OpenPGP, GnuPG, et paranoïa

Jean-Benoist Leger

Mercredi 23 janvier 2018

Besoins

Dans un monde idéal

Quels serait l'intérêt de la cryptographie dans un monde où :

- personne n'est surveillé,
- aucune identité n'est usurpée,
- tous les groupes d'intérêt travaillent en harmonie,
- la garantie de la Loi suffit à préserver la Liberté,
- les étudiants travaillent sérieusement leurs UV.

Probablement, aucun.

Besoins

Dans le monde réel

Dans le monde réel, nous constatons que :

- nous sommes surveillés par ceux sensé garantir notre Liberté,
- nous sommes surveillés par des groupements d'intérêts,
- nos identités sont usurpés,
- nous sommes une cible, à titre collectif ou individuel.

La cryptographie offre certains moyens de se protéger et de se prémunir.

Besoins

Mais. . .

Et si « ***Je n'ai rien à cacher*** ».
Je vais vous demander de :

- publier l'**intégralité** de votre correspondance privée,
- des manière définitive et **irrévocable**.

Besoins

Bilan

- La paranoïa n'est qu'une forme de prudence.
- Trop prudents jamais nous ne seront.
- Nous pouvons regretter un manque de prudence, rarement un excès.
- Il faut évaluer un modèle de risque.
- Il ne faut trop dégrader l'utilisabilité.
- Il faut prendre conscience des risques, en accepter certains, se prémunir contre les autres.

Besoins

Limitations

- L'article 434-15-2 du code pénal dispose : *Est puni de trois ans d'emprisonnement et de 270 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.*
  Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 euros d'amende.
- Seul le contenu des communications pourra être protégée via OpenPGP. D'autres moyens existent pour protéger l'existence des communications.

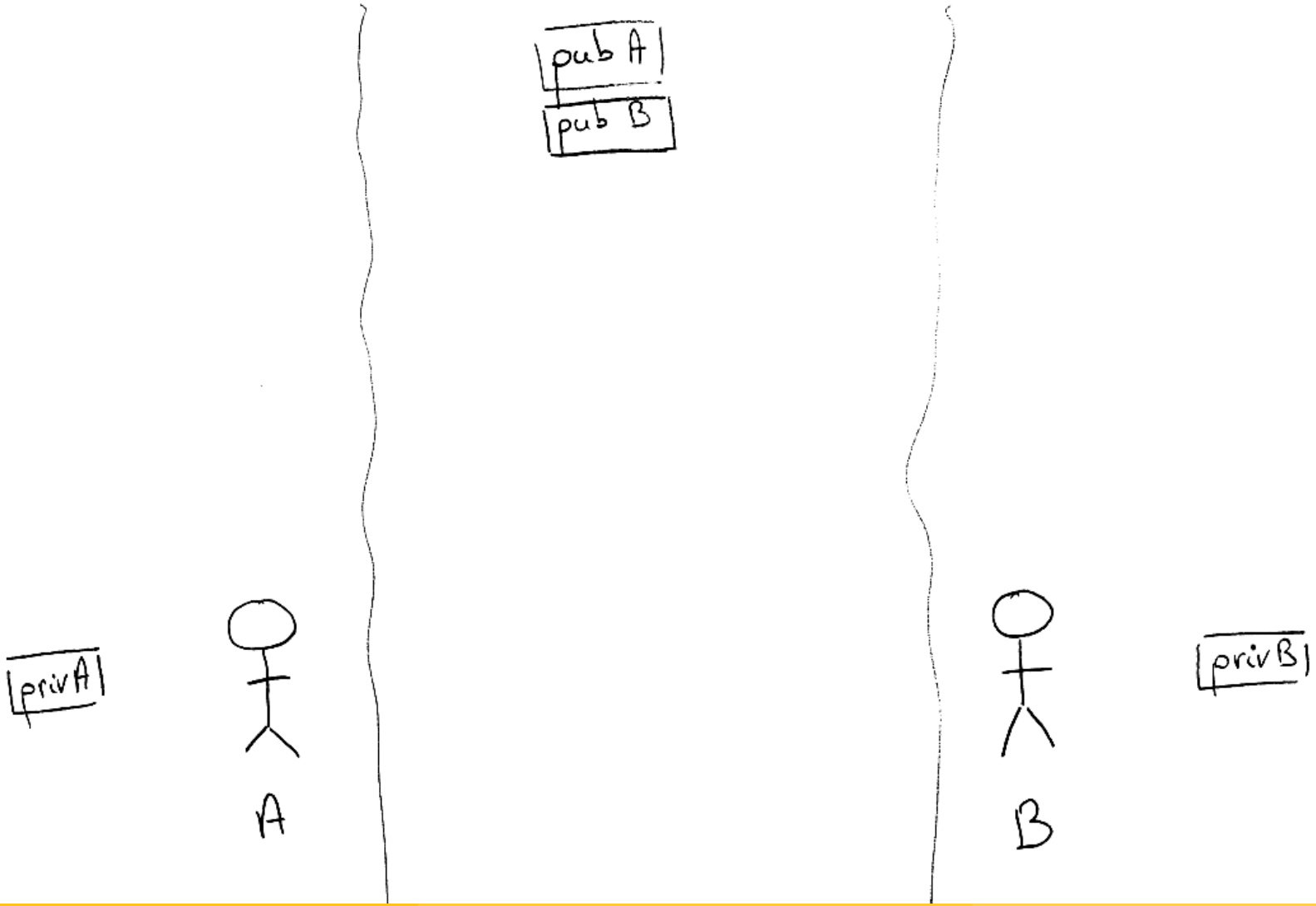
Cryptographie asymétrique

Utilité

- En cryptographie symétrique : autant de clef que de couples de correspondants.
- En cryptographie asymétrique : autant de paires de clefs que de correspondants.

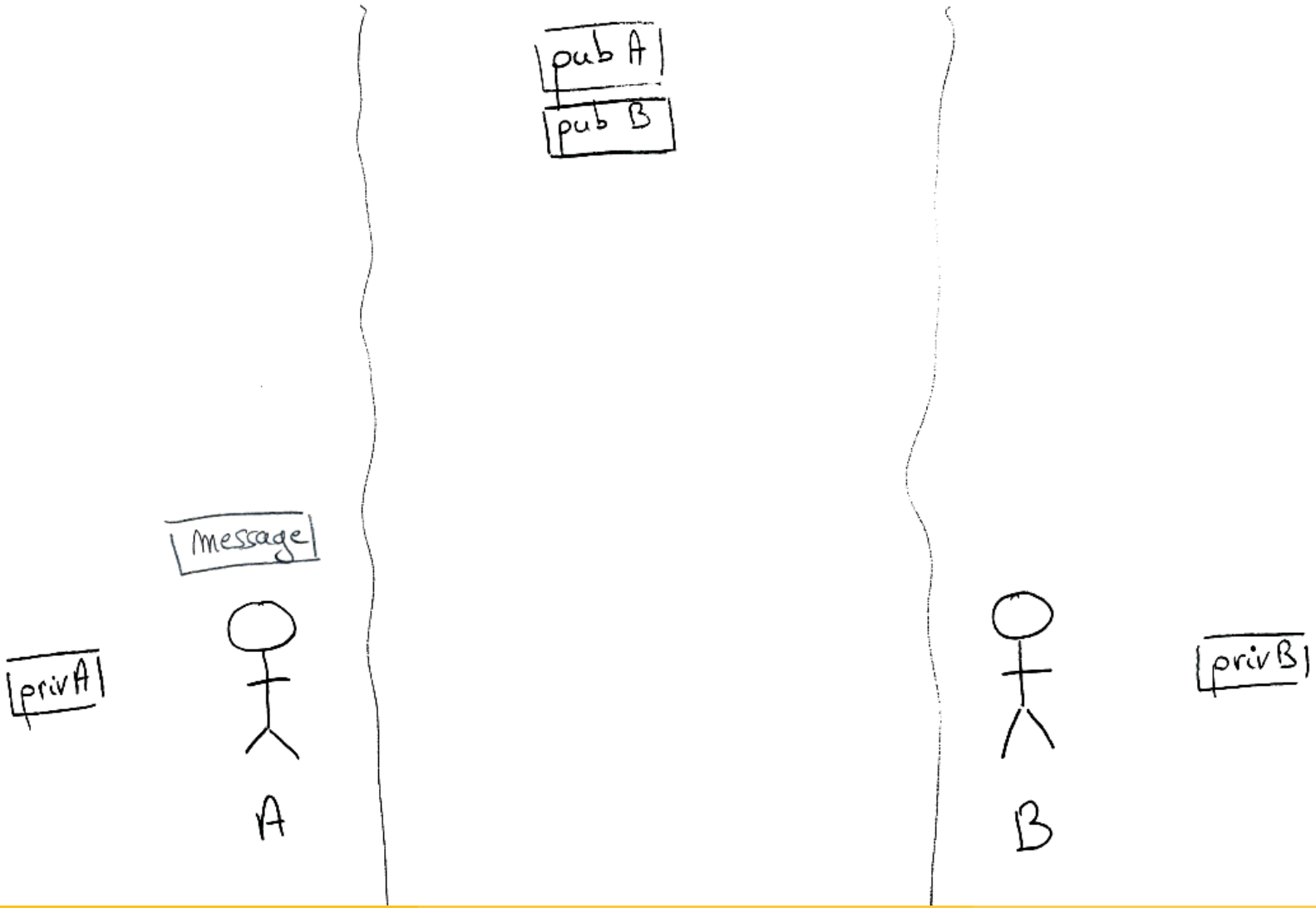
Cryptographie asymétrique

Principe



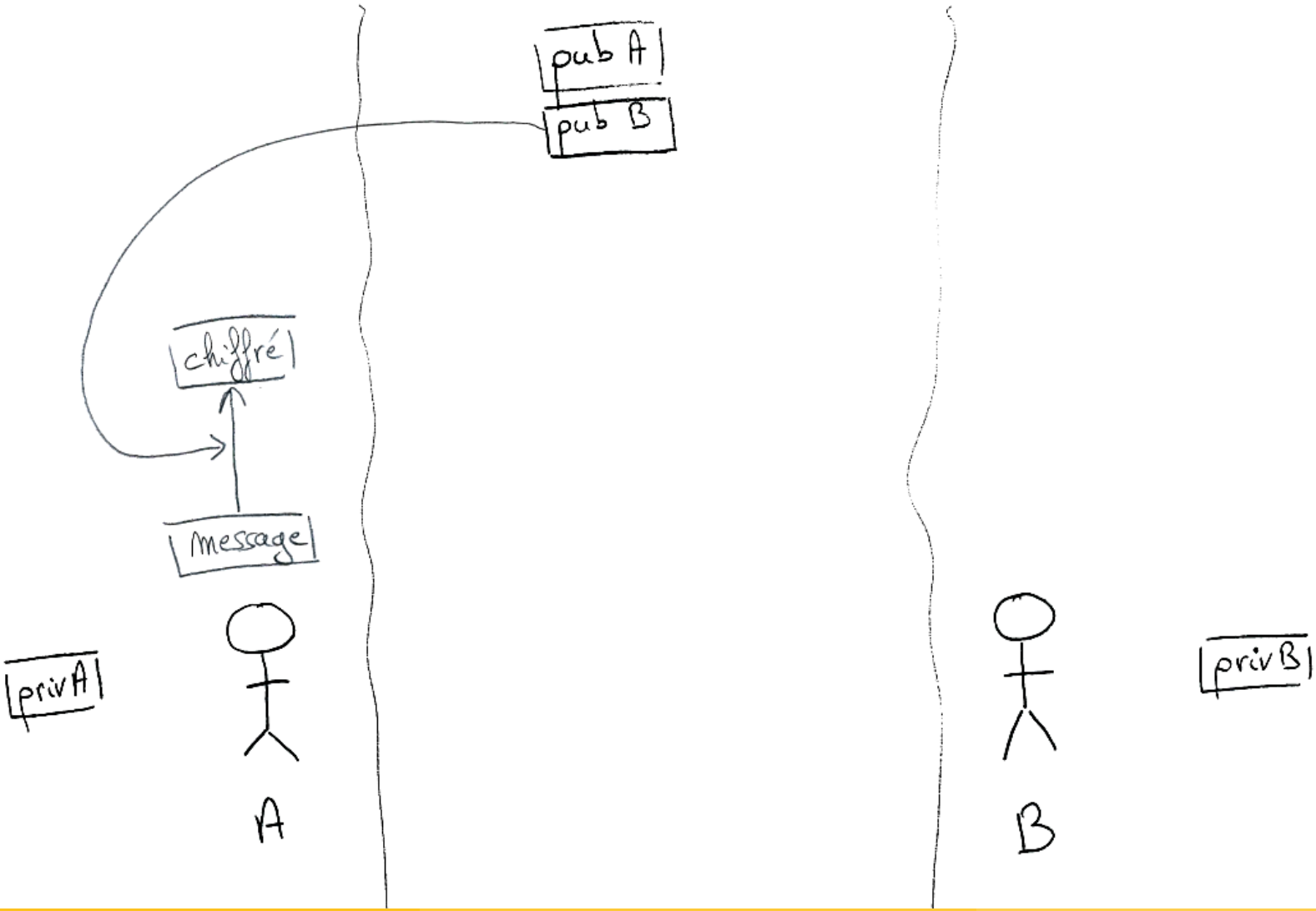
Cryptographie asymétrique

Principe



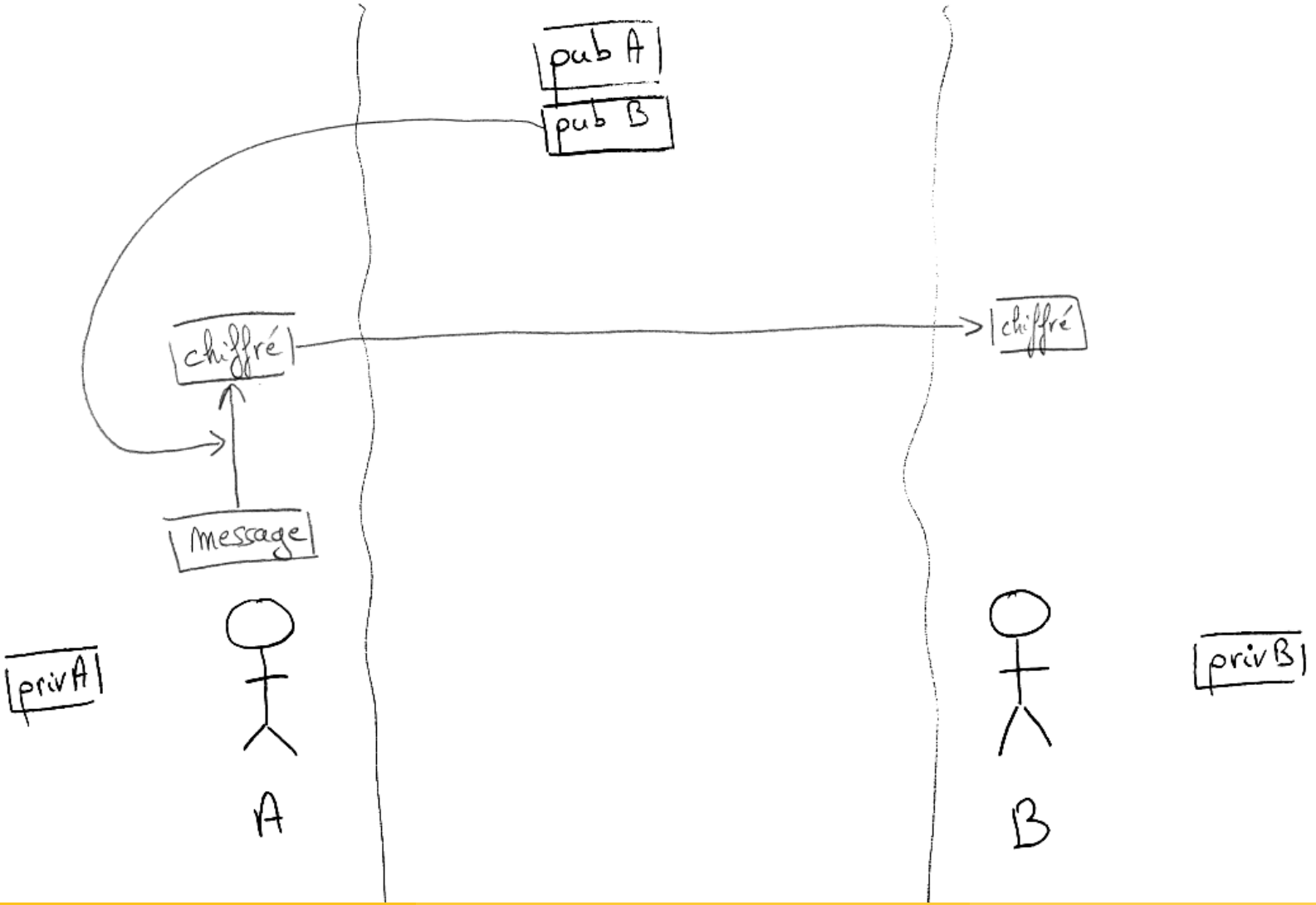
Cryptographie asymétrique

Principe



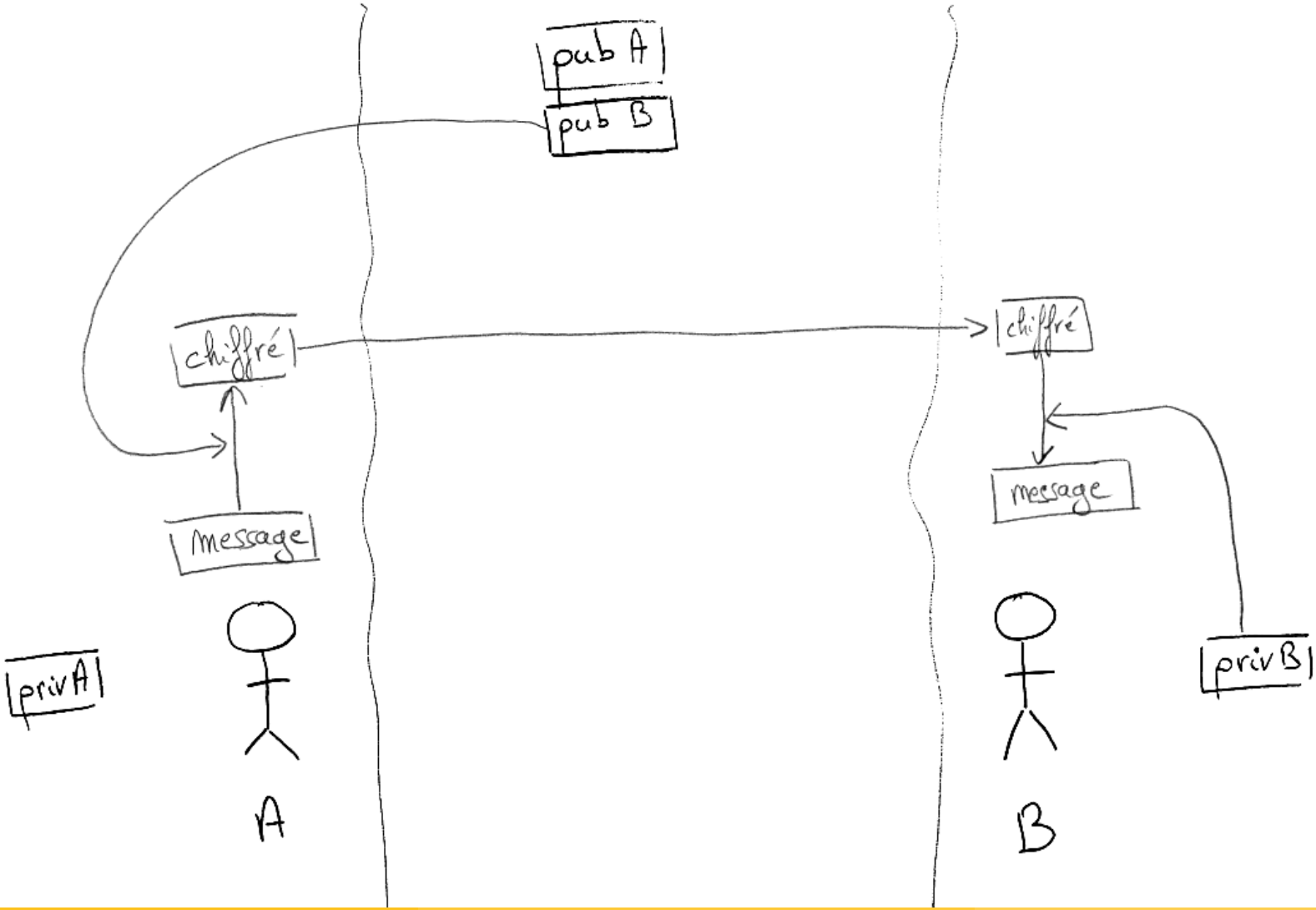
Cryptographie asymétrique

Principe



Cryptographie asymétrique

Principe



Cryptographie asymétrique
RSA

Les maths, c'est chiant (pour les étudiants), mais sur des slides, c'est très chiant (pour tout le monde cette fois).

Cryptographie asymétrique
RSA

La mise en pratique c'est encore mieux.

OpenPGP

Clef RSA

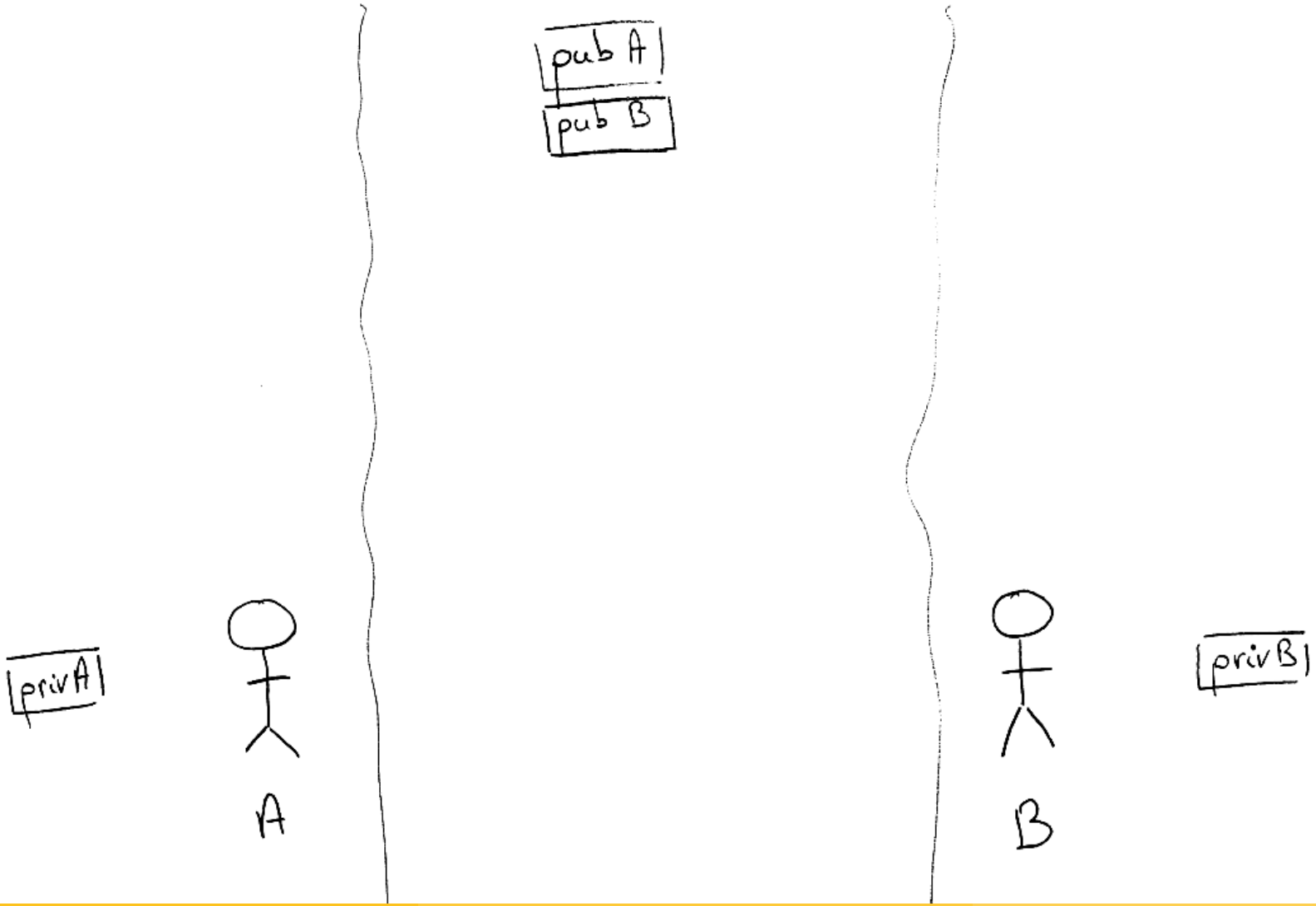
- La clef publique (au sens strict) est constitué de :
  - n,
  - e,
  - taille de la clef,
  - timestamp de génération.
- La clef privée est constitué de
  - la clef publique (au sens strict),
  - d,
  - p, q,
  - des valeurs précalculées.

Identification :

- fingerprint : Condensat SHA1 de la clef publique,
- identifiant : 4 derniers octets du fingerprint,
- identifiant long : 8 derniers octets du fingerprint.

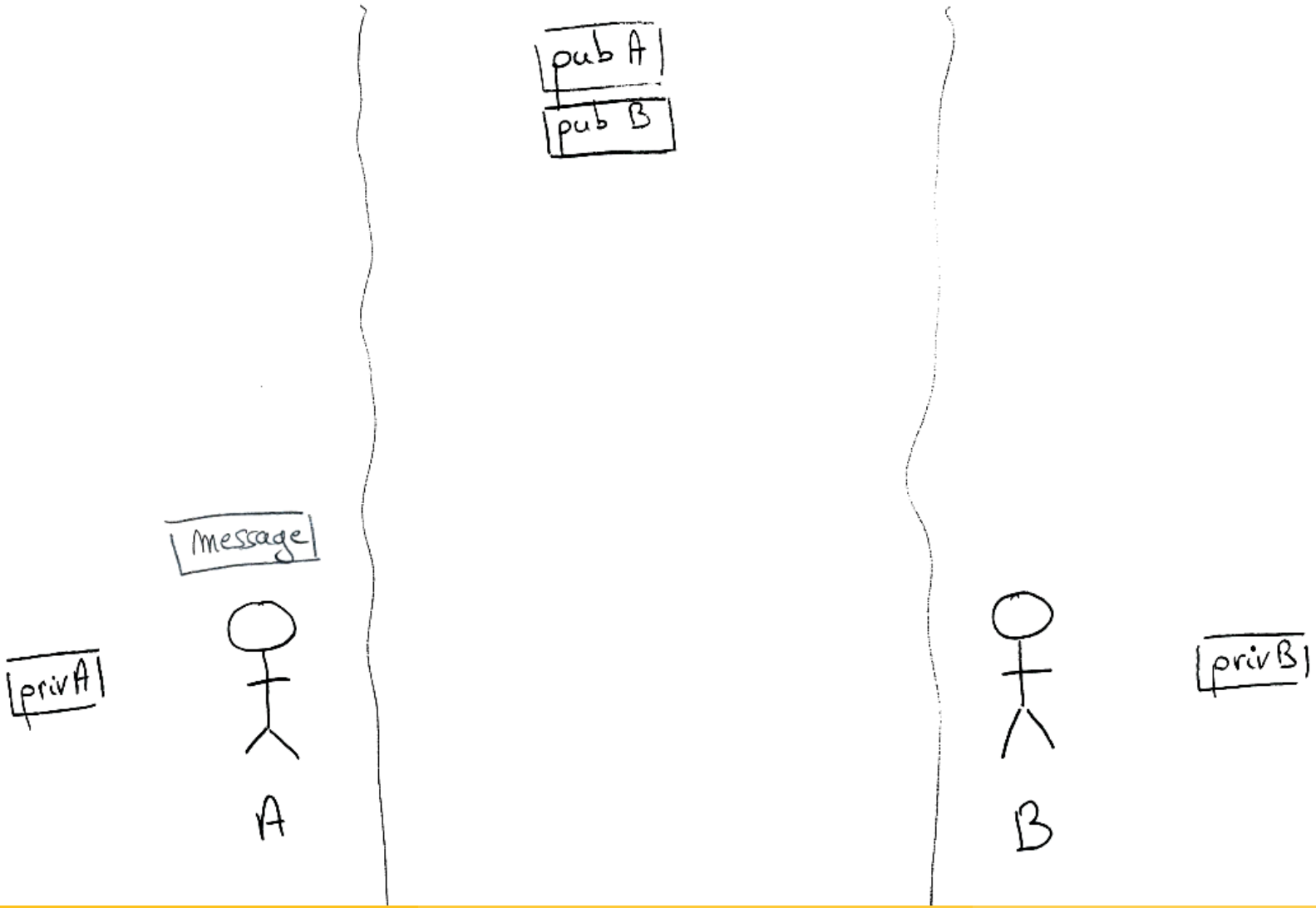
Cryptographie asymétrique

Chiffrement



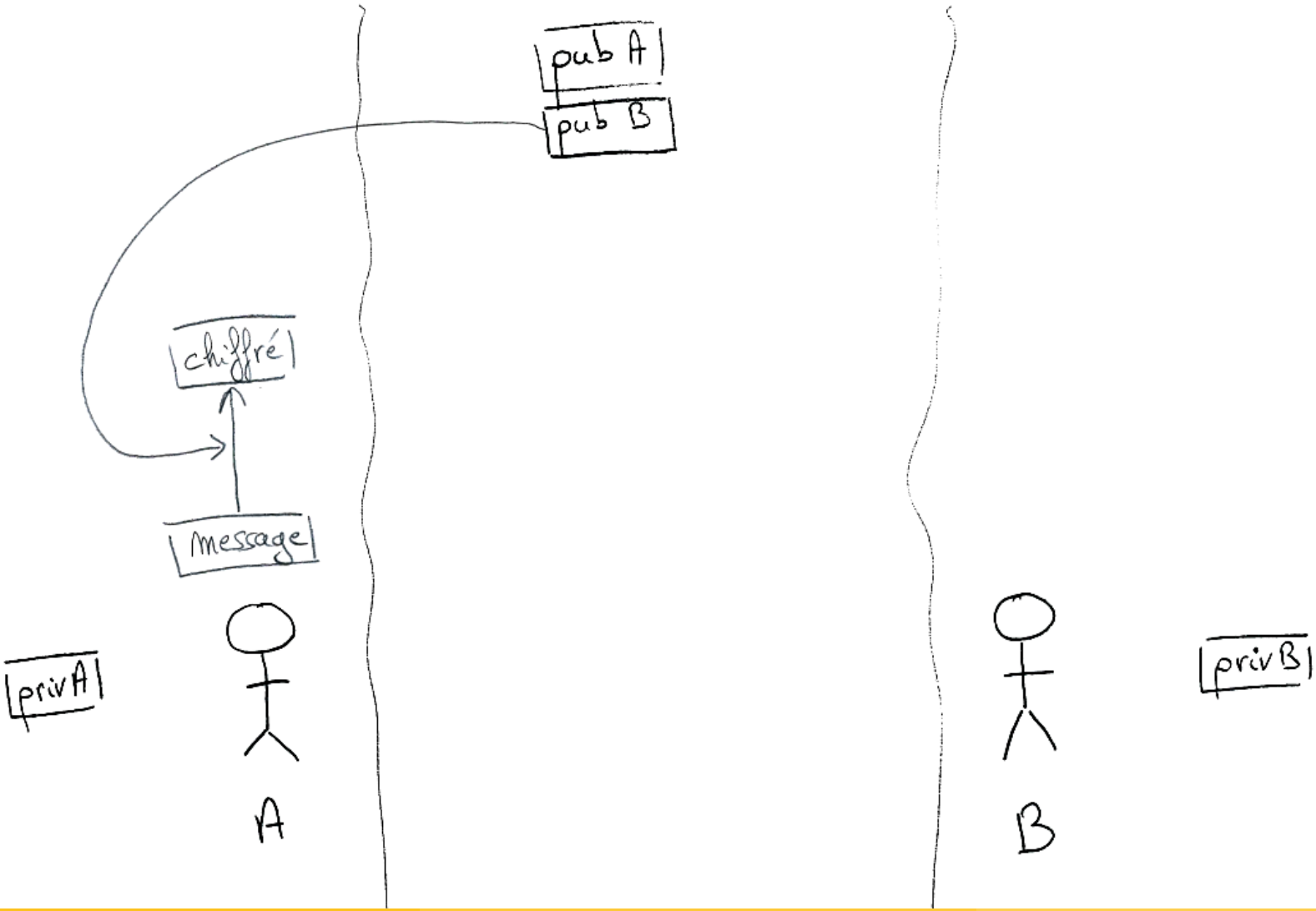
Cryptographie asymétrique

Chiffrement



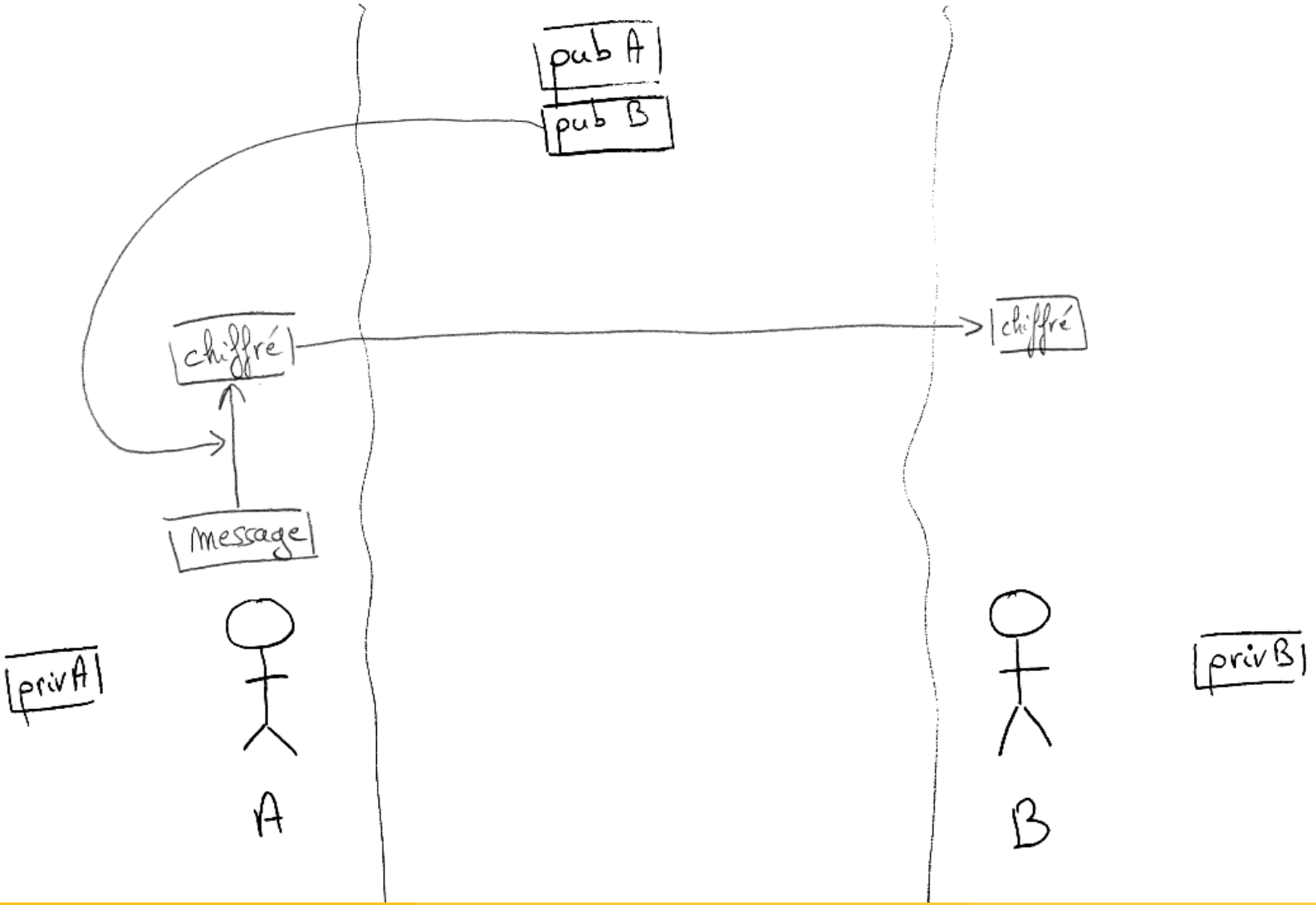
Cryptographie asymétrique

Chiffrement



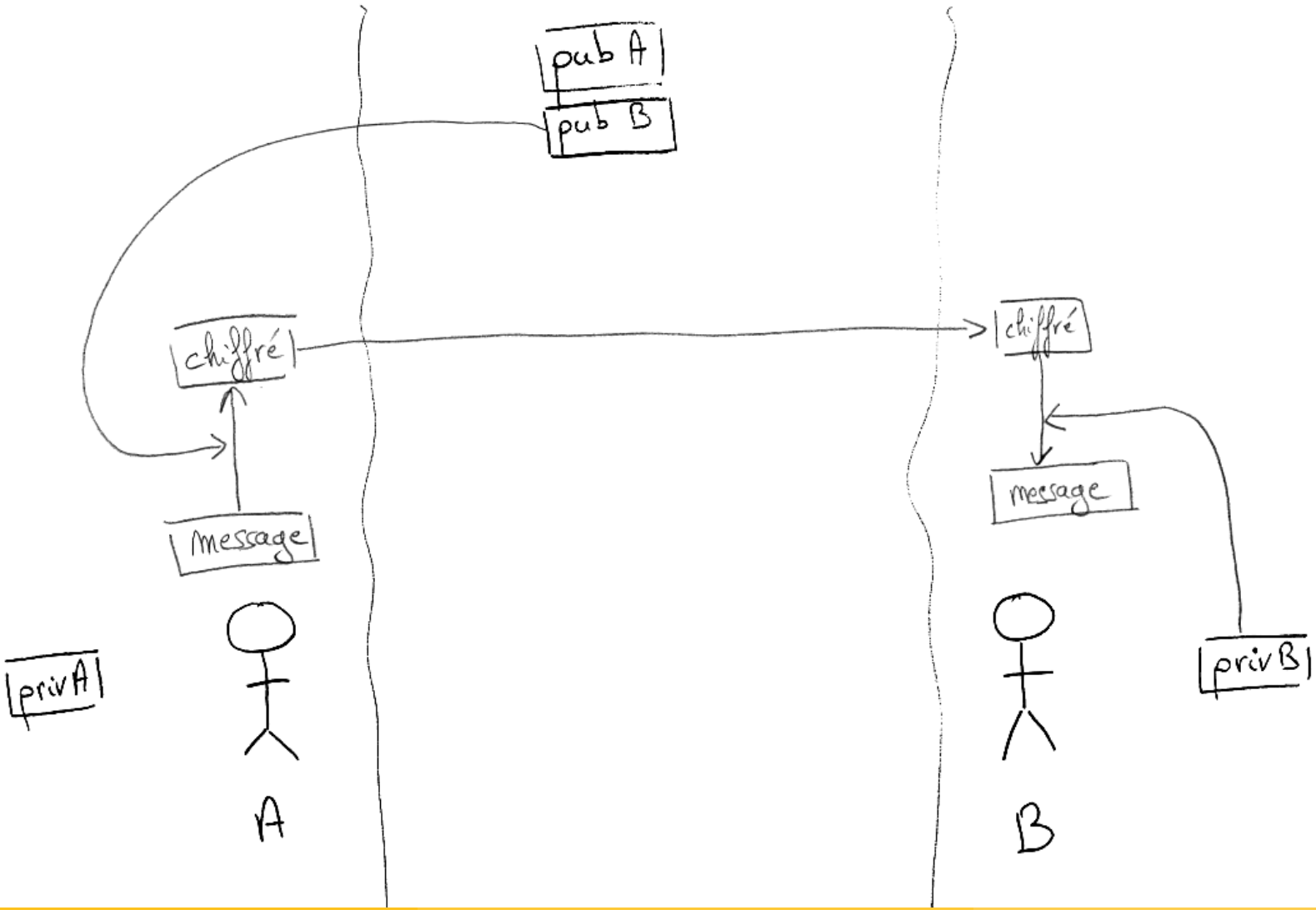
Cryptographie asymétrique

Chiffrement



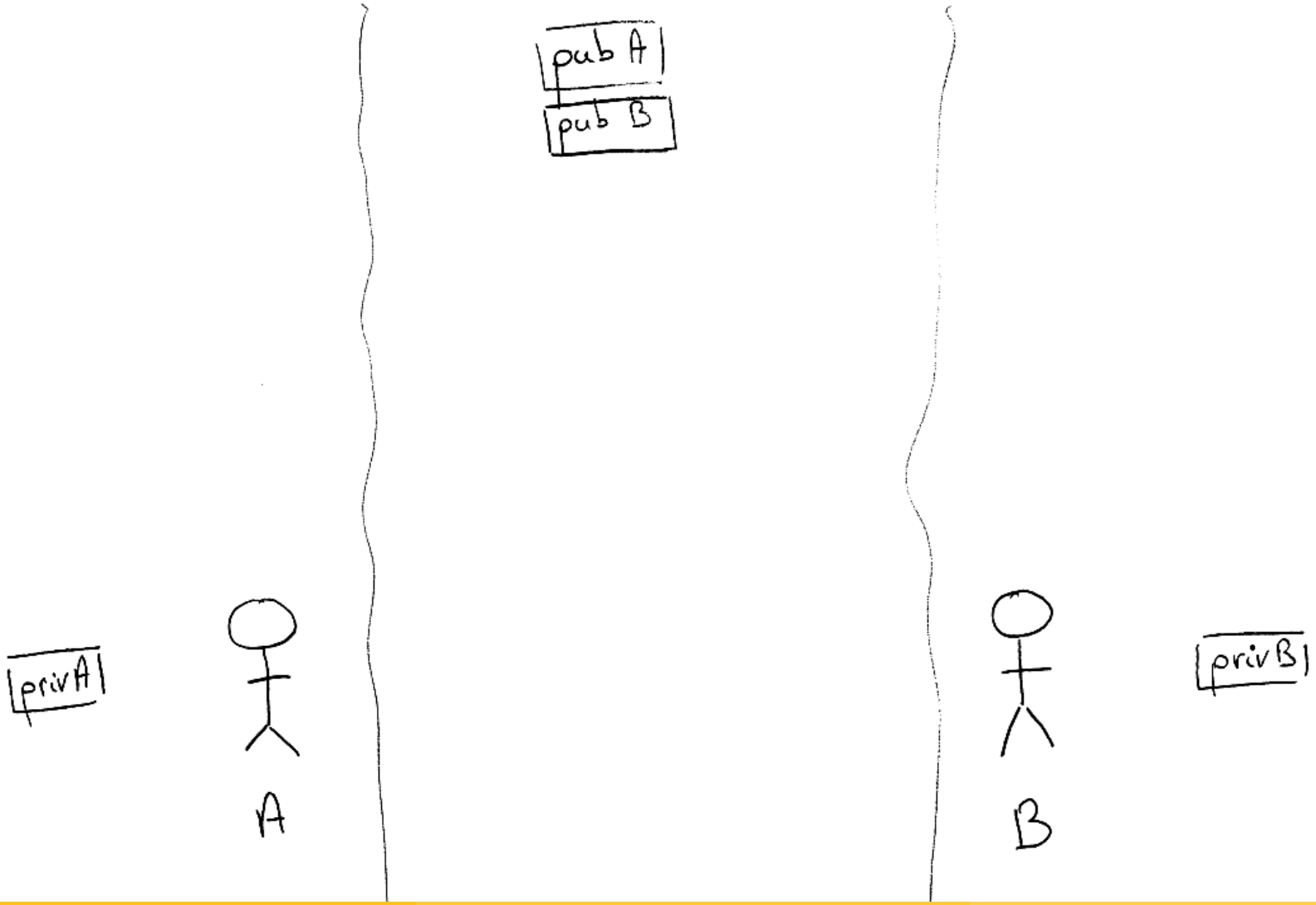
Cryptographie asymétrique

Chiffrement



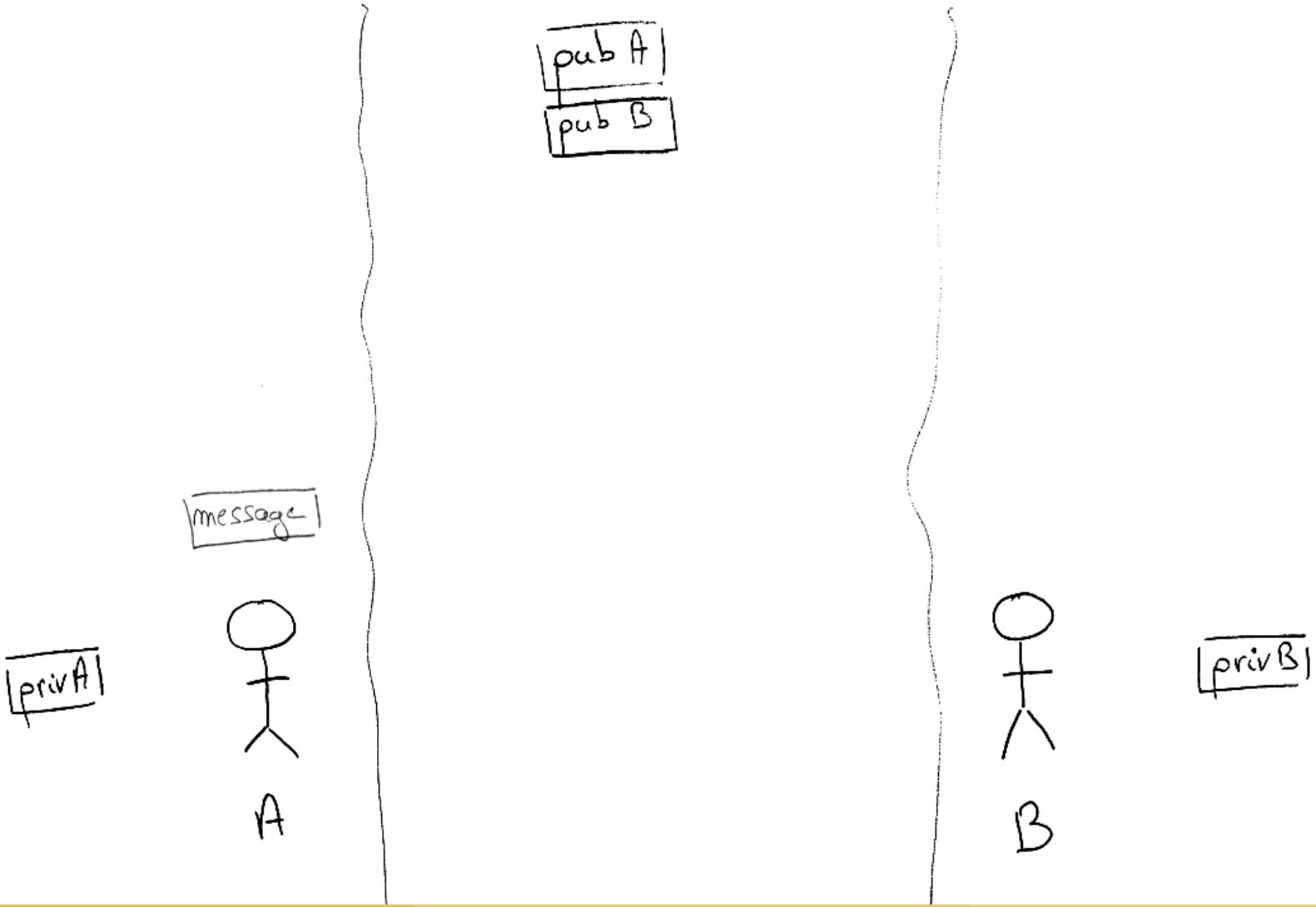
Cryptographie asymétrique

Signature



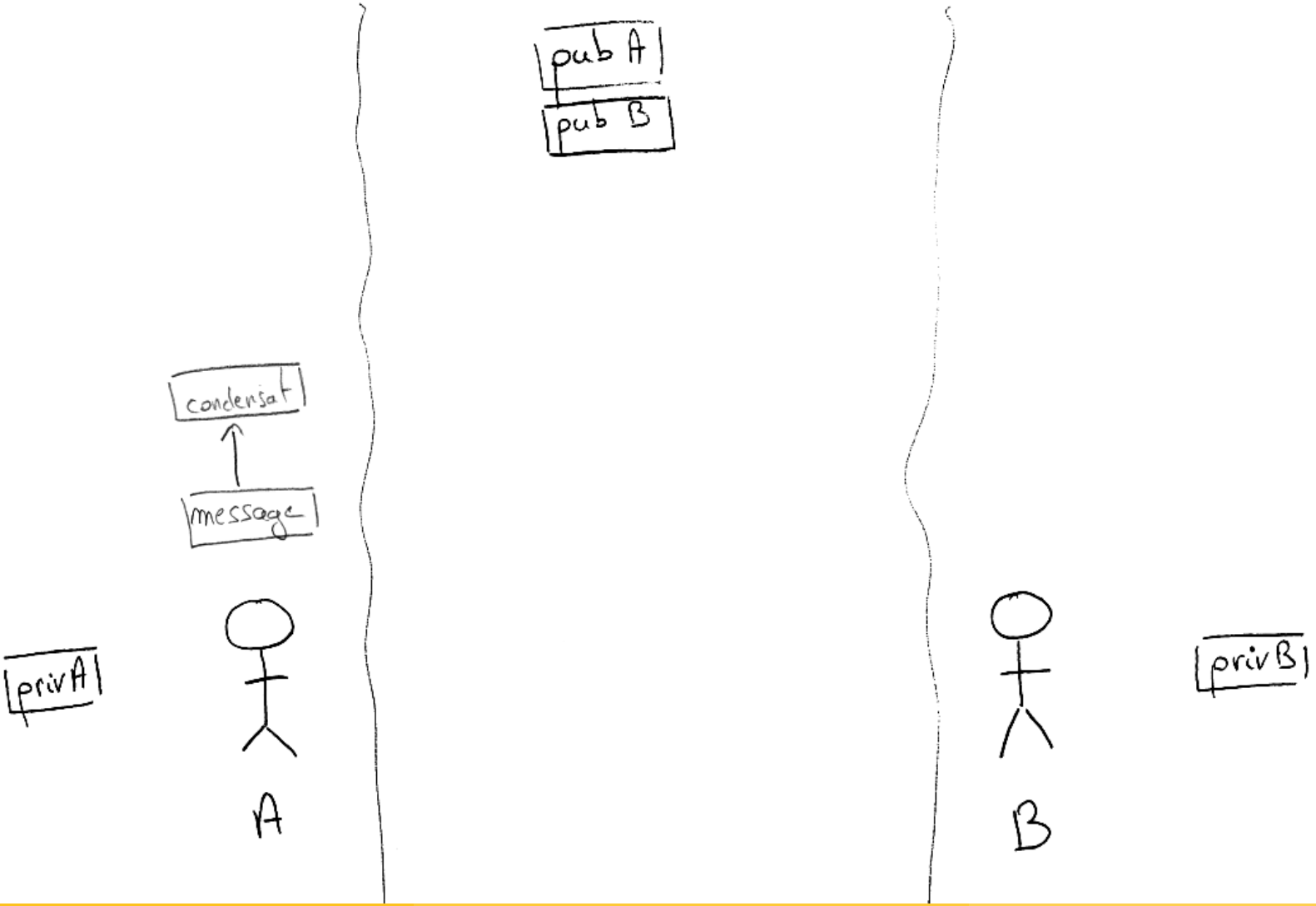
Cryptographie asymétrique

Signature



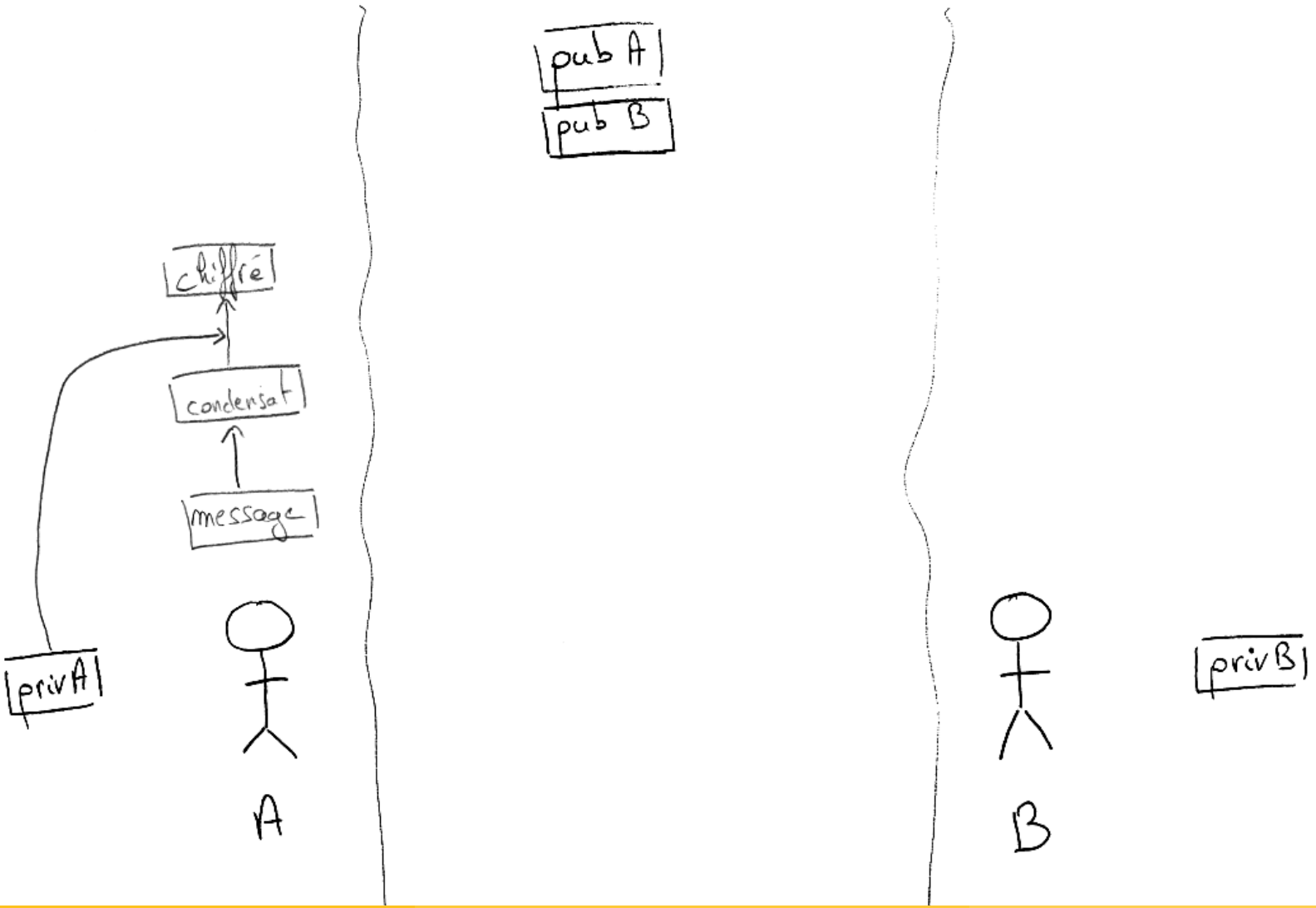
Cryptographie asymétrique

Signature



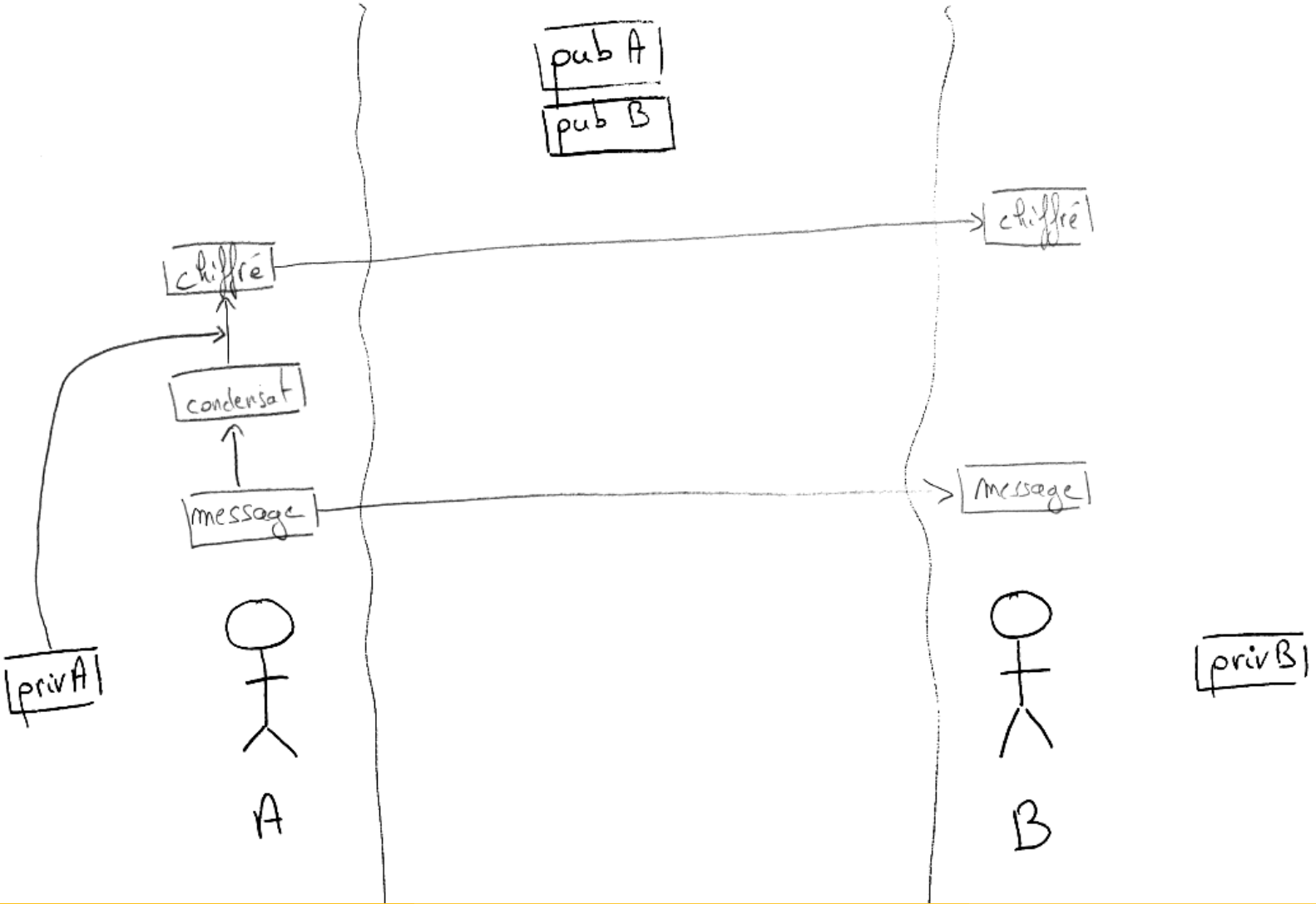
Cryptographie asymétrique

Signature



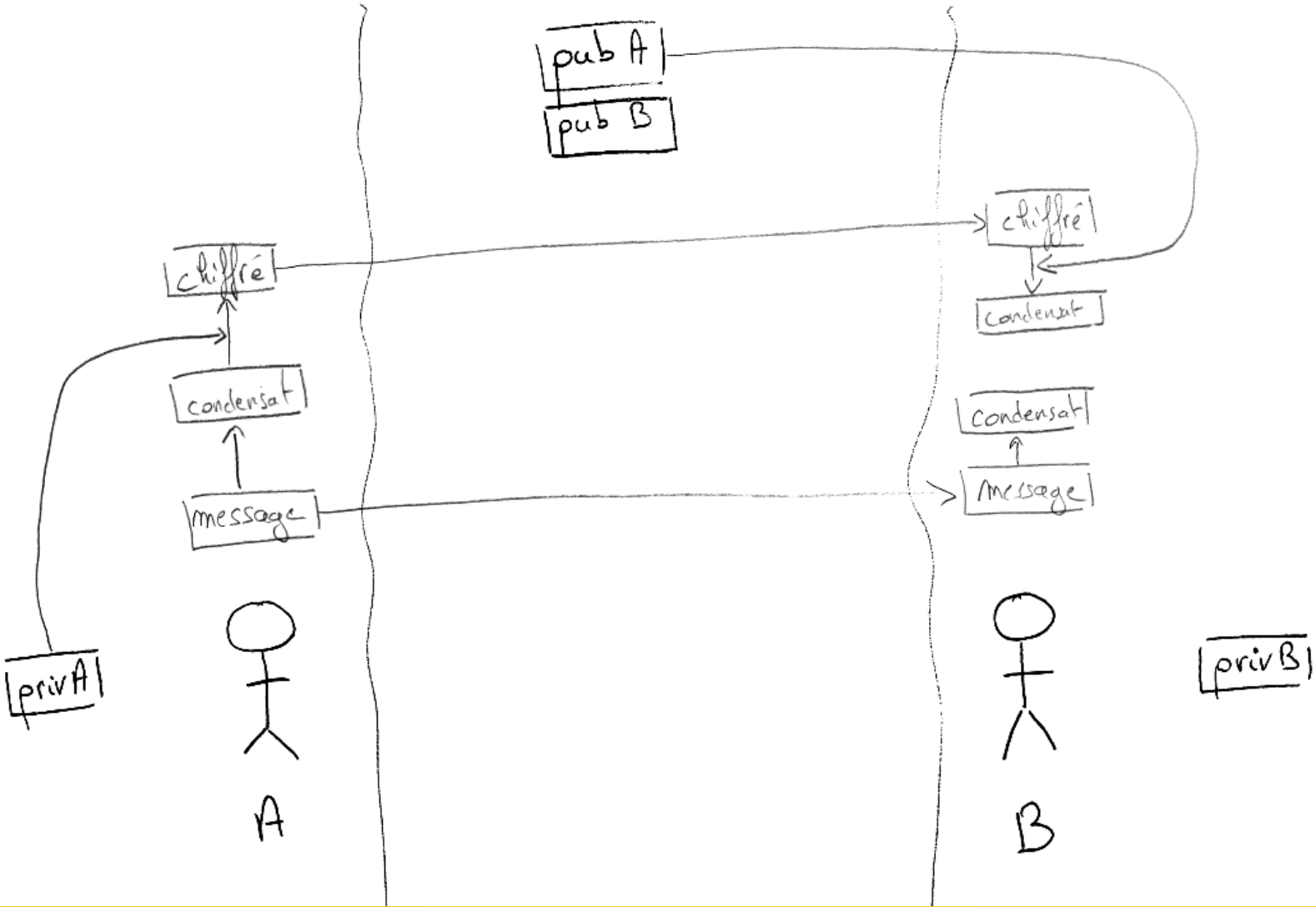
Cryptographie asymétrique

Signature



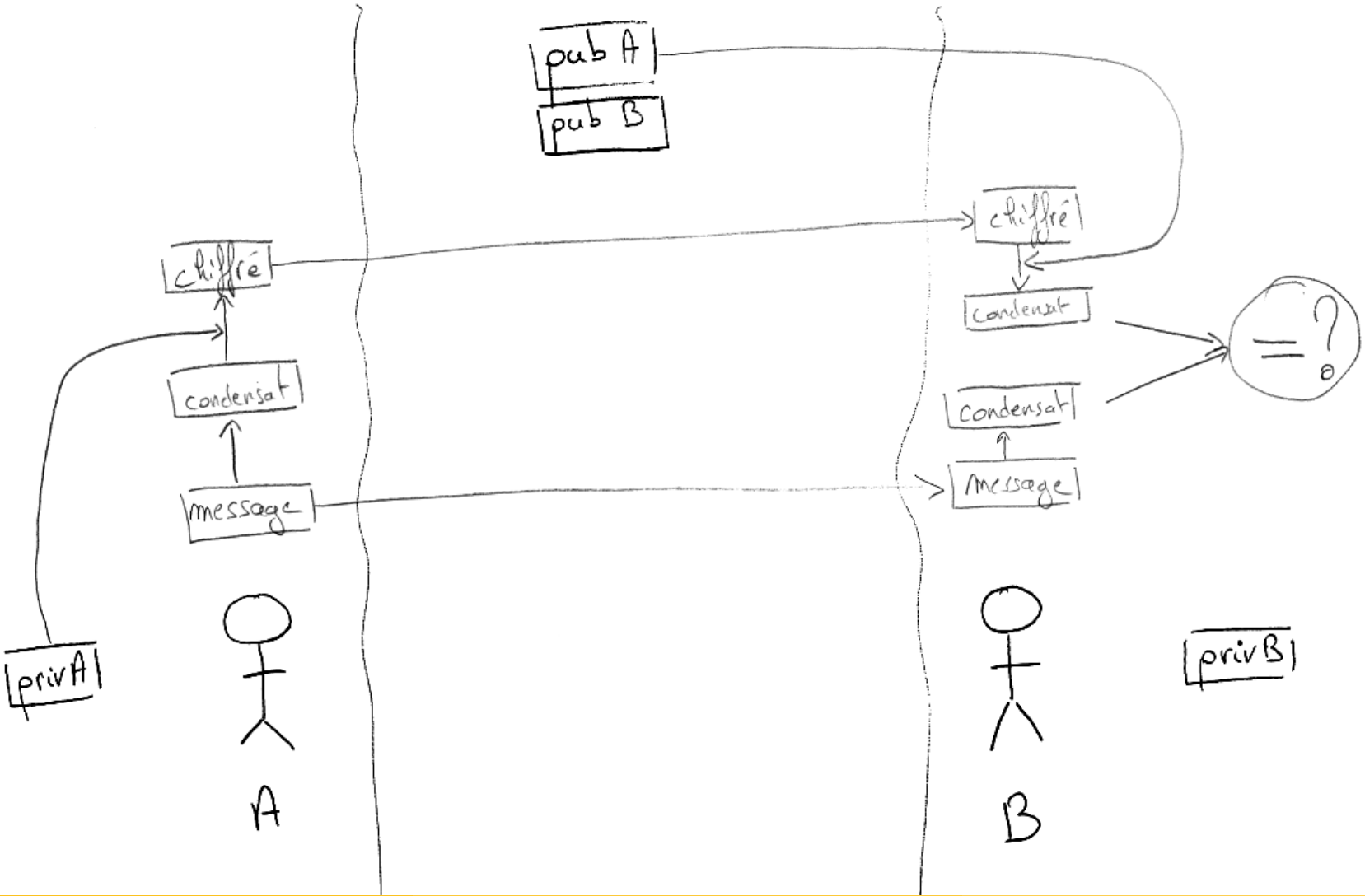
Cryptographie asymétrique

Signature



Cryptographie asymétrique

Signature



OpenPGP

Sous-clefs

- Sous-clef de chiffrement :
  - très souvent présentes,
  - permet d'utiliser openPGP pour signer et pour chiffrer/dechiffrer avec des clefs différentes,
  - permet de rendre indépendant le renouvelement de la sous-clef de la clef principale.
- Sous-clef de signature :
  - peu utilisée,
  - permet de signer du contenu (et non de certifier), sans disposer de la clef principale,
  - permet de rendre indépendant le renouvelement de la sous-clef de la clef principale.

OpenPGP

Certification

Ceci étant dit, comment s'assurer que :

- la clef publique soit associée à un nom,
- la clef publique soit bien celle de la personne avec laquelle nous voulons communiquer,
- les sous-clefs soient bien celle de la clef considérée

Le mécanisme de **certification** permet répondre à ces question.

OpenPGP

Clef publique au sens large

Une clef publique au sens large est constituée de :

- la clef publique au sens strict,
- des identités, avec pour chaque identité :
  - une certification signée avec la clef publique au sens strict (self-sig), *de facto* obligatoire pour que la clef soit utilisable,
  - les certifications d'autres personnes, facultatives,
- les parties publiques au sens strict de chaque sous-clef, avec pour chacune :
  - une certification signée avec la clef publique au sens strict (self-sig), *de facto* obligatoire pour que la clef soit utilisable,

OpenPGP

Mise en œuvre

Point de vocabulaire :

- OpenPGP est le nom de standard (RFC4880),
- GnuPG est le nom de l'implémentation la plus répandue,
- gpg est le nom de l'executable de l'implémentation GnuPG,
- PGP est le nom de l'implémentation historique (avant standardisation).

Dans les fait on mélange tout, en laissant le soin de décoder à l'arrivée.
Au boulot !

GnuPG

Validité et confiance

Attention, deux concepts différents :

- la validité associée à la clef de A est la croyance que j'ai au fait que la clef de A soit bien la clef de A,
- la confiance au propriétaire associée à la clef de A, est la croyance que j'ai que les certification que fait A sont légitimes.

Problème : on nomme souvent les deux avec le terme confiance (trust), et laissant le soin de décoder à l'arrivée.

Modèle de confiance (au sens validité)

Certification d'identité

A certifie B signifie que :

- B a donné son *fingerprint* à A via un canal sécurisé,
- B a justifié son identité à A
- A a récupéré la clef de B et a vérifiée qu'il s'agissait de la bonne à l'aide du *fingerprint*.
- A a signé un certificat qu'il adjoint à la clef de B.
- A a envoyé sa certification à B, ou au monde entier.

Exemple de certification.

Modèle de confiance (au sens validité)

Modèle historique, modèle PGP

On considère qu'est valide une clef :

- certifiée par moi,
- certifiée par une clef valide auquelle j'accorde une confiance entière,
- certifiée par trois clefs valides auquelles j'accorde une confiance au propriétaire marginale.

Condition supplémentaire, la longueur de la chaine de certification ne doit pas dépasser 5.
La confiance au propriétaire est quelque chose qui m'est propre et qui n'est communiqué nul part.
Attention : Une clef marginalement valide n'est pas valide, c'est une clef qui apparaît en bordure des clefs valides, mais avec un nombre insuffisant de certification (mais non nul).

Modèle de confiance (au sens validité)

Signing party

Classiquement, deux occasions de certifications :

- rencontres individuelles,
- signing party (**now**).

Modèle de confiance (au sens validité)
TOFU

Trust On First Use

Une clef est considérée comme valide si :

- l'identité A n'a jamais été utilisée,
- l'identité A n'a toujours été utilisée qu'avec cette clef,
- il n'y a qu'une seule clef associée à l'identitée A.

Modèle de confiance très faible, toutefois, c'est mieux que rien.

Usages

Exemples

Utilisation très courante dans :

- la signature des paquets de distributions,
- la signature des commits,
- la sécurisation des mails, signatures et chiffrement.

Conclusion

Un très bel outil, mais :

- protègez vos parties privées,
- ne protège que le contenu des communications, ne masque pas leur existences,
- ne vous sera d'aucune utilitée pour protéger des informations que vous divulguez par ailleurs.

OpenPGP, GnuPG, gpg, ne protégera jamais un utilisateur de sa propre stupidité.