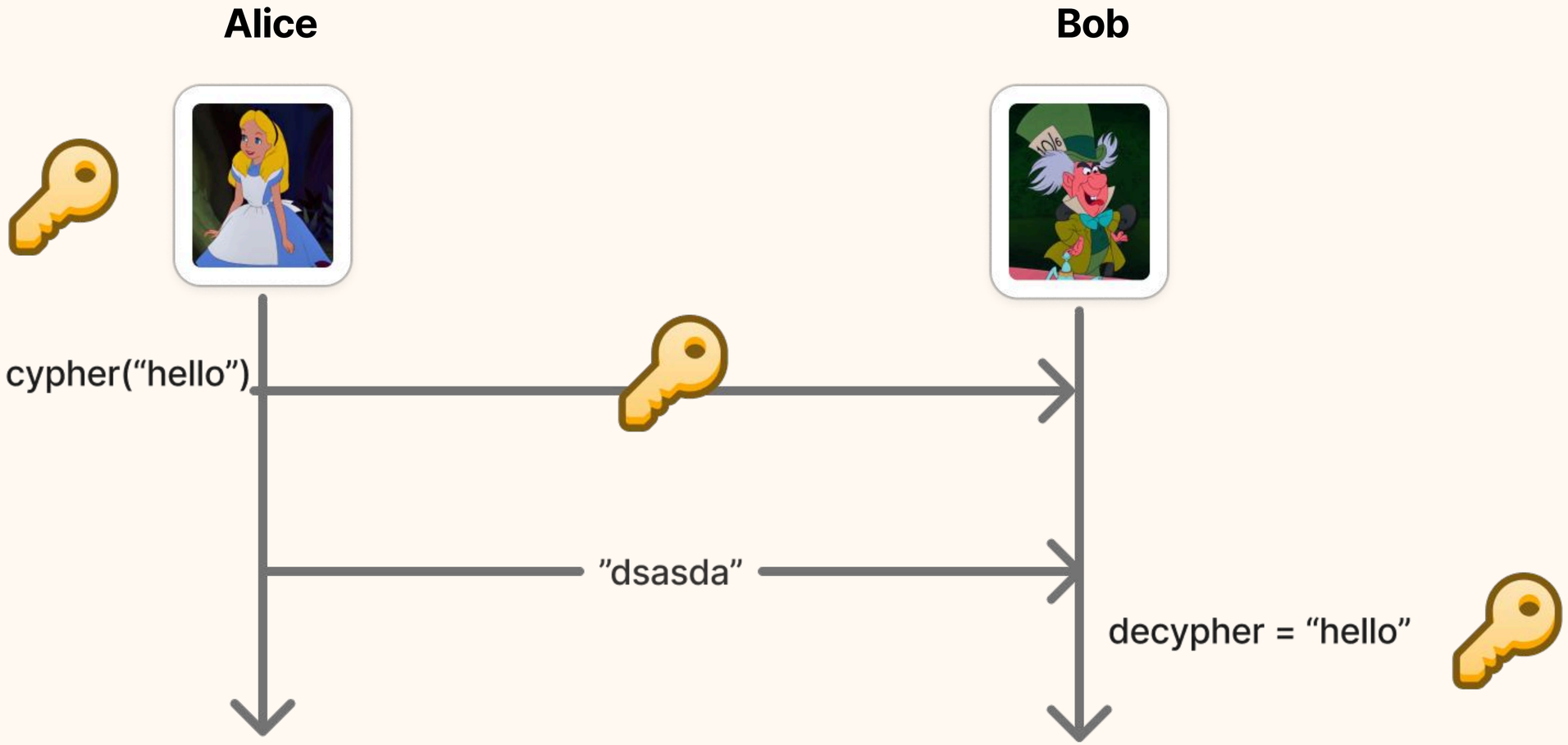


Chiffrement à clé secrète (ou symétrique)



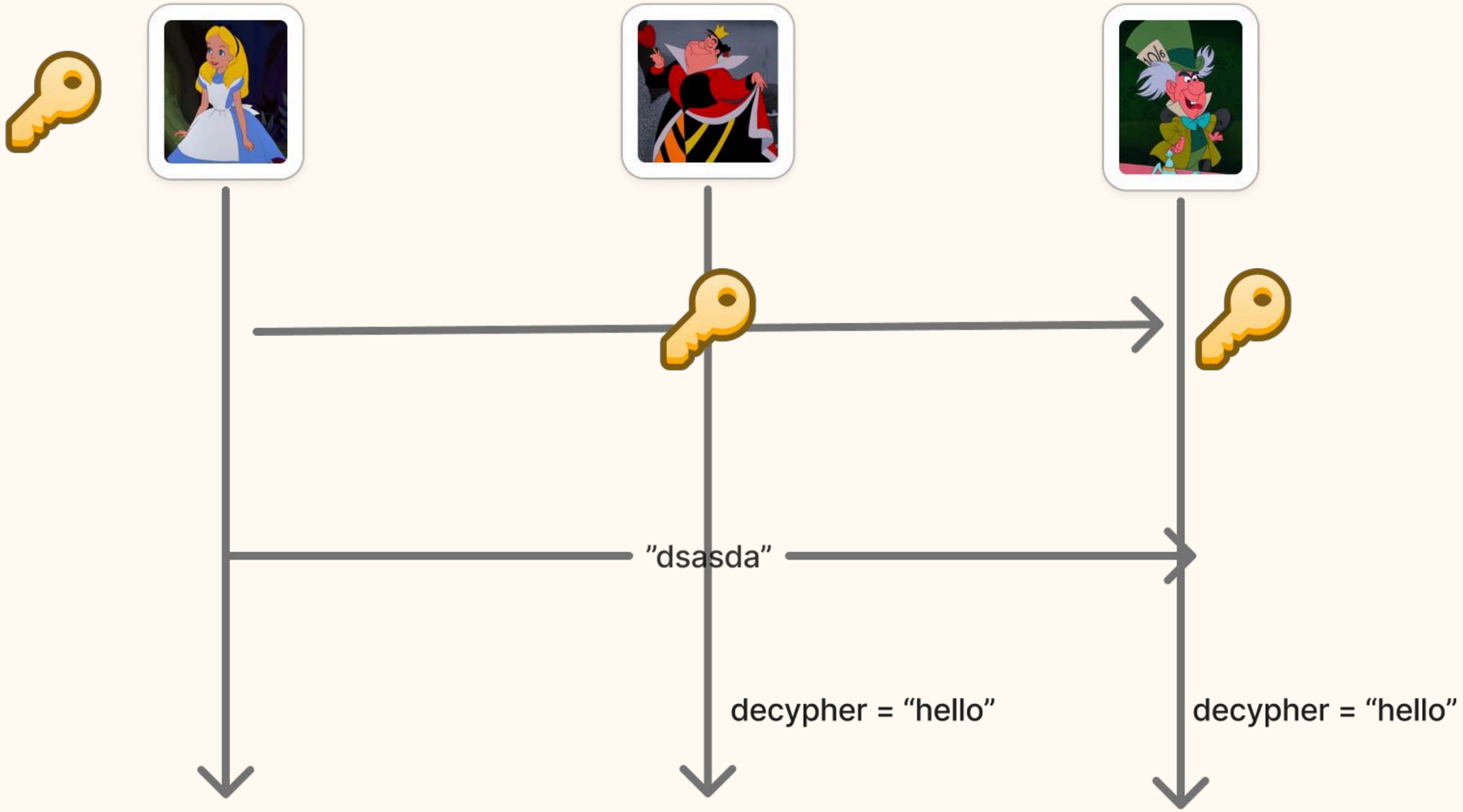
Chiffrement symétrique

En pratique

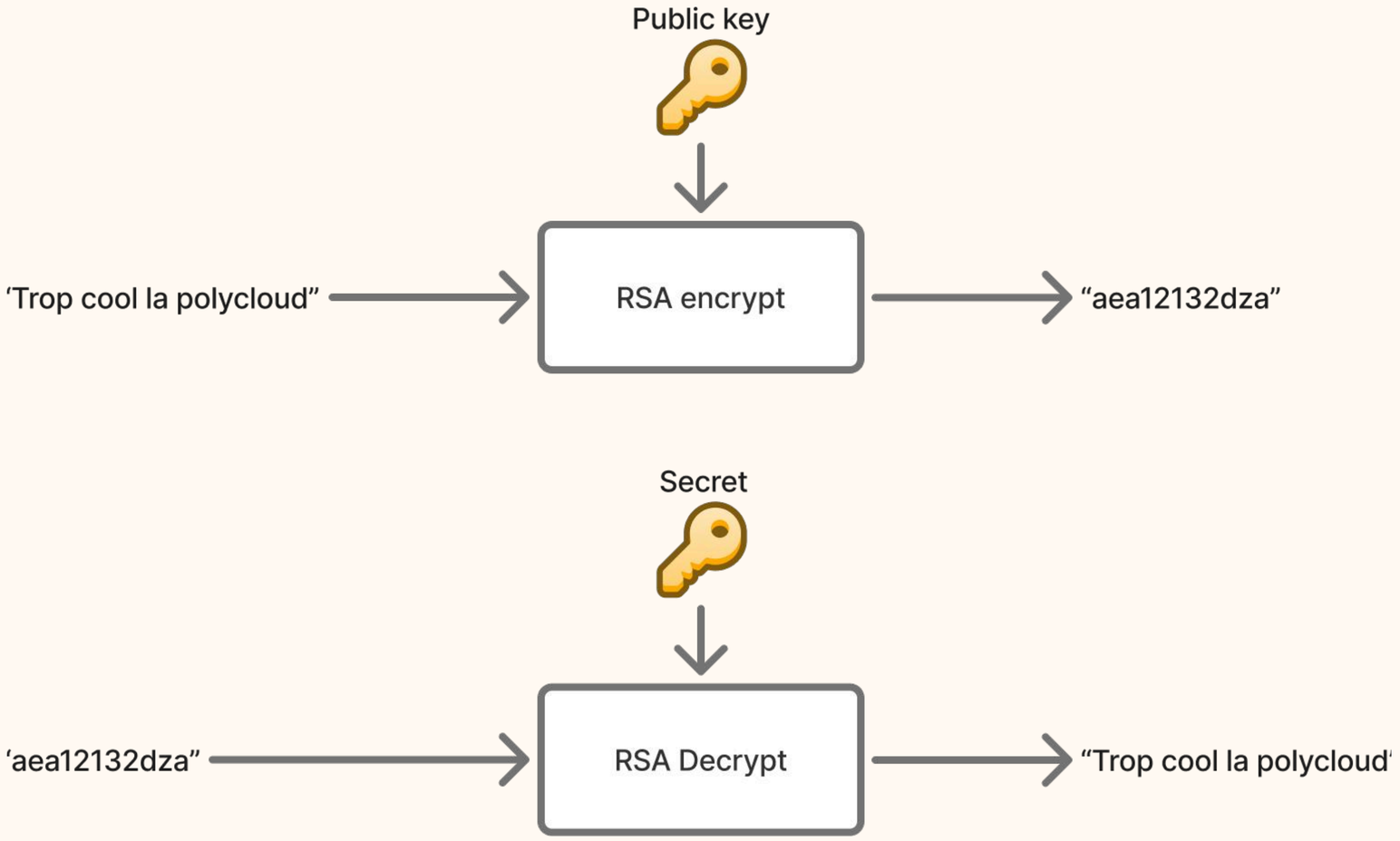


Attaque sur le chiffrement symétrique

L'échange de clé



Chiffrement à clé publique (ou asymétrique)



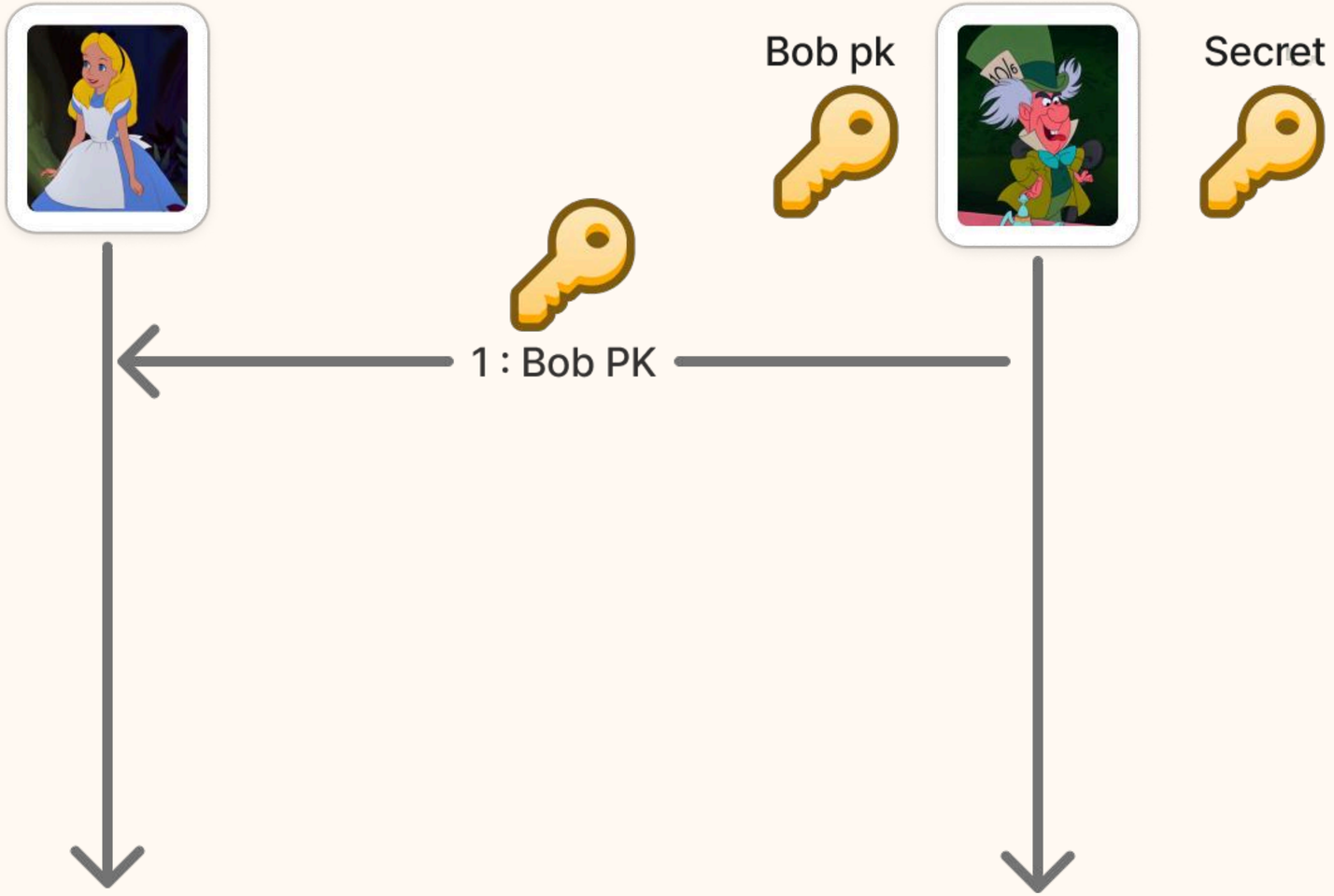
Clé publique

- Information à partager
- Permet de **chiffrer** un message

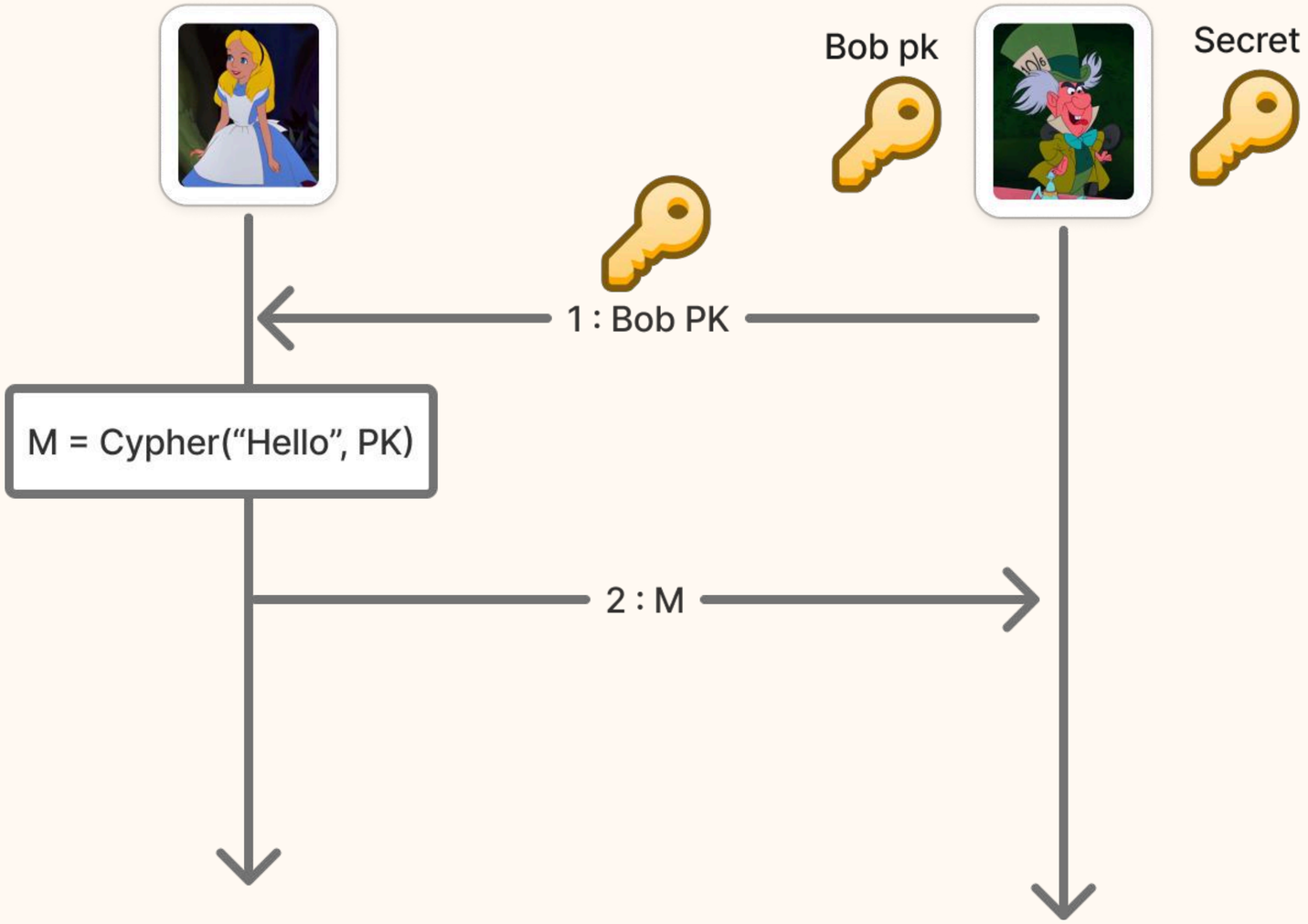
Clé privé

- **Secret** à ne **surtout pas partager**
- Permet de **déchiffrer** un message

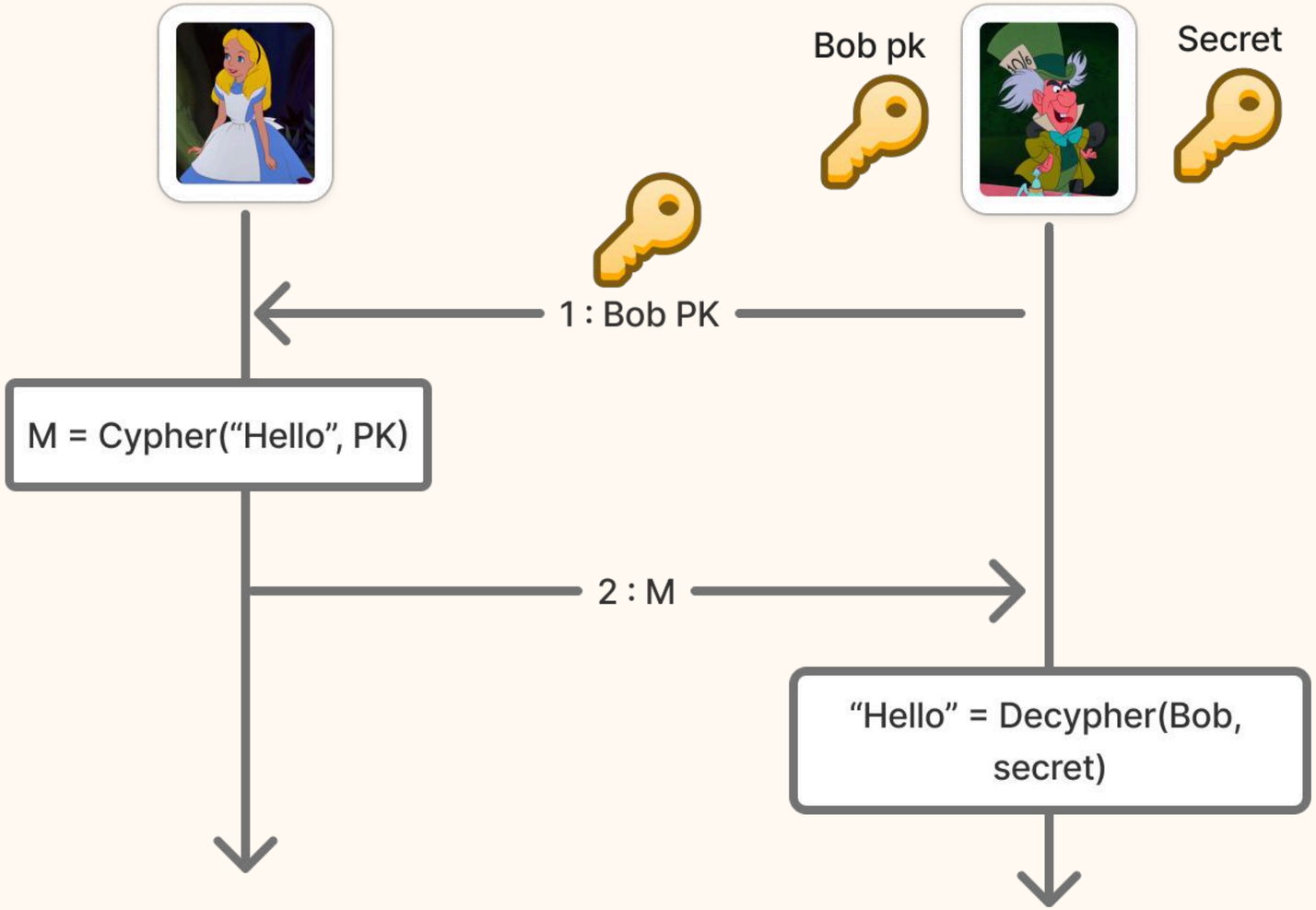
Chiffrement asymétrique



Chiffrement asymétrique



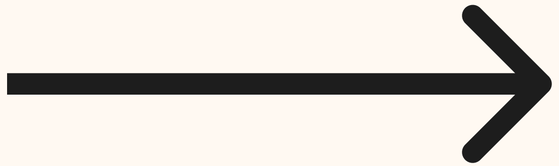
Chiffrement asymétrique



Signature asymétrique

Clé publique

Permet de **vérifier** un message



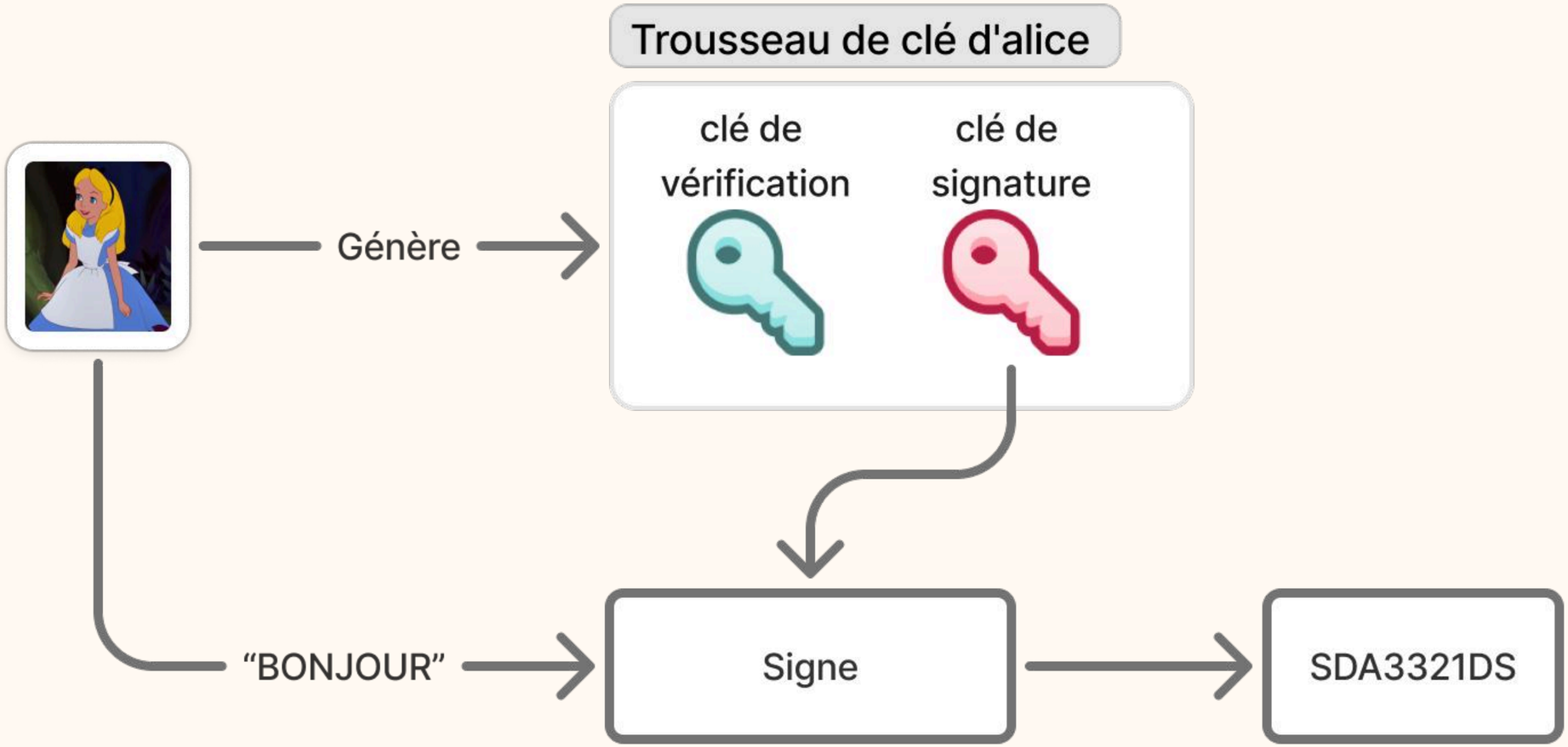
Clé privé

Permet de **signer** un message

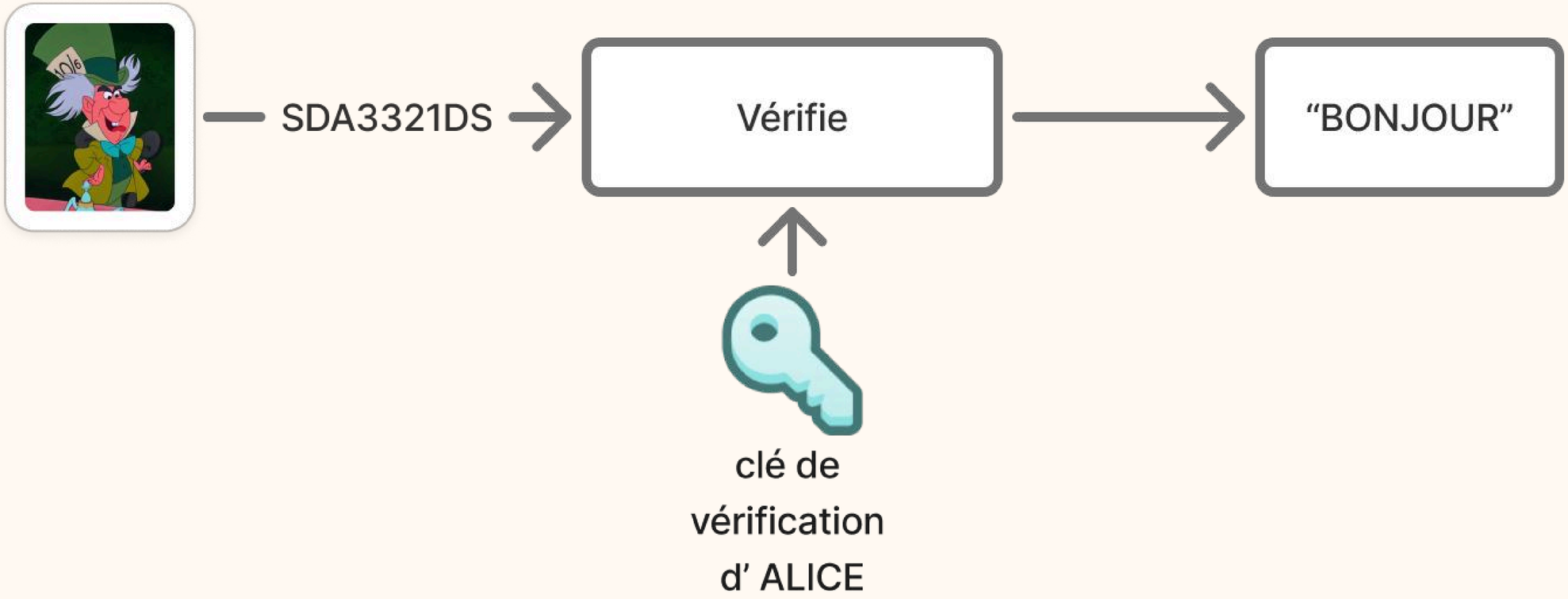
Authentification

- Un message ne peut être modifié que par son propriétaire

Signature asymétrique



Vérification



Contraintes de la cryptographie à clé secrète 😿

Messages de taille limitée

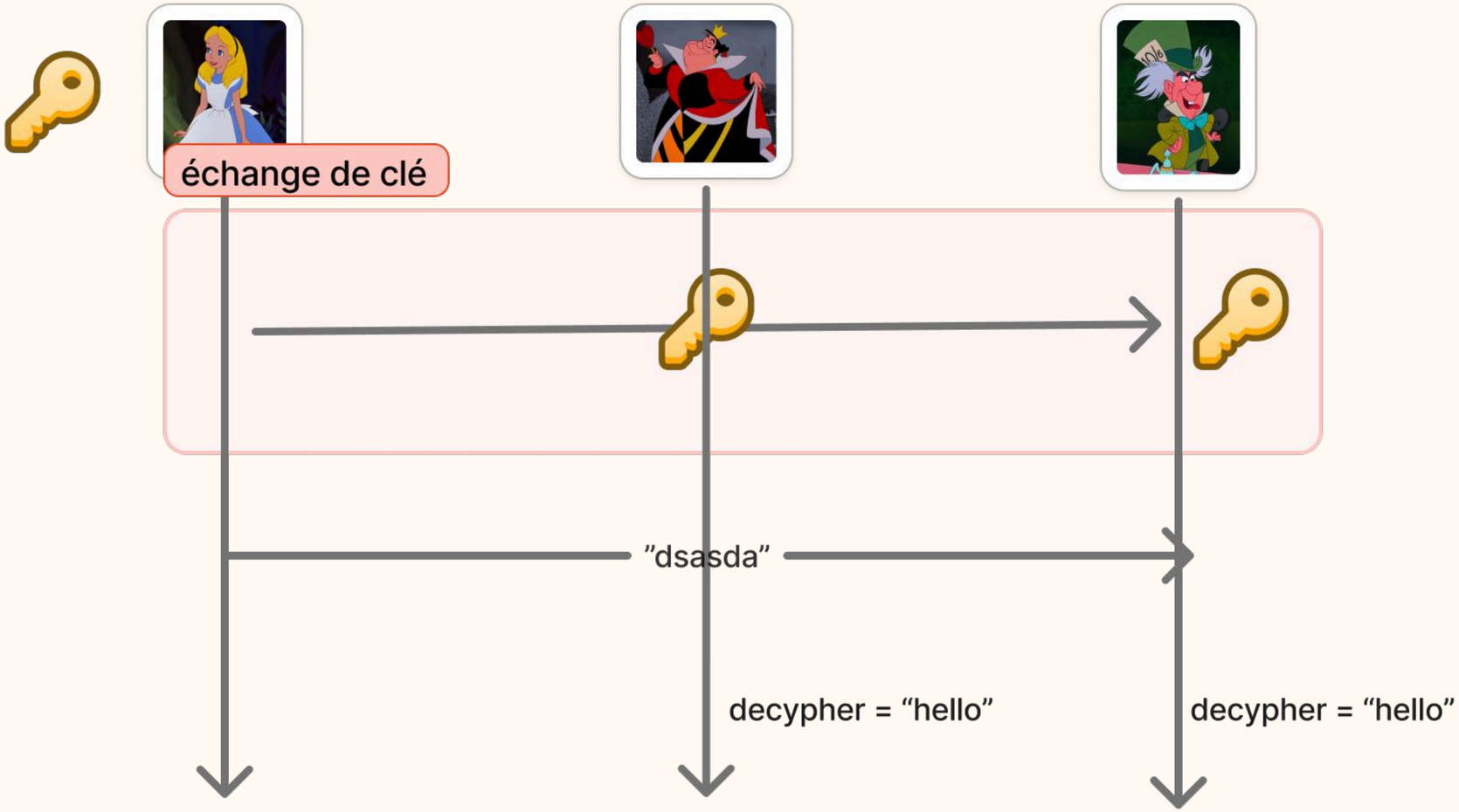
thread 'main' panicked at src/asymmetric.rs:26:10:
failed to encrypt: MessageTooLong

Problèmes de performance

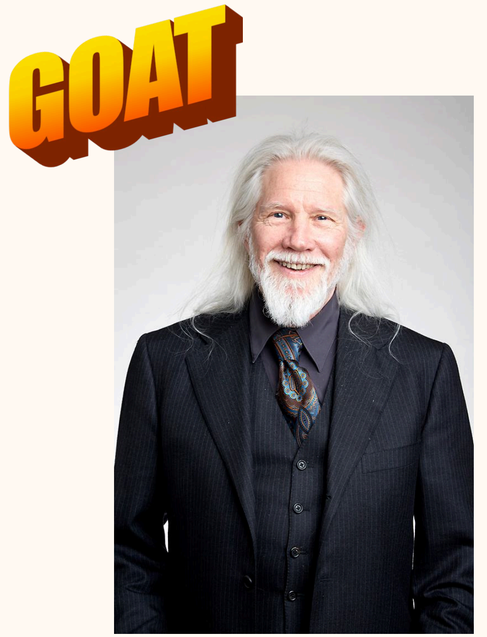
RSA (2048) → 2.646s
AES 256 GCM → 647µs

Reference : github.com/Courtcircuits/polycloud-lechaton

Protocole hybride



Echange de clé de Diffie Hellman (1976)



Whitfield Diffie

Objectif :

- Définir un **secret commun** de façon **sécurisée**
- Secret commun ⇒ clé de chiffrement symétrique

Martin Hellman

Chiffrement asymétrique

Problème du logarithme discret

“Connaissant g, X et P, trouver x”

$$g^x \bmod P = X$$

Clé publique

(g, P)

Clé privé

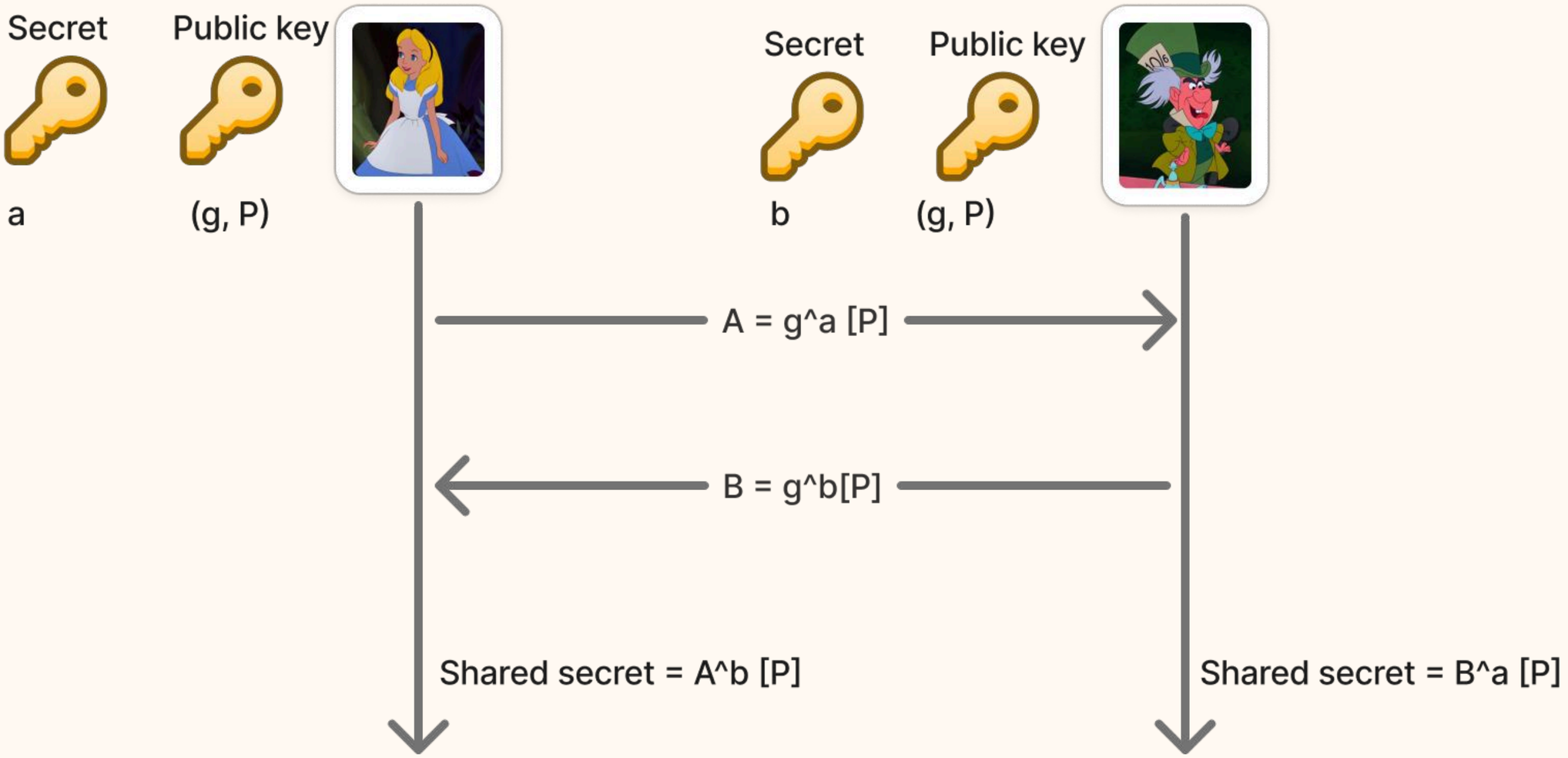
x

Chiffré

X

Source : elliptic curves (lecture 9 - MIT 2022)

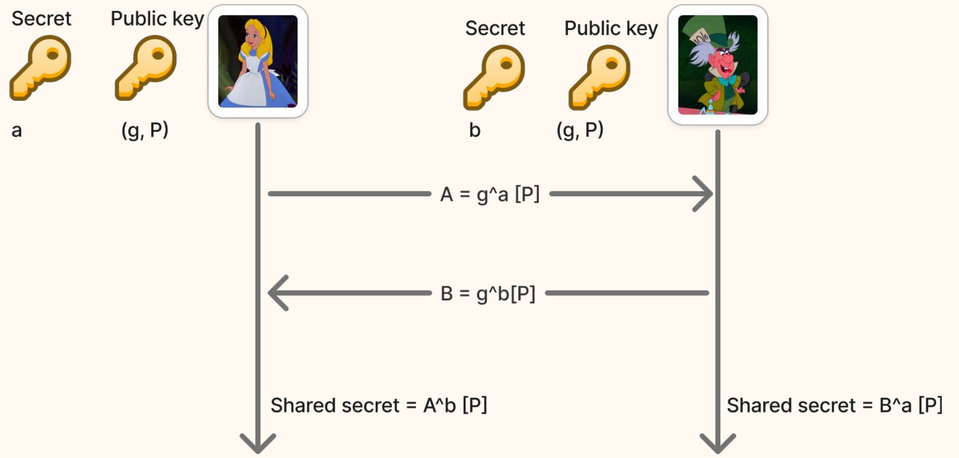
Échange de clés asymétrique (Diffie Hellman)



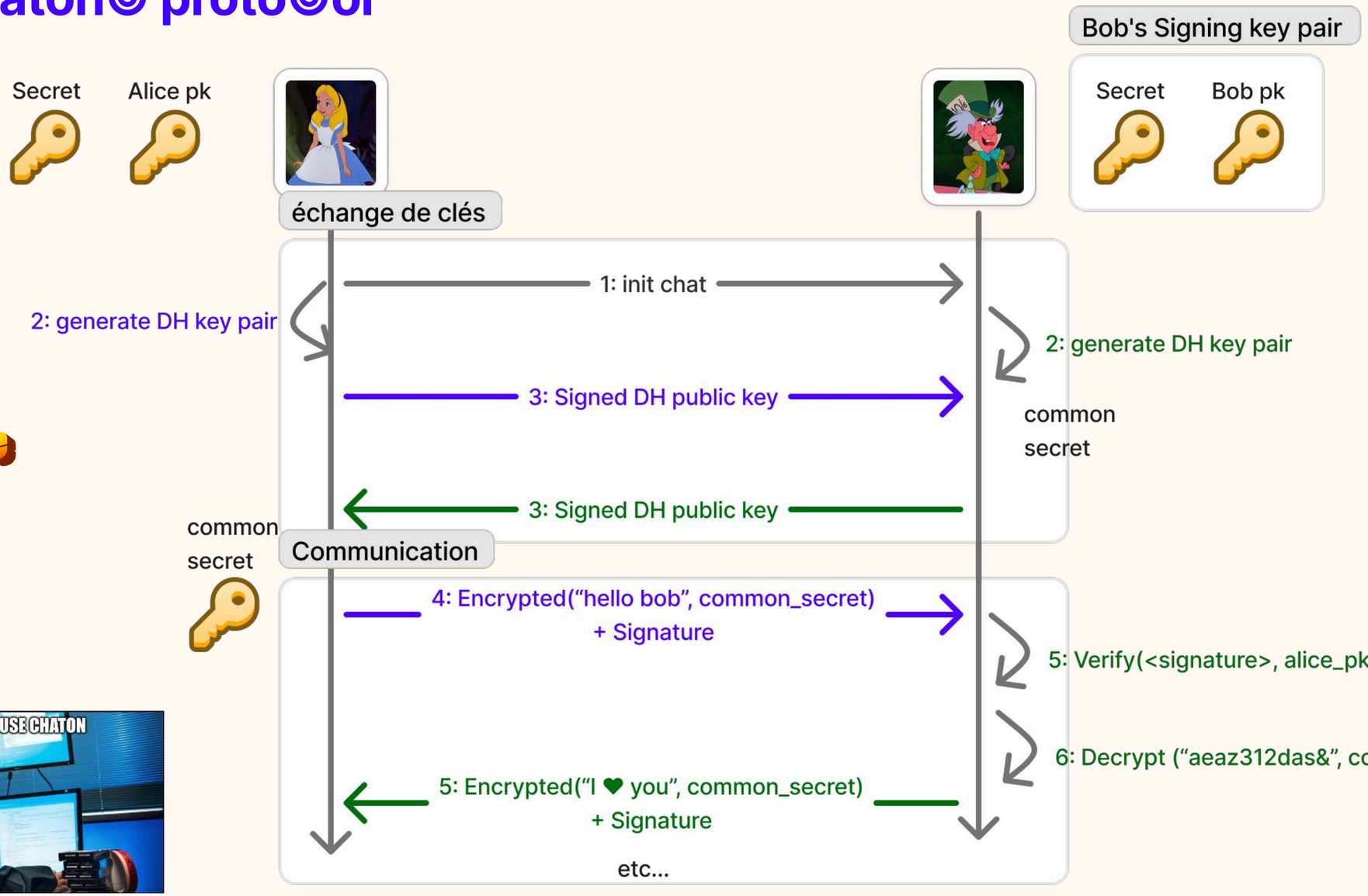
Échange de clés asymétrique (Diffie Hellman)

Secret en commun :

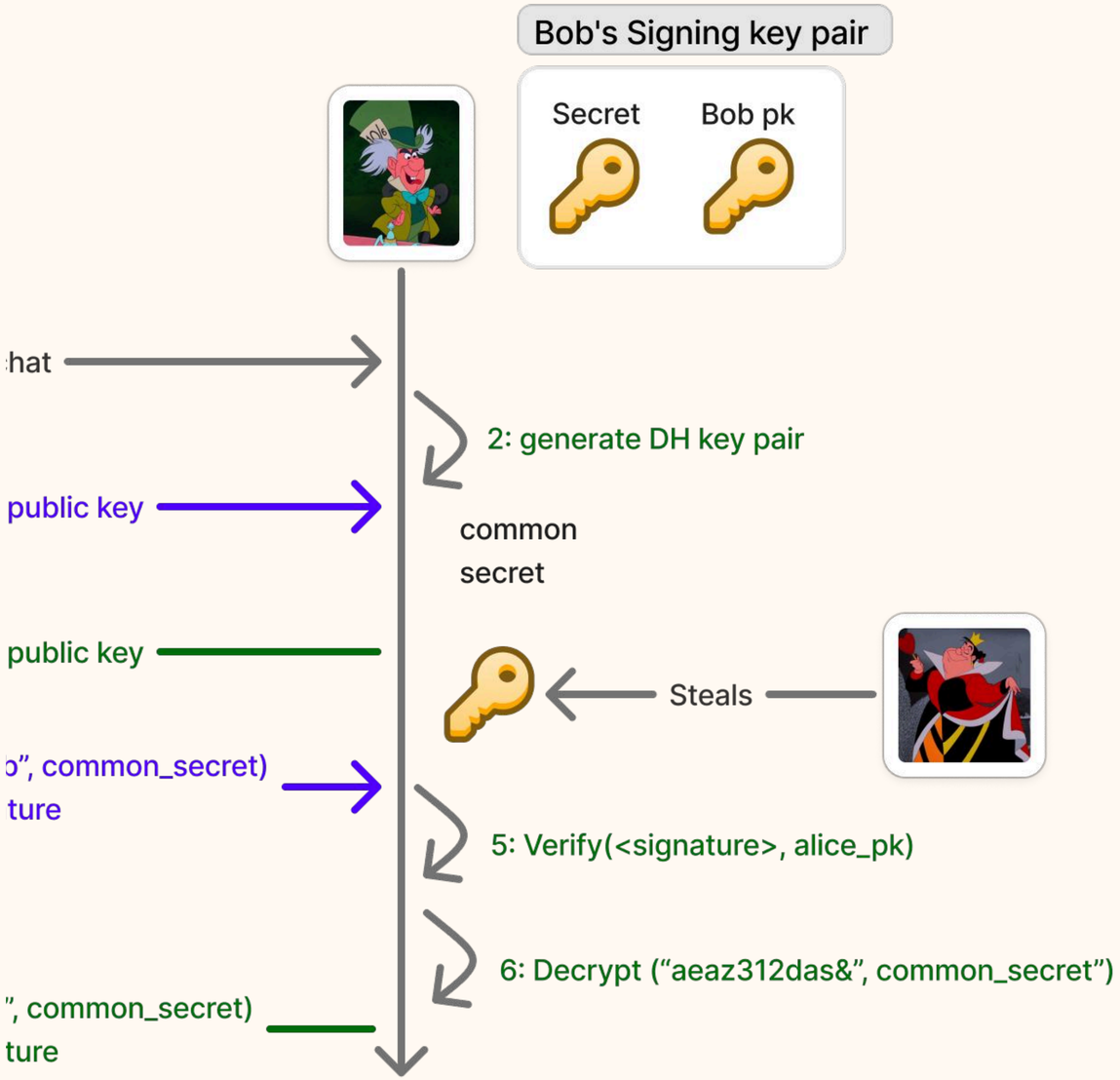
$$A^b = (g^a)^b = g^{a*b} = (g^b)^a = B^a$$



Le chaton© proto©ol



Malory is back...



Scénarios de compromission

- Backdoor
- Social engineering
- Phishing
- Vol d'appareil
- ...

The Double Ratchet algorithm

Ou protocole Signal

Au programme

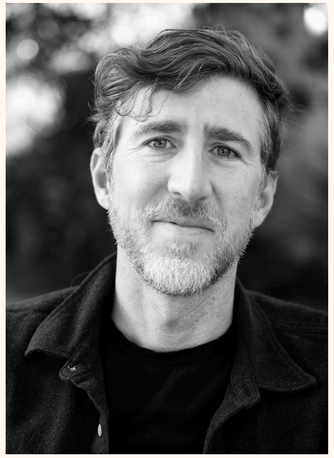
0. Histoire
1. Dérivation de clé
2. Ratchet diffie hellman
3. Mise en application

Signal Protocol (2016)

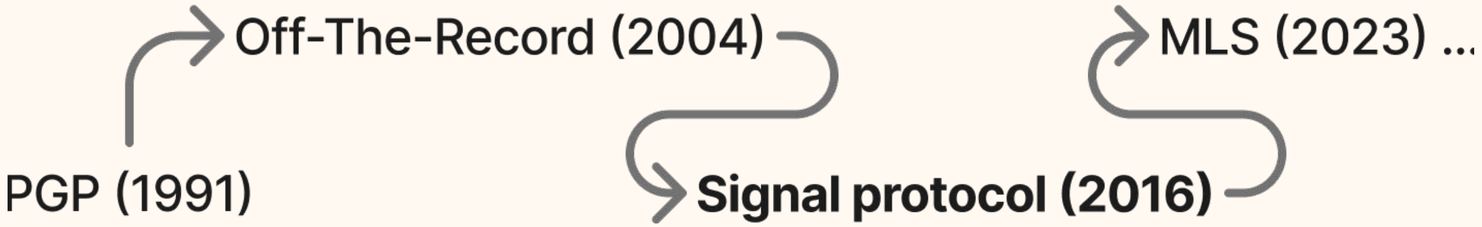
Noms :

- Double ratchet algorithm
- Signal protocol
- Axolotl algorithm

Trevor Perrin



Moxie Marlinspike



Propriétés

Propriétés cryptographiques du Double Ratchet Algorithm

Propriétés du DRA (double ratchet algorithm)

✅ Chiffrement de bout-en-bout

Les messages passant par le système ne sont lisible que d’un bout à l’autre du système.

✅ Authentification

Le message a bien été envoyé par le bon auteur sans alteration par un tiers

Propriétés du DRA (double ratchet algorithm)

✅ Chiffrement de bout-en-bout

Les messages passant par le système ne sont lisible que d'un bout à l'autre du système.

✅ Authentification

Le message a bien été envoyé par le bon auteur sans alteration par un tiers

🆕 Confidentialité de transmission

Chaque message a une clé **unique.**

Lit. : Handbook of applied cryptography (1997)

🆕 Confidentialité persistente

La compromission d'un message ne compromet pas l'ensemble de la conversation

Lit. : On post compromise security (2016) - department of Computer Science - University of Oxford

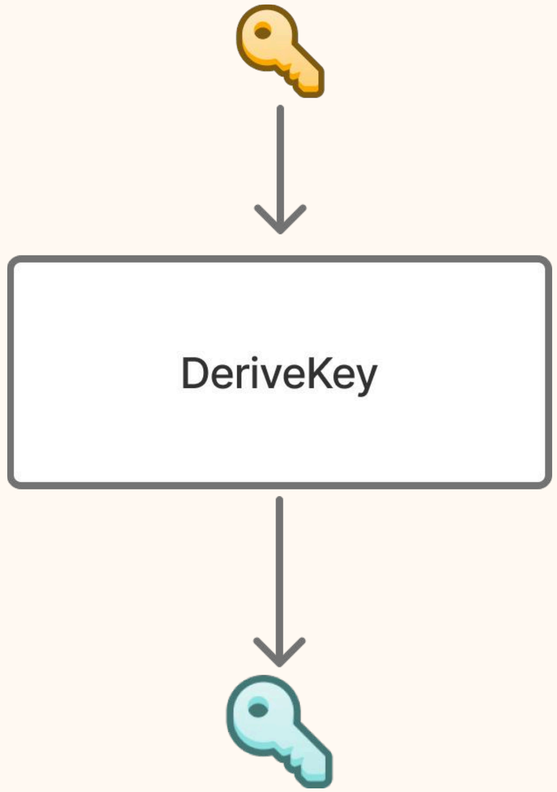
Source : Sofía Celi - [Cryptography Meetup] The double-ratchet algorithm: its security and privacy.

Confidentialité de transmission (backward secrecy)

🆕 Confidentialité de transmission

Chaque message a une clé **unique.**

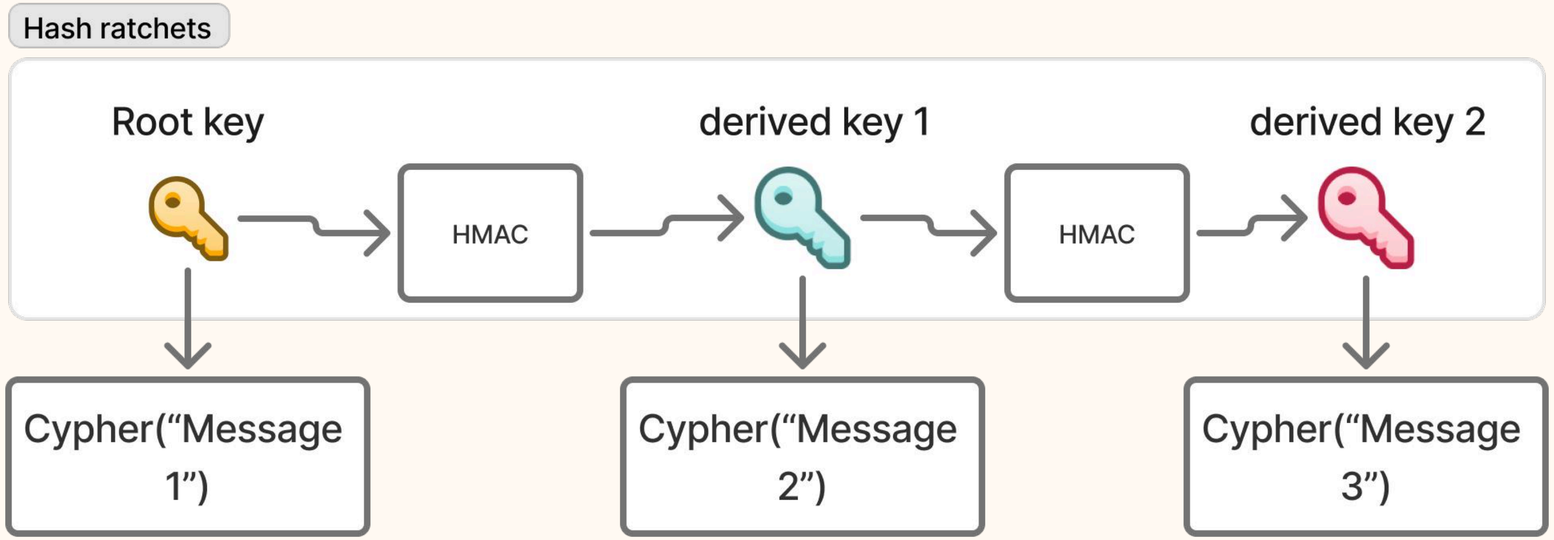
- **DeriveKey = Hash**



Confidentialité de transmission - Hash ratchet

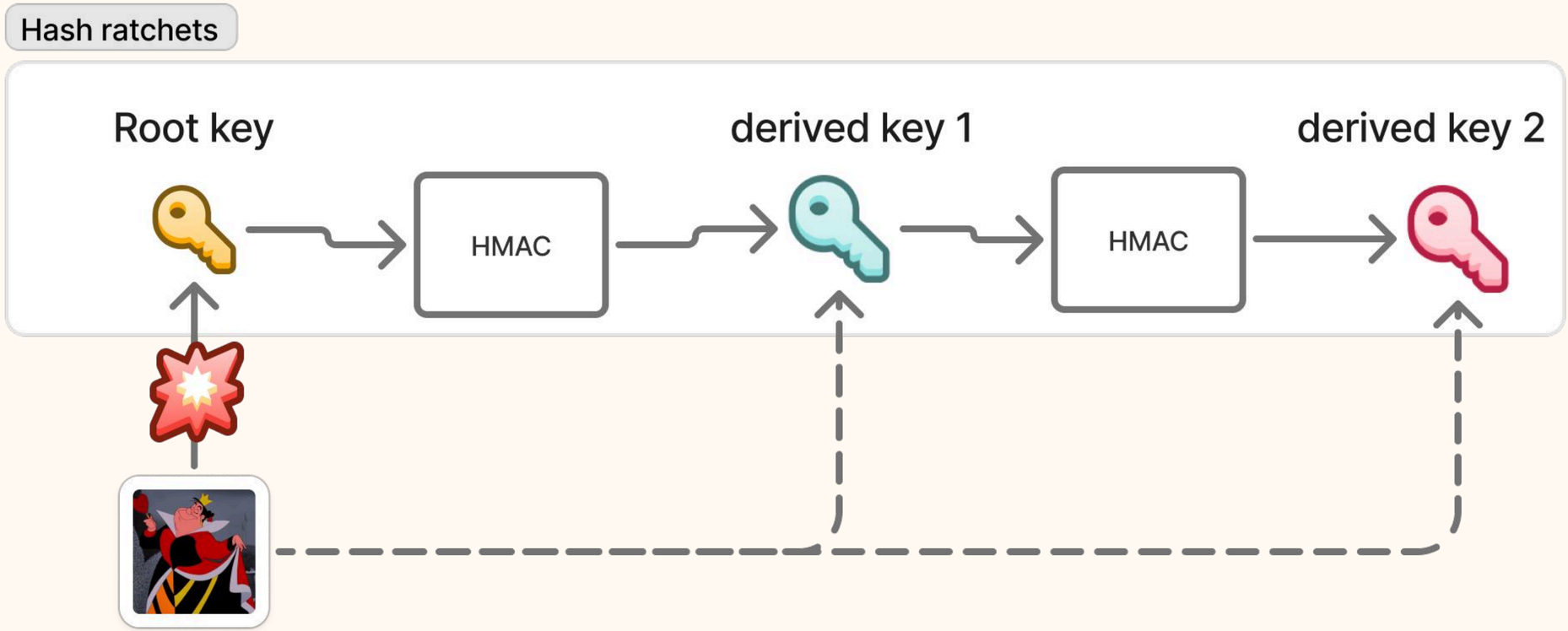
🆕 Confidentialité de transmission

Chaque message a une clé **unique.**



Source: signal DRA specification

Confidentialité de transmission - Hash ratchet

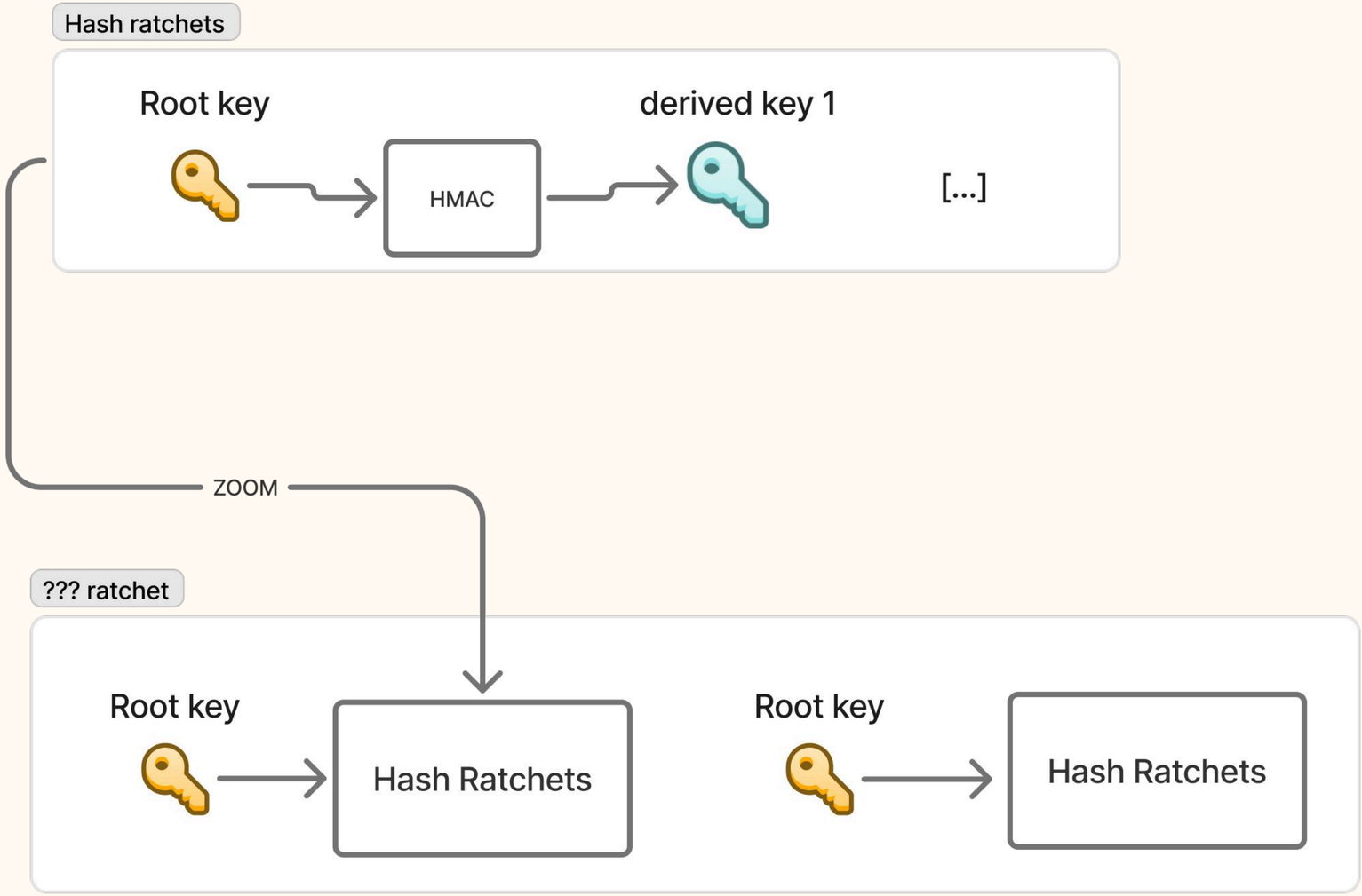


Source: signal DRA specification

Confidentialité persistente (post-compromise security)

🆕 Confidentialité persistente

La compromission d'un message ne compromet pas l'ensemble de la conversation

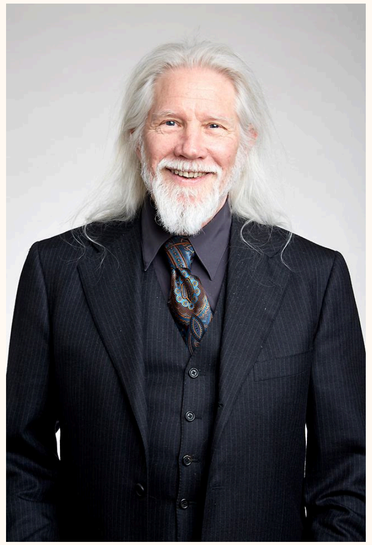


Source: signal DRA specification

Problématique :

- Définir un **secret commun** de façon **sécurisée**
- Secret commun à la base de la chaîne clé

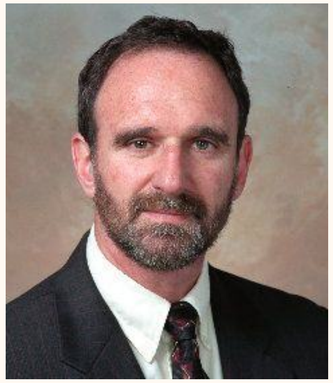
Diffie Hellman - Flashback !!!



Whitfield Diffie

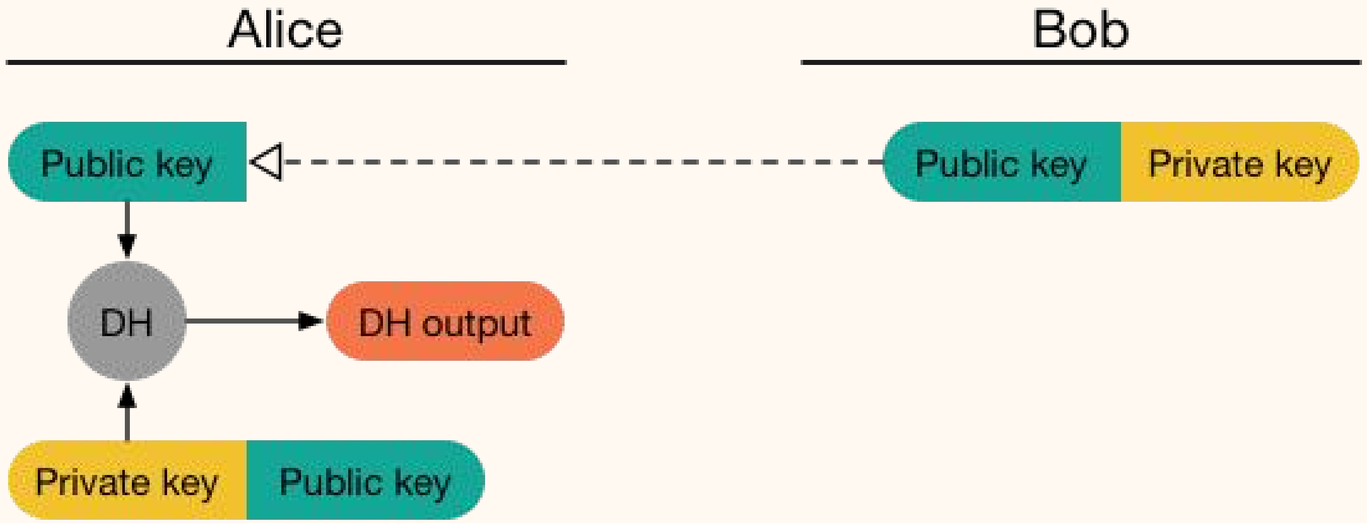
Objectif :

- Définir un **secret commun** de façon **sécurisée**
- Secret commun ⇒ clé de chiffrement symétrique



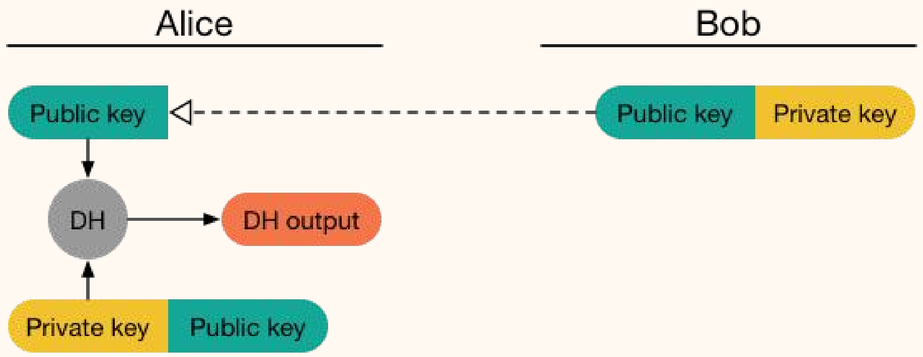
Martin Hellman

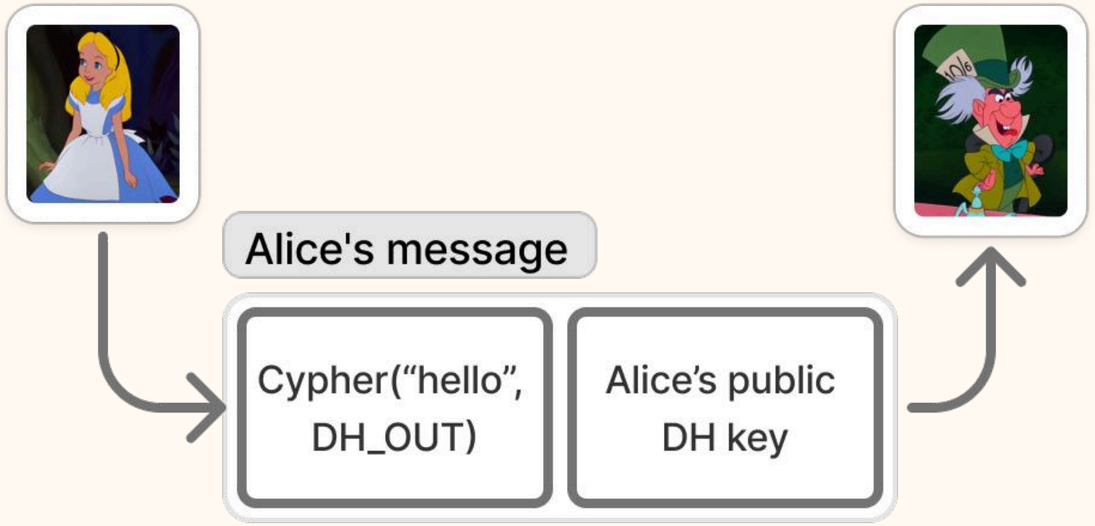
Diffie Hellman ratchet



Source: signal DRA specification

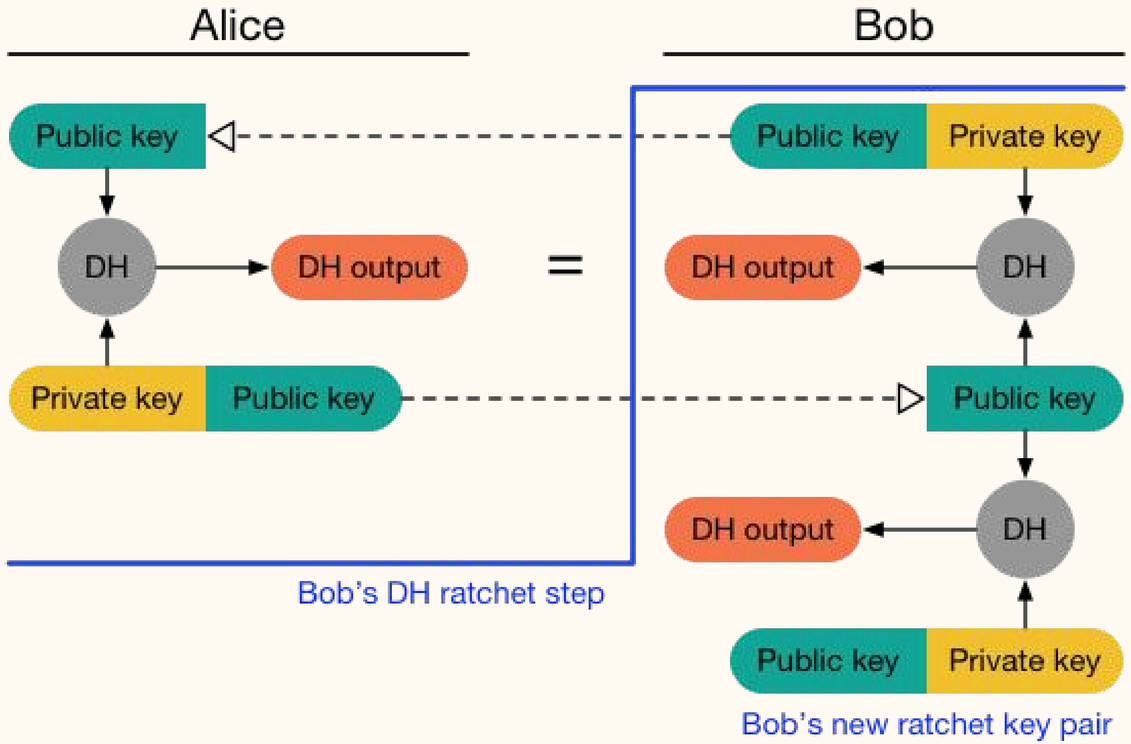
Diffie Hellman ratchet





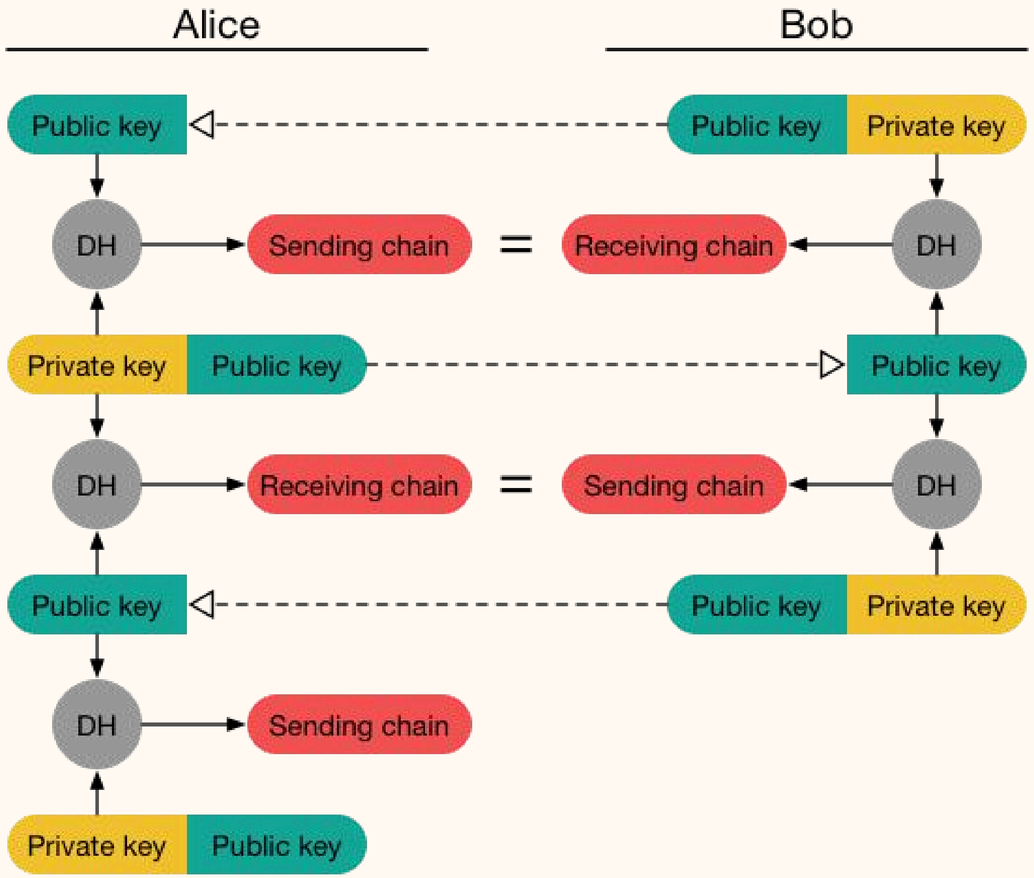
Source: signal DRA specification

Diffie Hellman ratchet

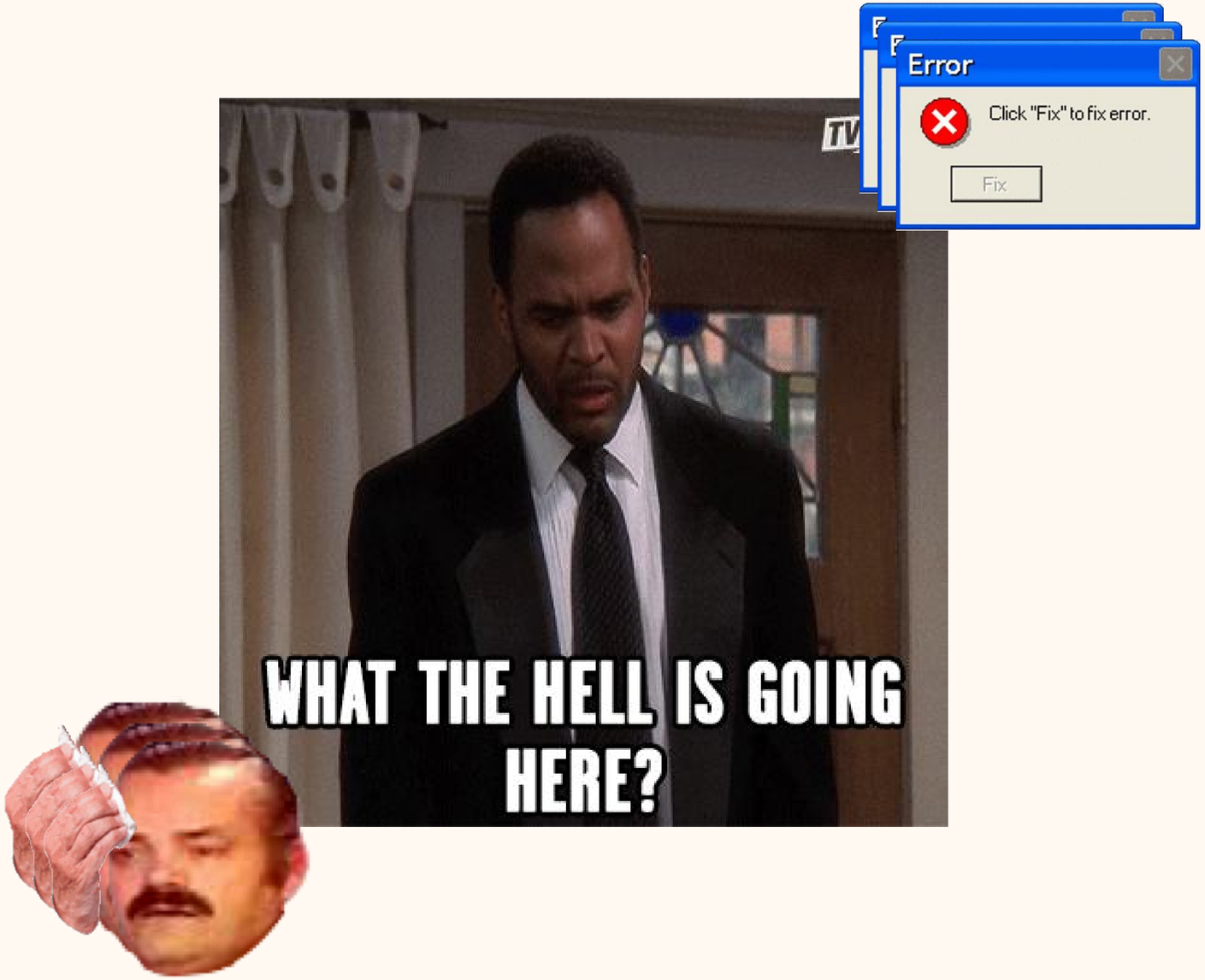


Source: signal DRA specification

Diffie Hellman ratchet



Source: signal DRA specification


Error
Click "Fix" to fix error.
Fix
WHAT THE HELL IS GOING HERE?

Deep dive

alice and bob entered the chat

Alice 03:25

Bonjour bob !!!!

Comment ça va ?

Bob 03:34

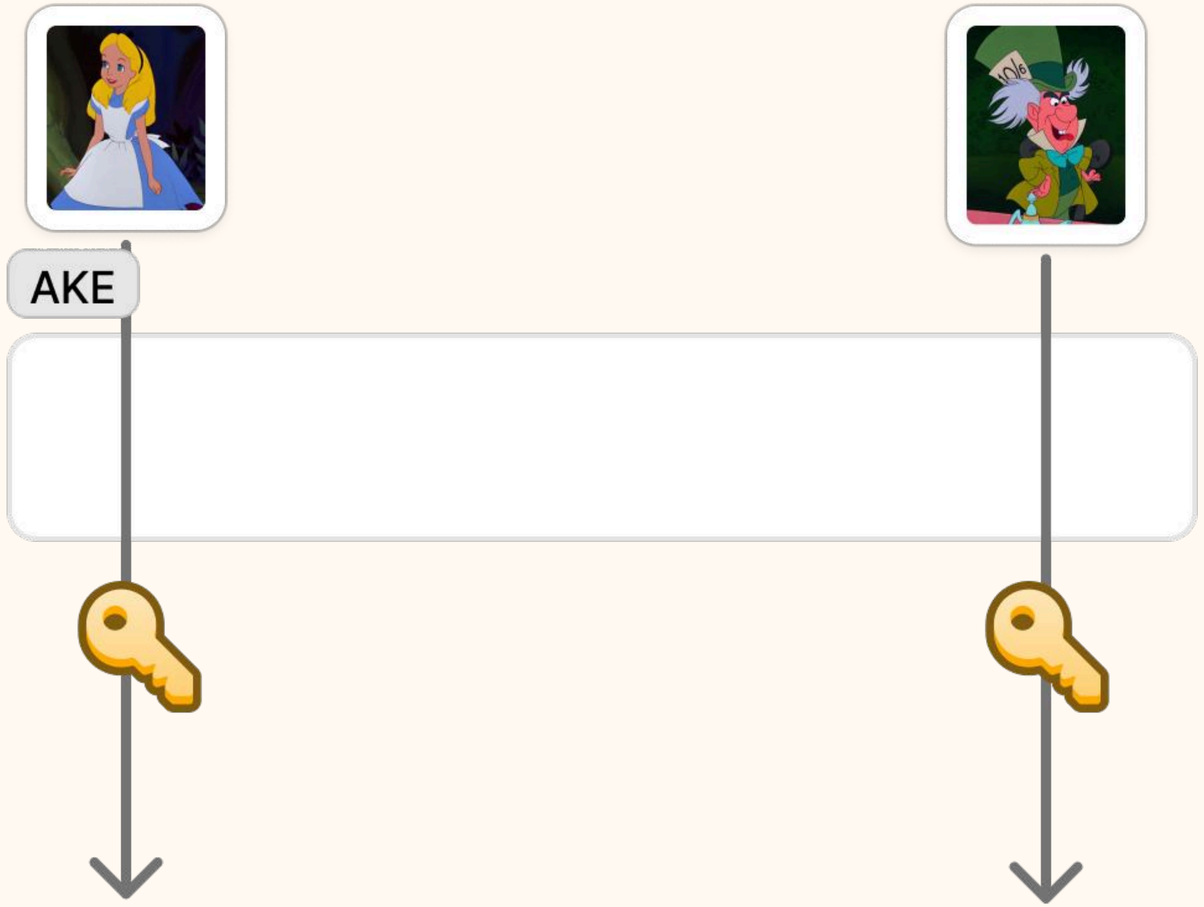
Trop bien et toi ?

Deep dive

Alice s’inscrit

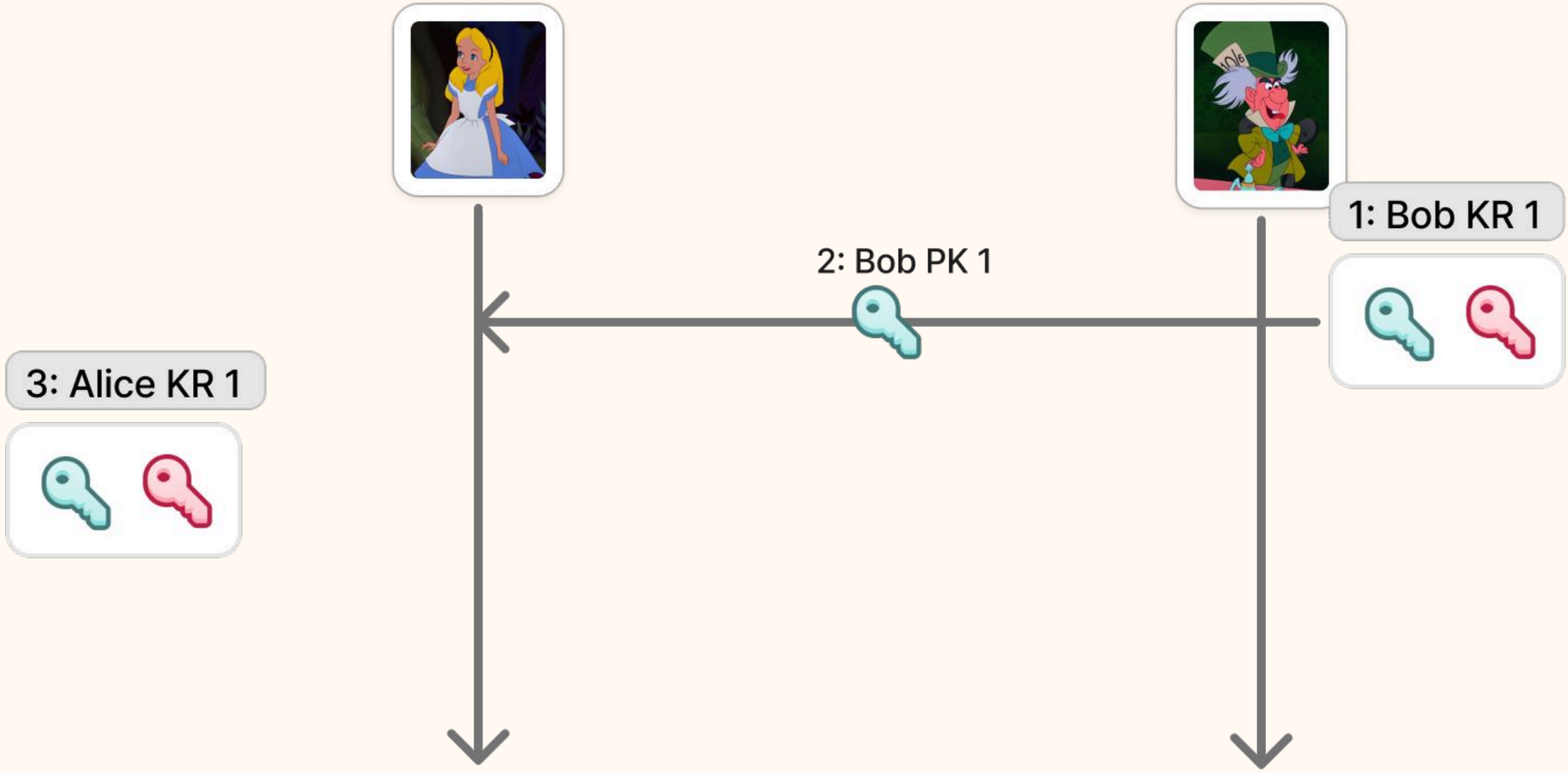
Deep dive

Alice et Bob entrent en contact - Authenticated key agreement



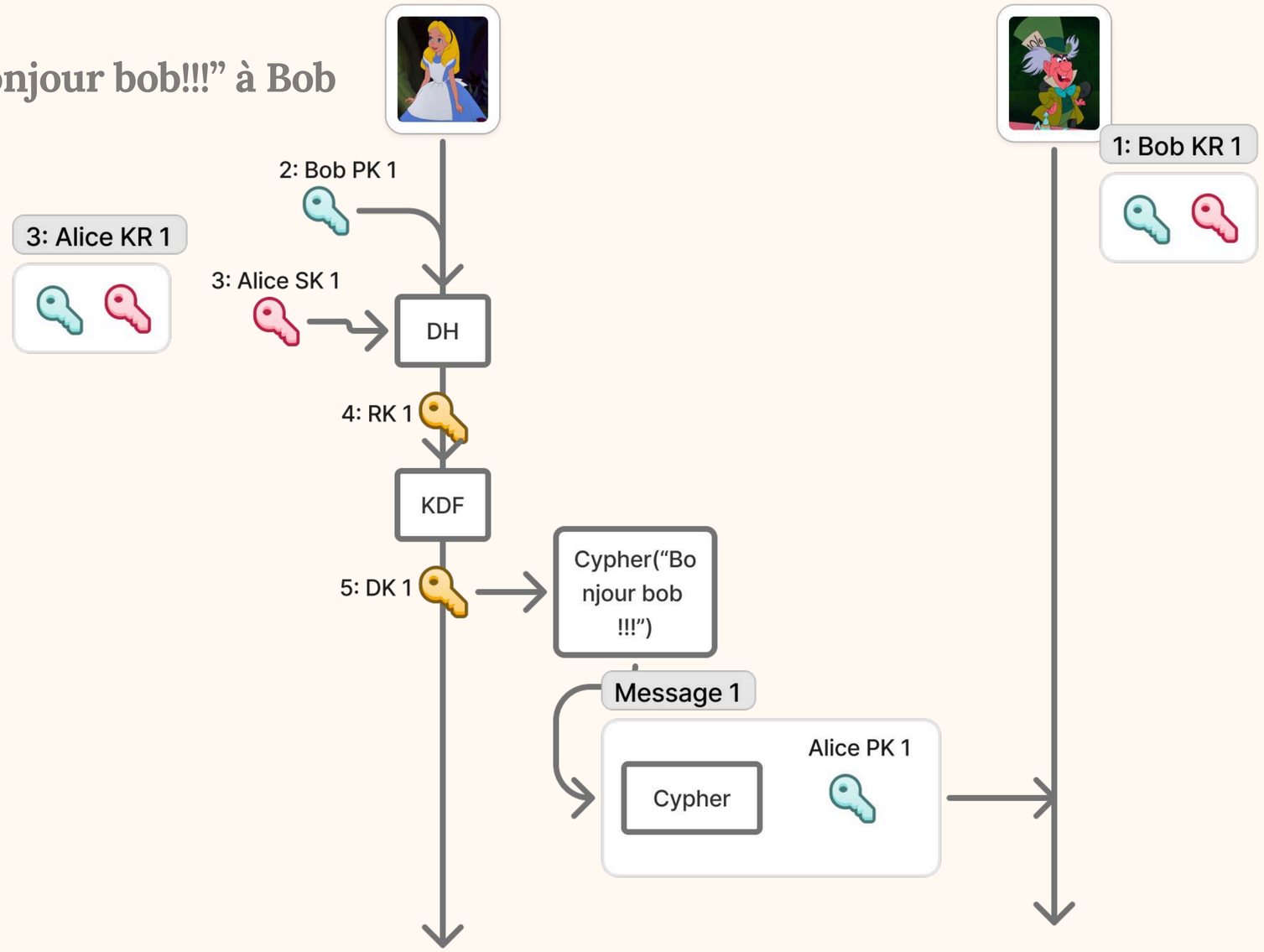
Deep dive

Alice et Bob entrent en contact - Diffie Hellman initial



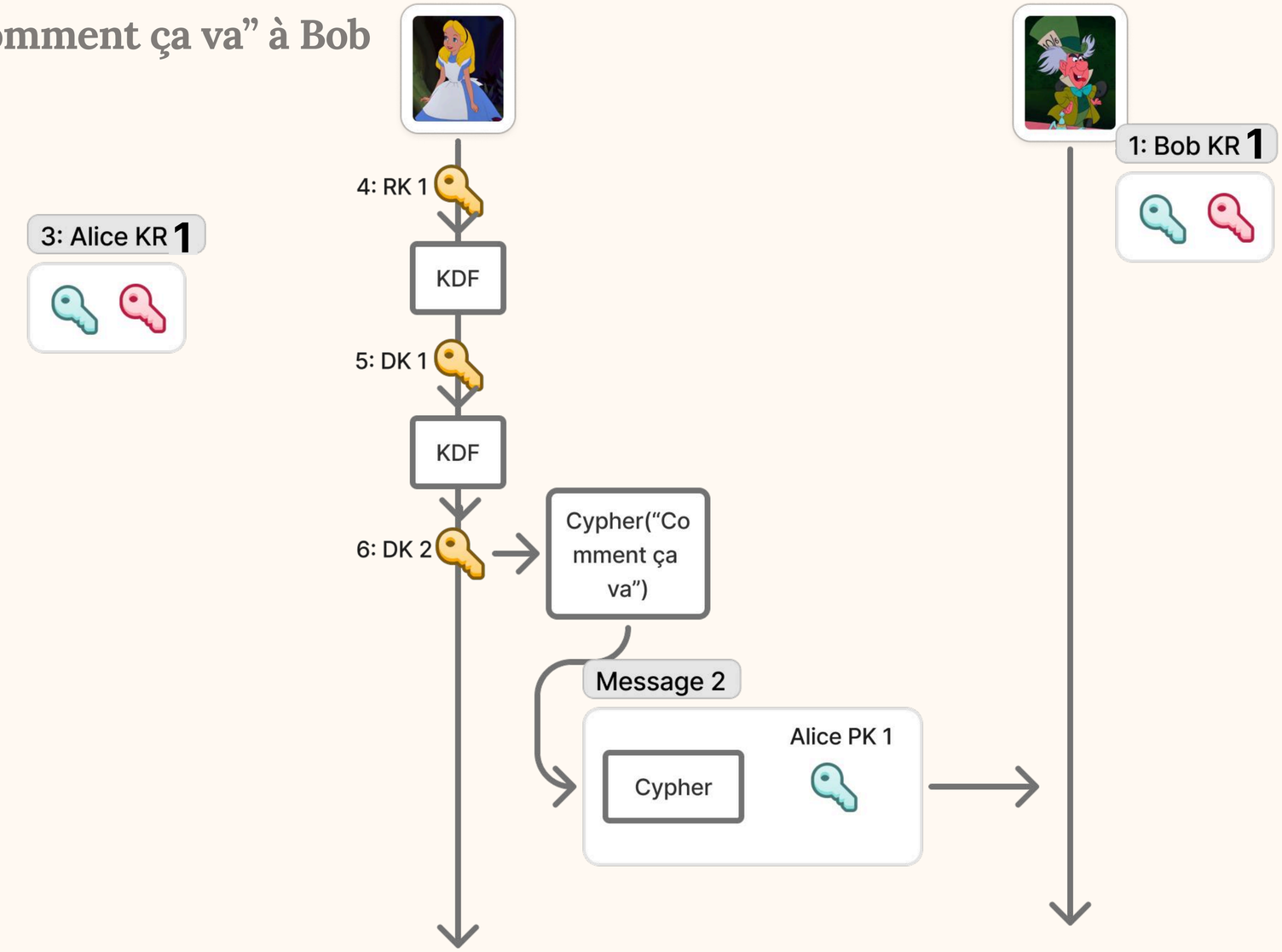
Deep dive

Alice envoie “Bonjour bob!!!” à Bob



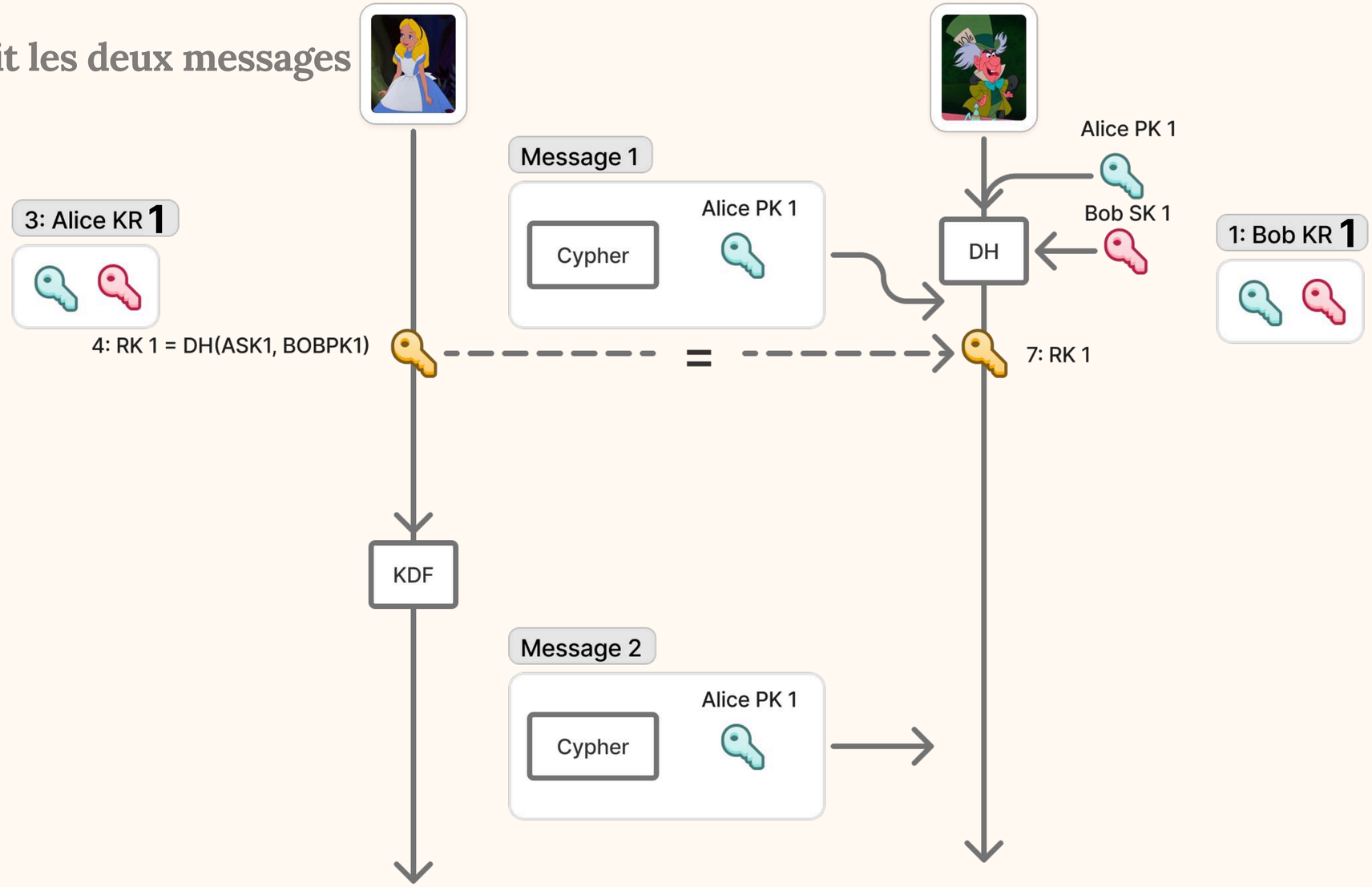
Deep dive

Alice envoie “Comment ça va” à Bob



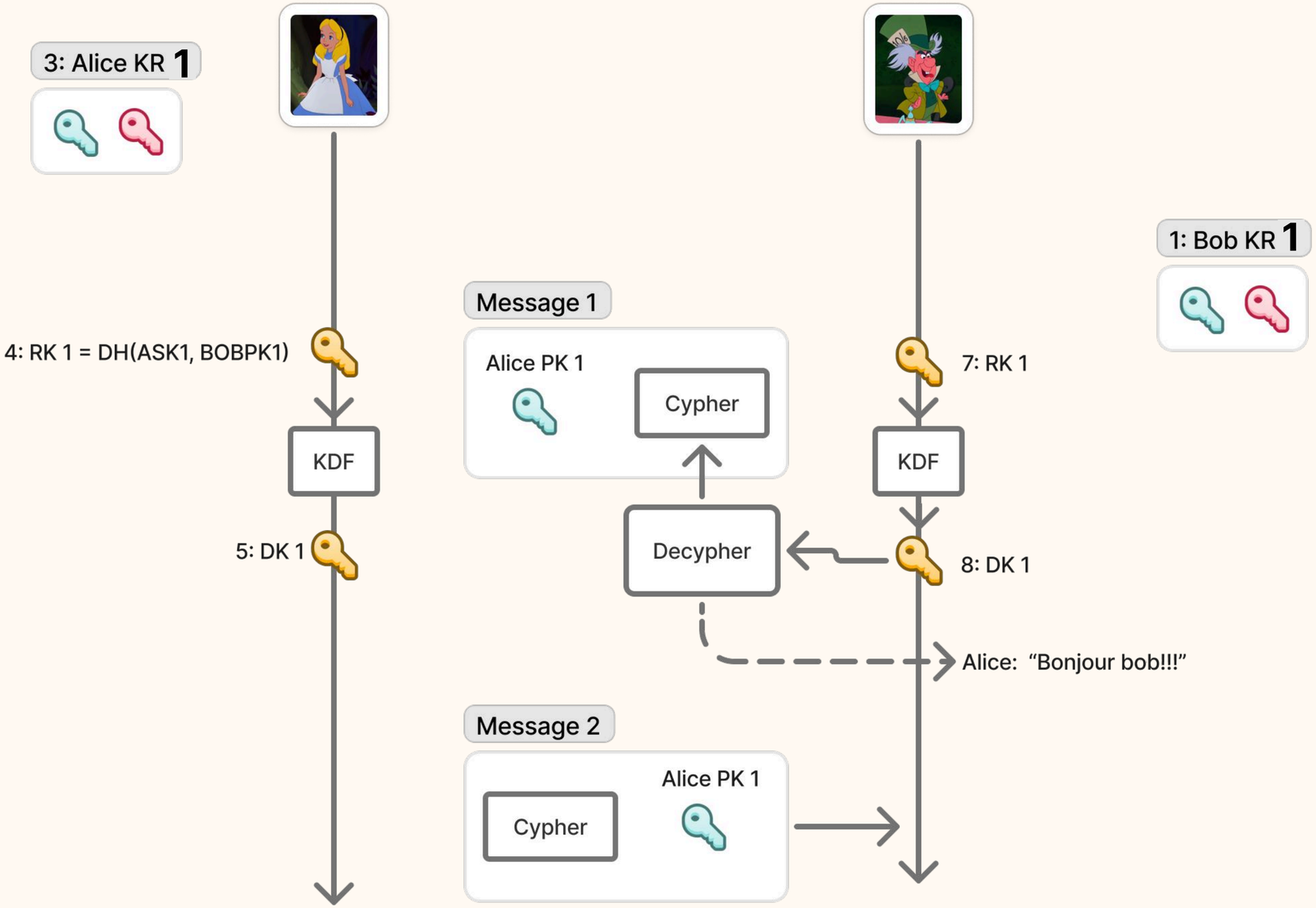
Deep dive

Bob reçoit les deux messages



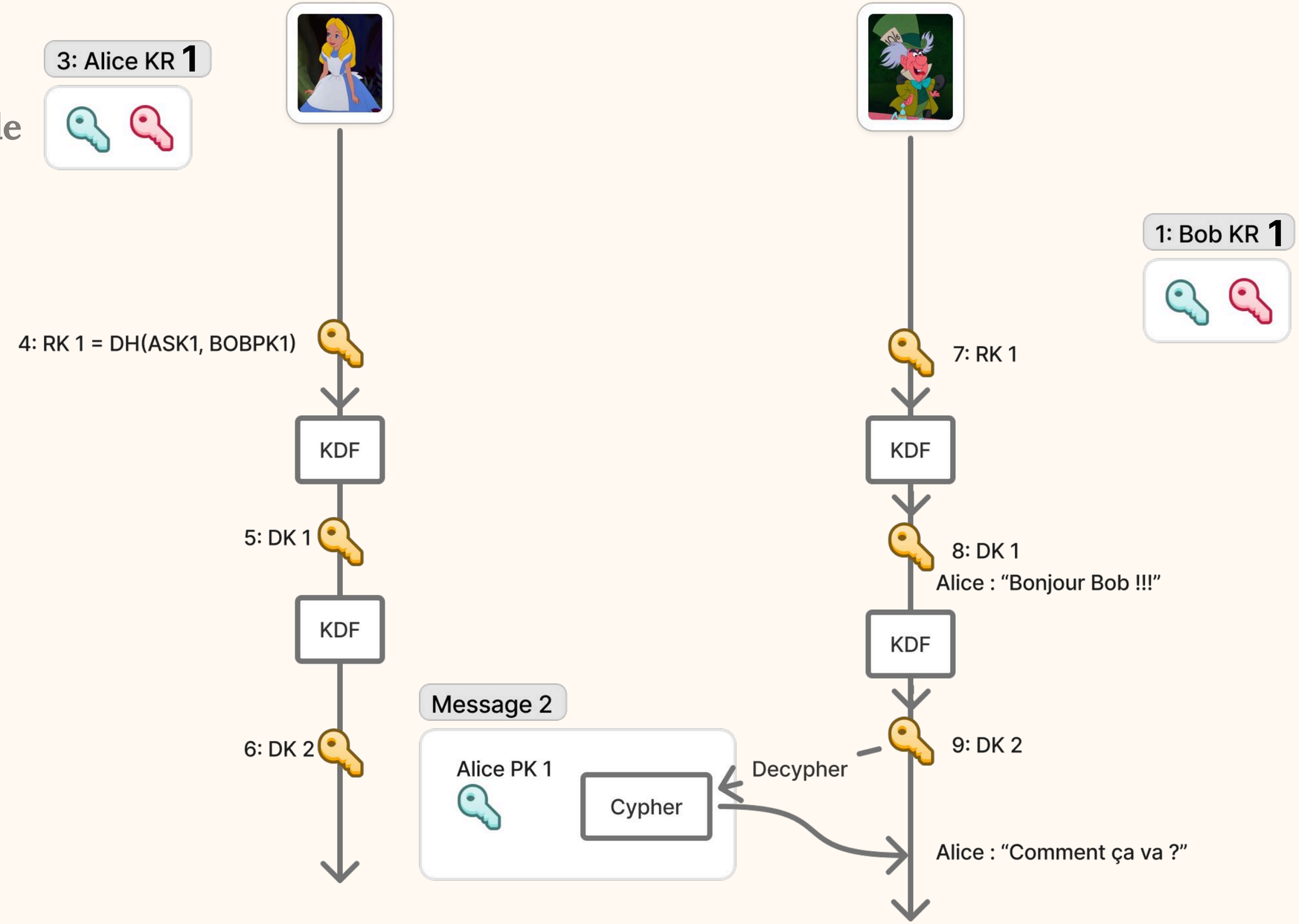
Deep dive

Bob déchiffre le premier message



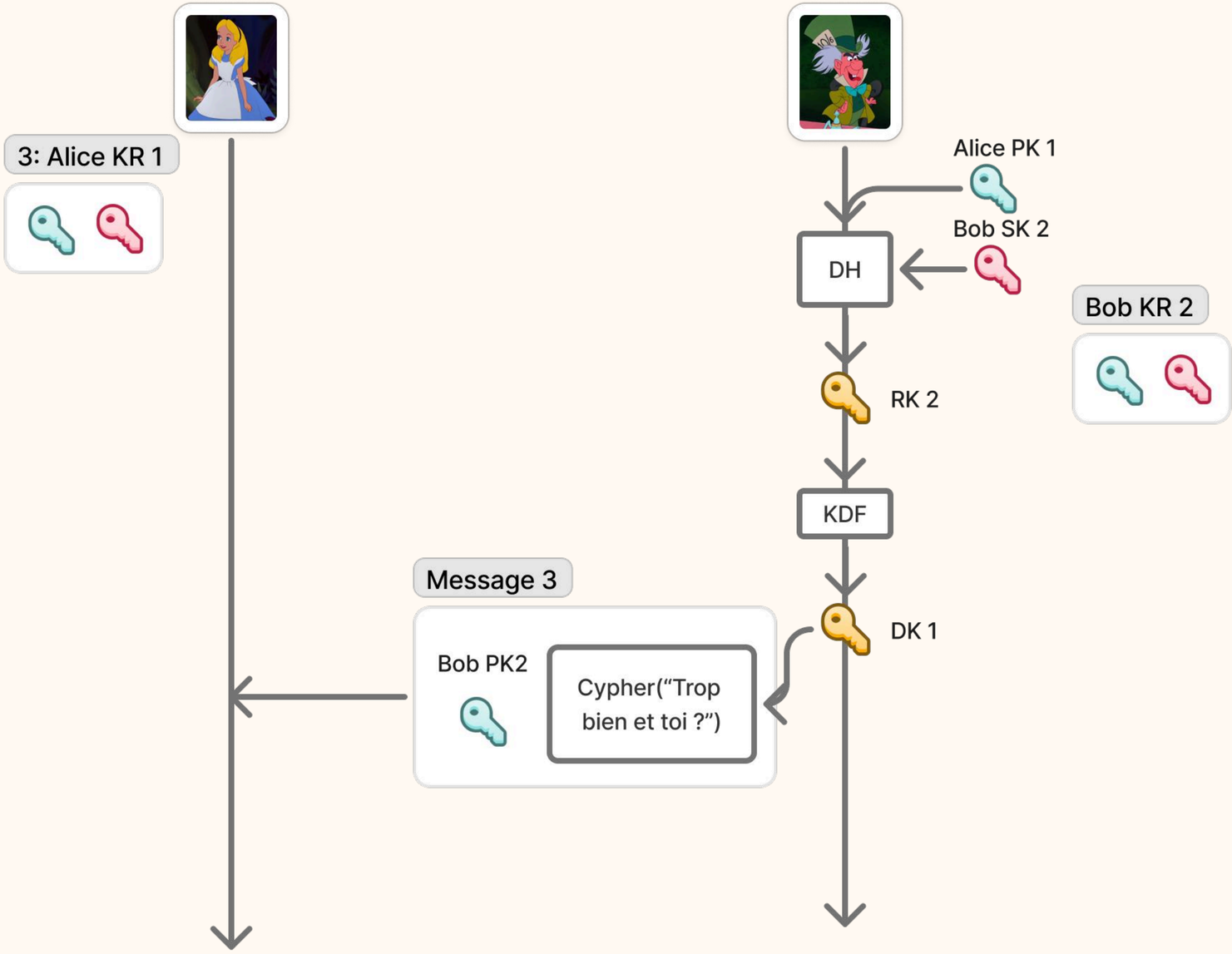
Deep dive

Bob déchiffre le deuxième message



Deep dive

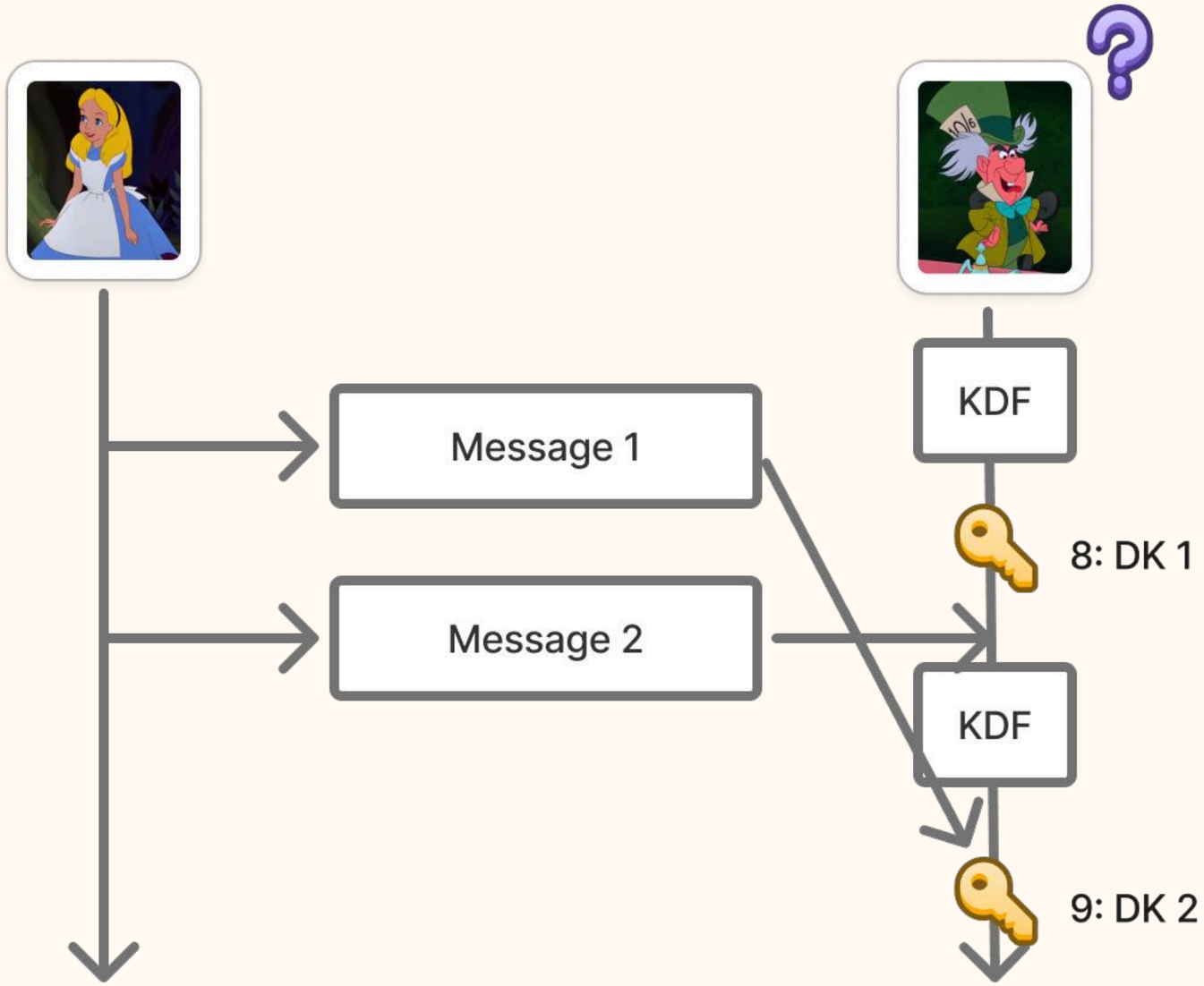
Bob envoie : “Trop bien et toi ?” à Alice



Le double ratchet algorithm n’est pas parfait 😿

1. Out of order messages
2. Seulement deux participants
3. Compromission temporaire possible

Out of order messages

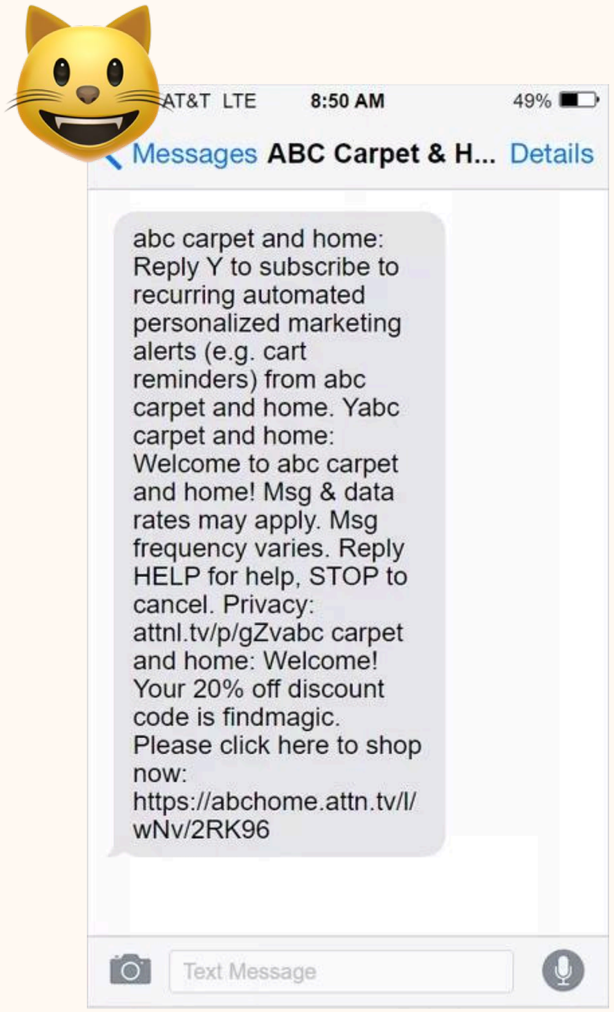


Le double ratchet algorithm n’est pas parfait 😿

1. Out of order messages
2. Seulement deux participants
3. Compromission temporaire possible

Le double ratchet algorithm n’est pas parfait 😿

Compromission temporaire possible



Pour aller plus loin

Articles :

- Signal specification
- Proton specification
- Open PGP for devs
- How Diffie-Hellman Fails in Practice
- Matthew Green’s Blog

Talks

- How signal messaging protocol works
- How signal works
- The double-ratchet algorithm: its security and privacy.

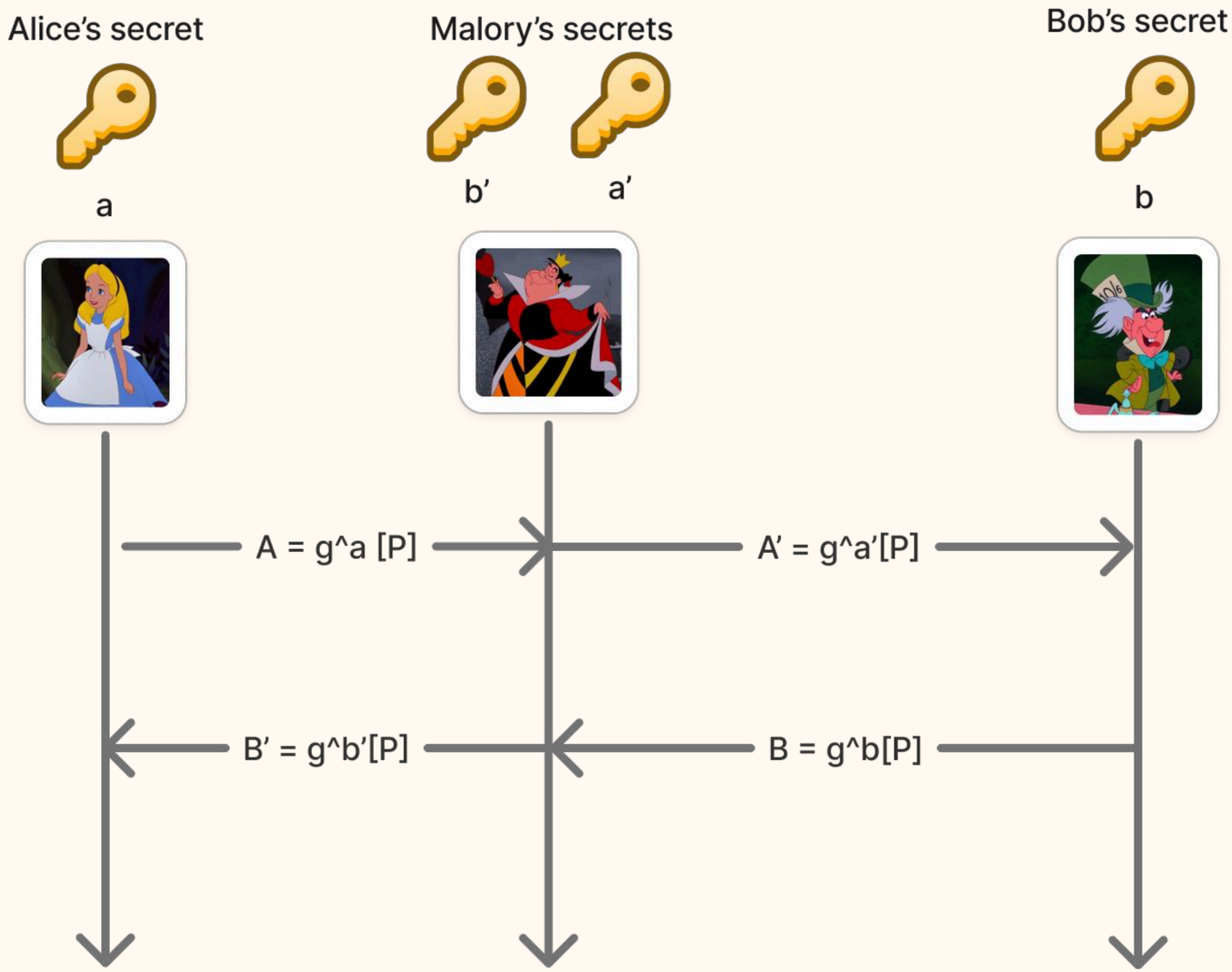
Merci !!!

Des questions ?

Annexes

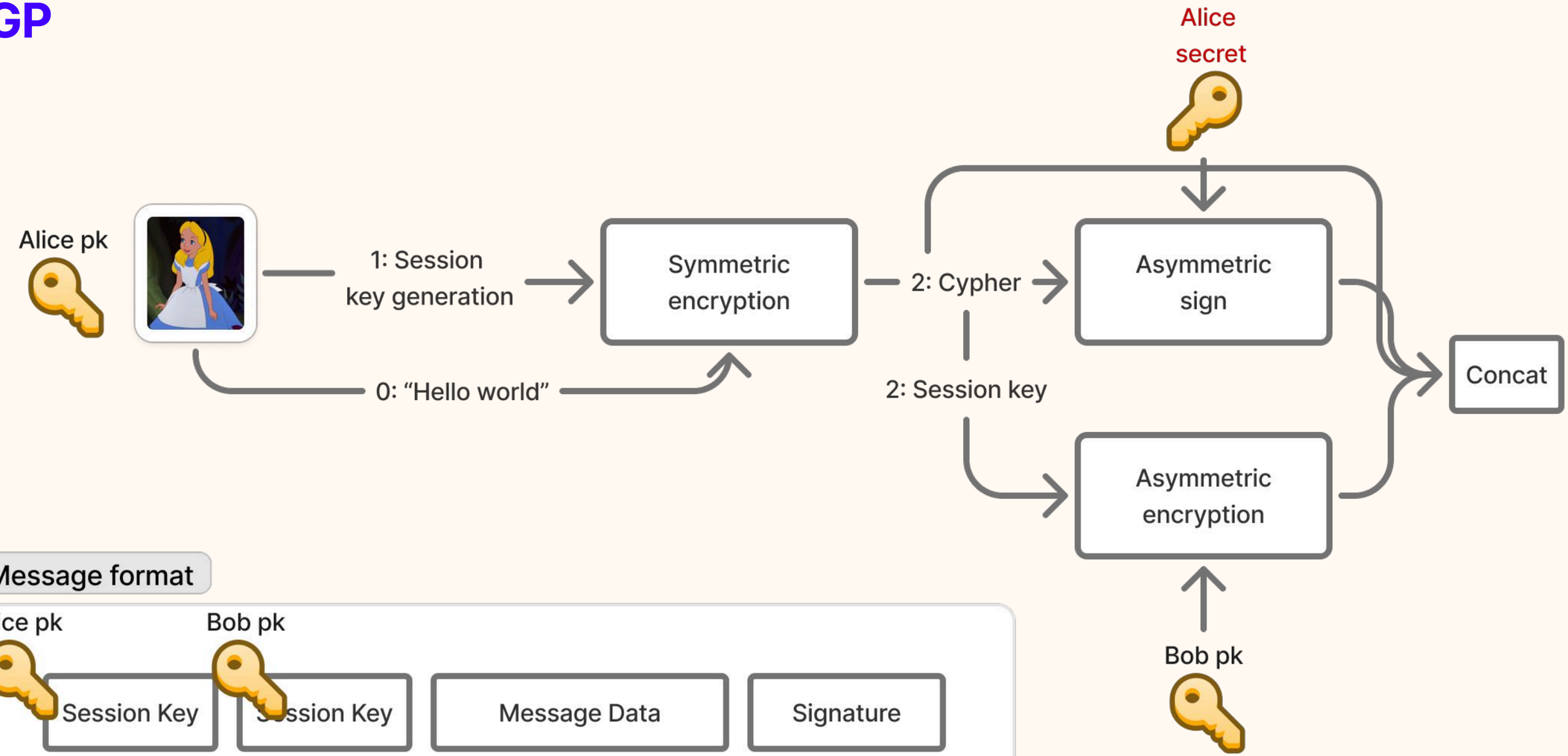
Parce que 50 minutes c’est court...

Attaque sur Diffie Hellman



Source : imperfect forward secrecy (David Adrian et a.l.)

PGP



Source: ProtonMail Security Features and Infrastructure