

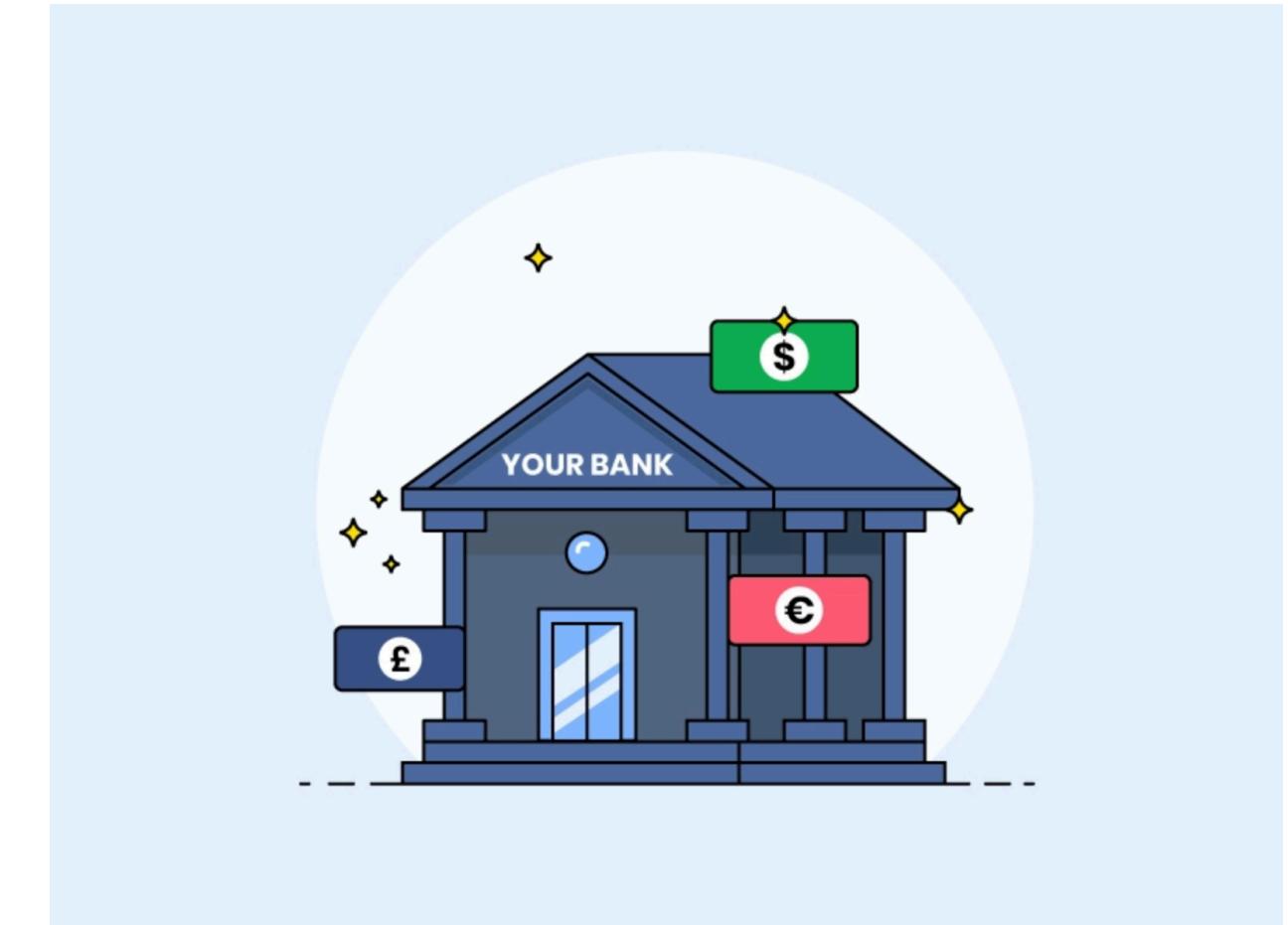


HTTP

le mot de passe
et les données sensibles
sont visibles

login:jean
password: anguille29

un espion écoute
(WireShark) et lit en clair les données
sensibles



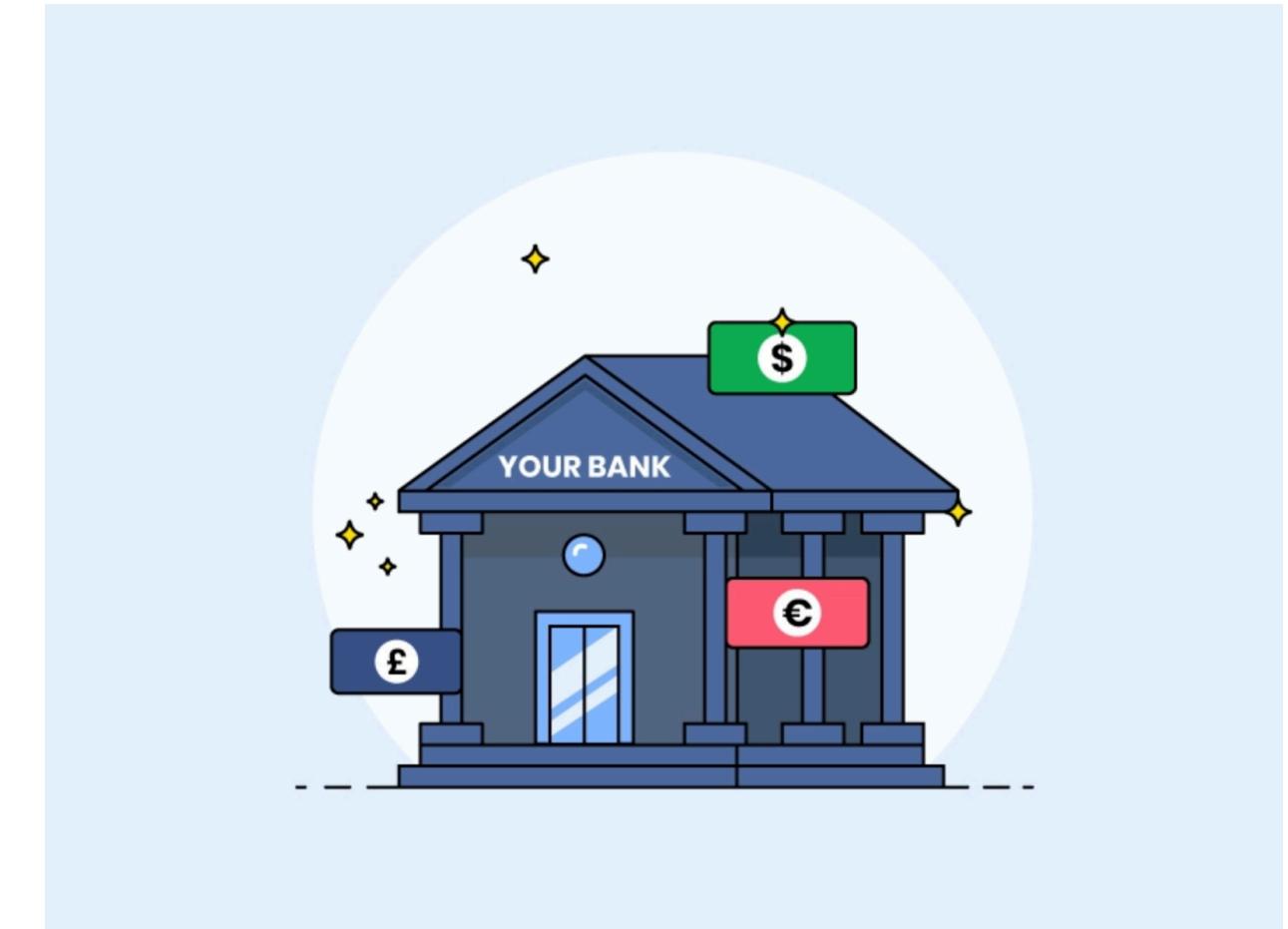


HTTPS

le mot de passe
et les données sensibles
sont chiffrés

login:ZE4FddeEFZ
password: GrrTTT65ddd

l'espion écoute
et lit du charabia inutilisable





**login: jean
password: anguille29**



**login: ZE4FddeEFZ
password: GrrTTT65ddd**



Clé de chiffrement + algorithme de chiffrement

LE CRYPTAGE



Lettre cryptée par Marie-Antoinette à destination du comte de Fersen, son amant, durant la révolution française.

Le cryptage de la correspondance de Marie-Antoinette est un sujet passionnant qui a suscité de nombreuses recherches et théories. La reine utilisait diverses techniques pour écrire des lettres secrètes à son amant, le comte de Fersen, pendant la Révolution française. Ces lettres étaient souvent écrites dans une forme de code ou de cryptage pour empêcher les agents de l'ordre national de les intercepter. Les chercheurs ont réussi à déchiffrer certaines de ces lettres, grâce à l'analyse linguistique et à l'étude des habitudes de la reine en matière d'écriture. Cependant, il existe toujours des lettres qui n'ont pas encore été déchiffrées complètement, ce qui ajoute à la mystique de cette histoire.



LE CRYPTAGE

Version très simplifiée du cryptage qui passait en réalité par un double chiffrage , mais il y avait un mot clé commun à M. Antoinette et Fersen.

MOT CLÉ : SECRETAIRE

M	O	N		B	I	E	N		A	I	M	É	
S	E	C	R	E	T	A	I	R	E	S	C	R	E
F	T												
S	E												
M	O												

Cryptage

S = rang 19

Décalage à partir de M vers la droite de 19 rangs -> F

Décryptage

S = rang 19

Décalage à partir de F vers la gauche de 19 rangs -> M

La question des historiens est : comment les 2 amants se passaient le mot clé, Marie-Antoinette étant enfermée aux tuileries et Fersen étant hors de France?



login: jean
password: anguille29

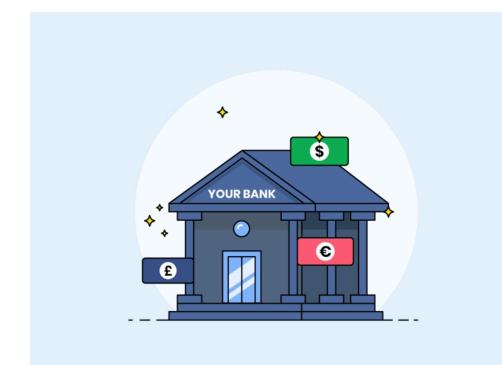


login: ZE4FddeEFZ
password: GrrTTT65dddd

REQUETE VERS
LA BANQUE

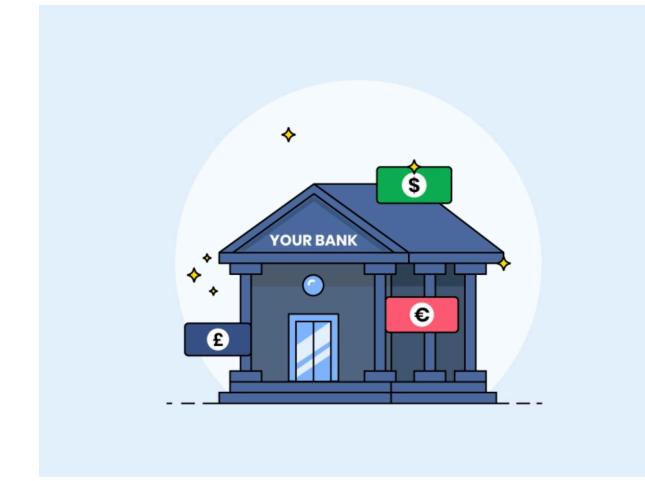


Clé de chiffrement + algorithme de chiffrement





Réception de
la requête



login: ZE4FddeEFZ
password: GrrTTT65dddd

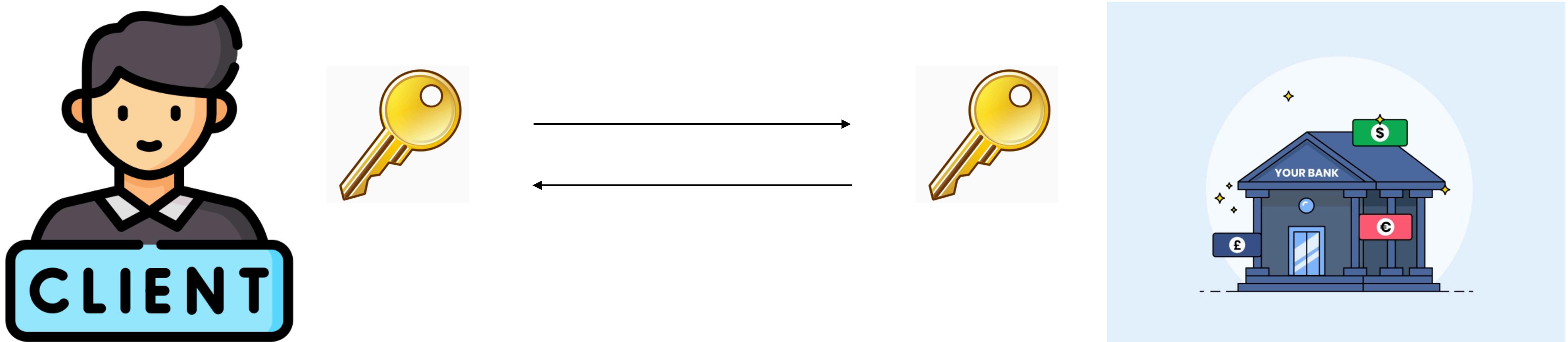


login: jean
password: anguille29



Clé de chiffrement + algorithme de déchiffrement

CRYPTOGRAPHIE SYMETRIQUE



Les 2 parties possèdent la même clef pour chiffrer et déchiffrer

Inconvénient : envoyer la clé en clair une 1ere fois expose au risque d'être lue par un hacker

CRYPTOGRAPHIE ASYMETRIQUE



CLÉ PRIVÉE



CLÉ PUBLIQUE



clé privée
de POLO

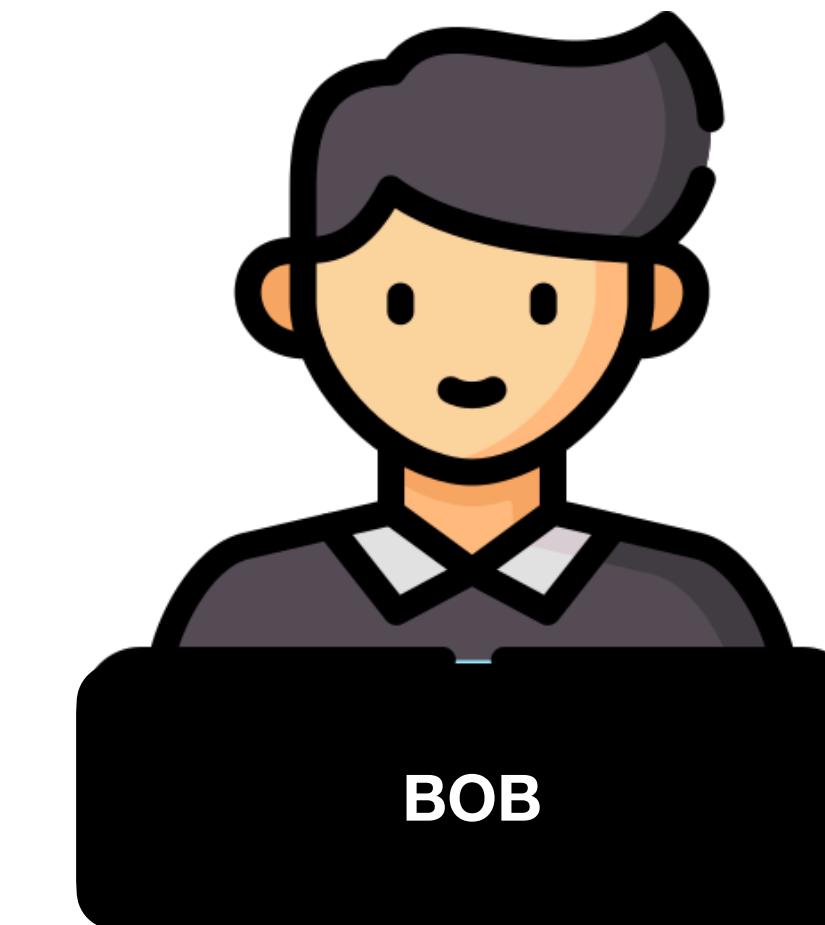


clé publique
de POLO

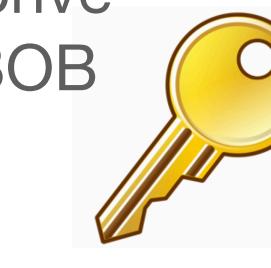


remarque: un utilisateur peut chiffrer
avec une 1ere clé
et déchiffrer avec une 2ème clé et
inversement.
Les clés sont liées.

Bob va sur le site de POLO
et reçoit la clé publique de polo



clé privée
de BOB



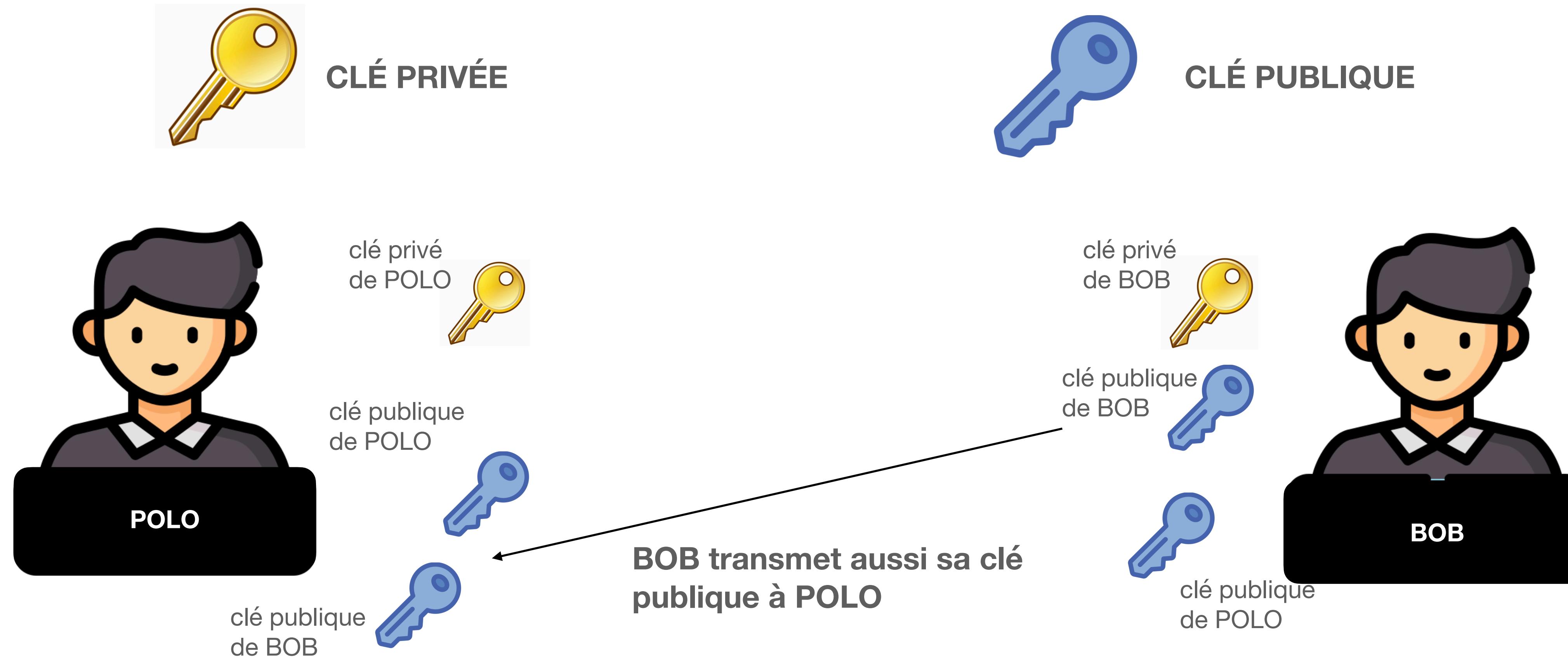
clé publique
de BOB



clé publique
de POLO

Remarque:
La clé privée n'est JAMAIS transmise

CRYPTOGRAPHIE ASYMETRIQUE



remarque: un utilisateur peut chiffrer avec une 1ere clé et déchiffrer avec une 2ème clé et inversement.
Les clés sont liées.

Remarque:
La clé privée n'est JAMAIS transmise

CRYPTOGRAPHIE ASYMETRIQUE



CLÉ PRIVÉE



CLÉ PUBLIQUE

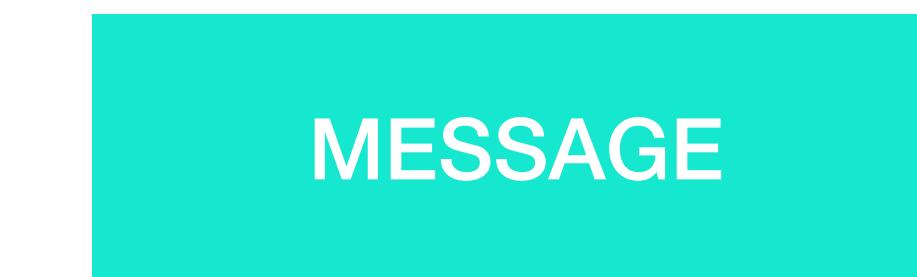


clé privée
de POLO

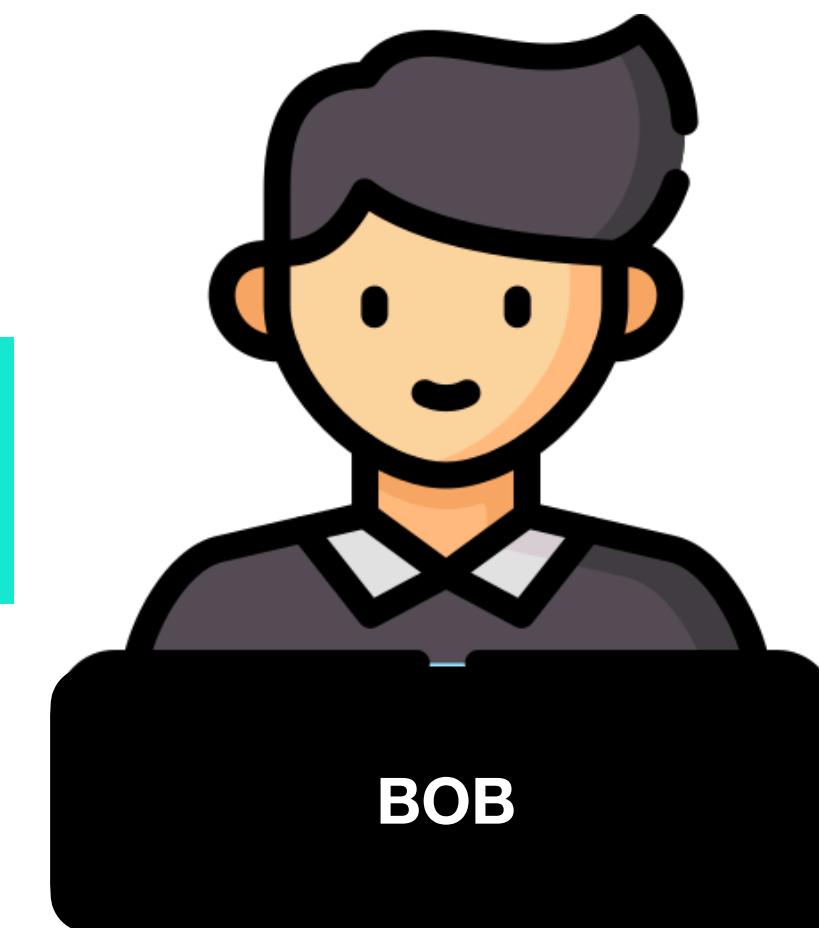


BOB envoie un message à POLO et utilise pour cela la clé publique de POLO pour crypter le message. Seul POLO pourra le déchiffrer avec sa clé privée

RT5TYYEG



clé publique
de POLO



RT5TYYEG

CRYPTOGRAPHIE ASYMETRIQUE



CLÉ PRIVÉE



CLÉ PUBLIQUE



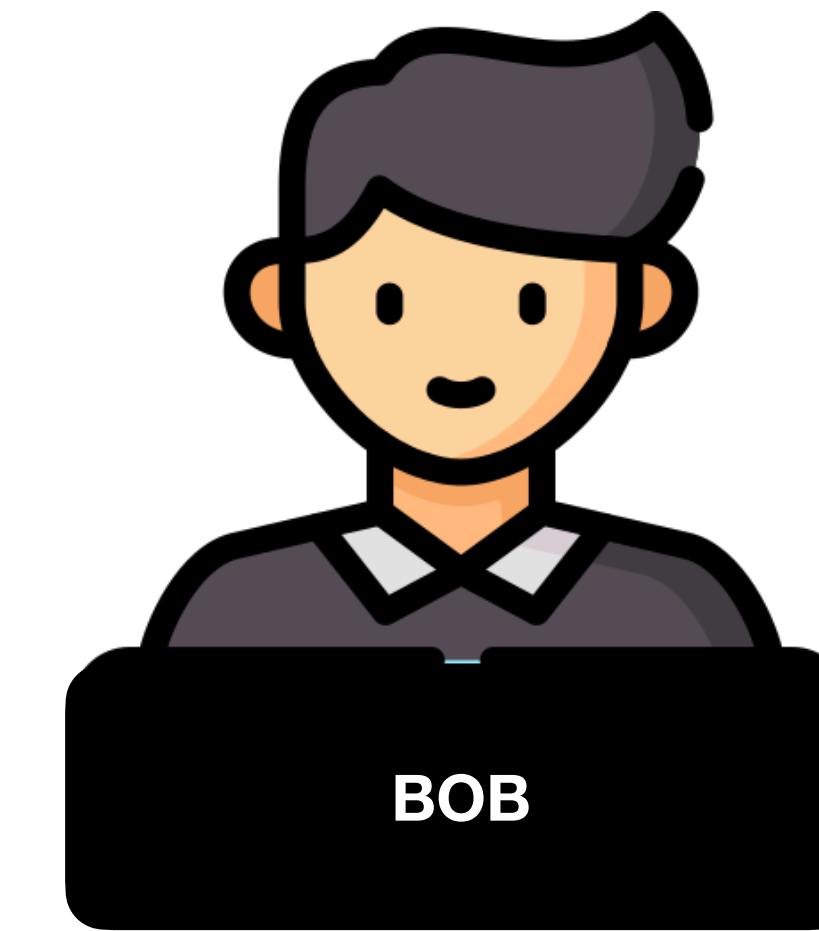
clé privée
de POLO

MESSAGE

POLO décrypte le message
avec sa clé privée



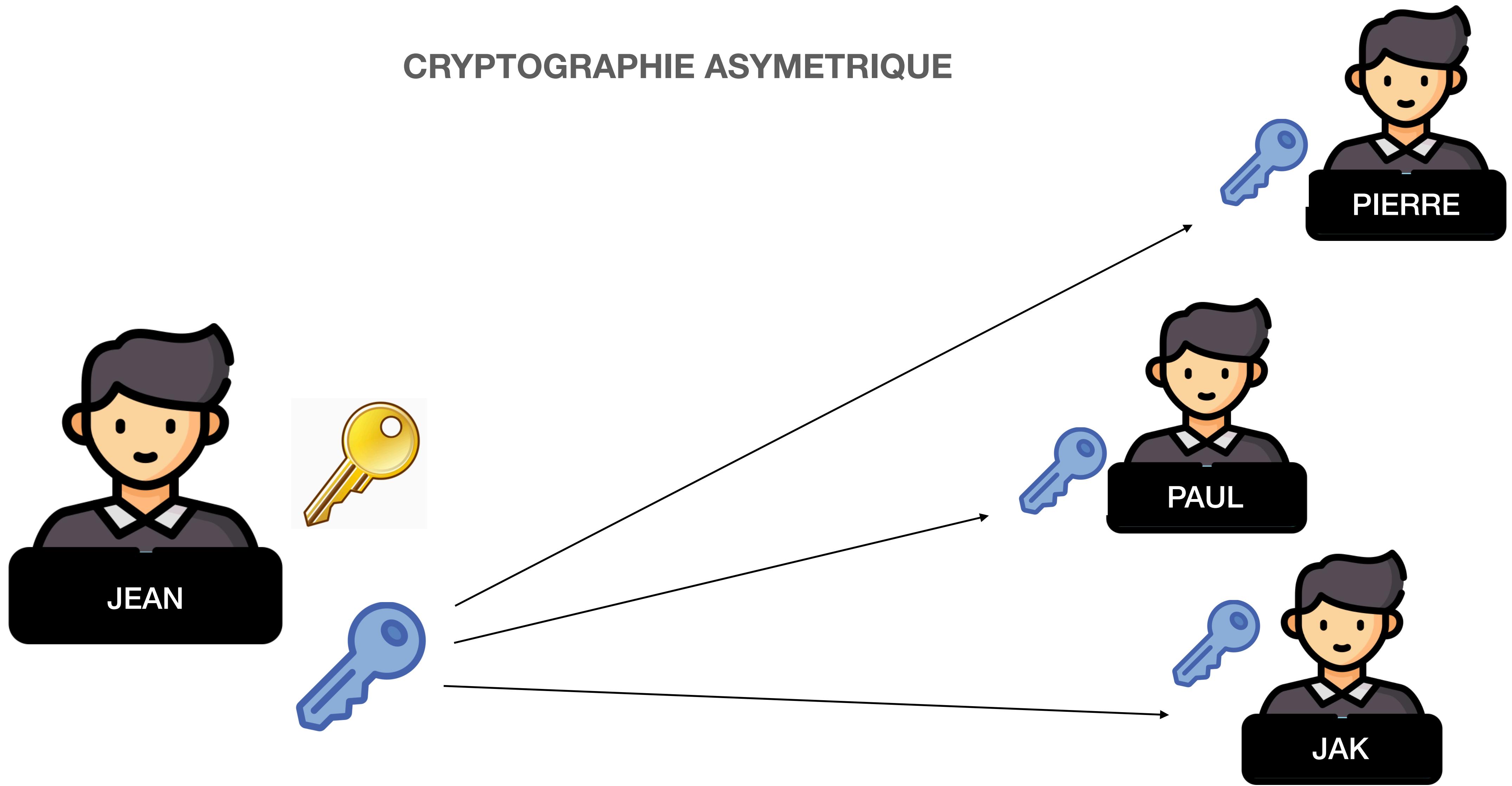
clé publique
de POLO



Si POLO répond à BOB il procède
de la même manière, il utilise la clé de BOB
pour crypter le message avant de l'envoyer

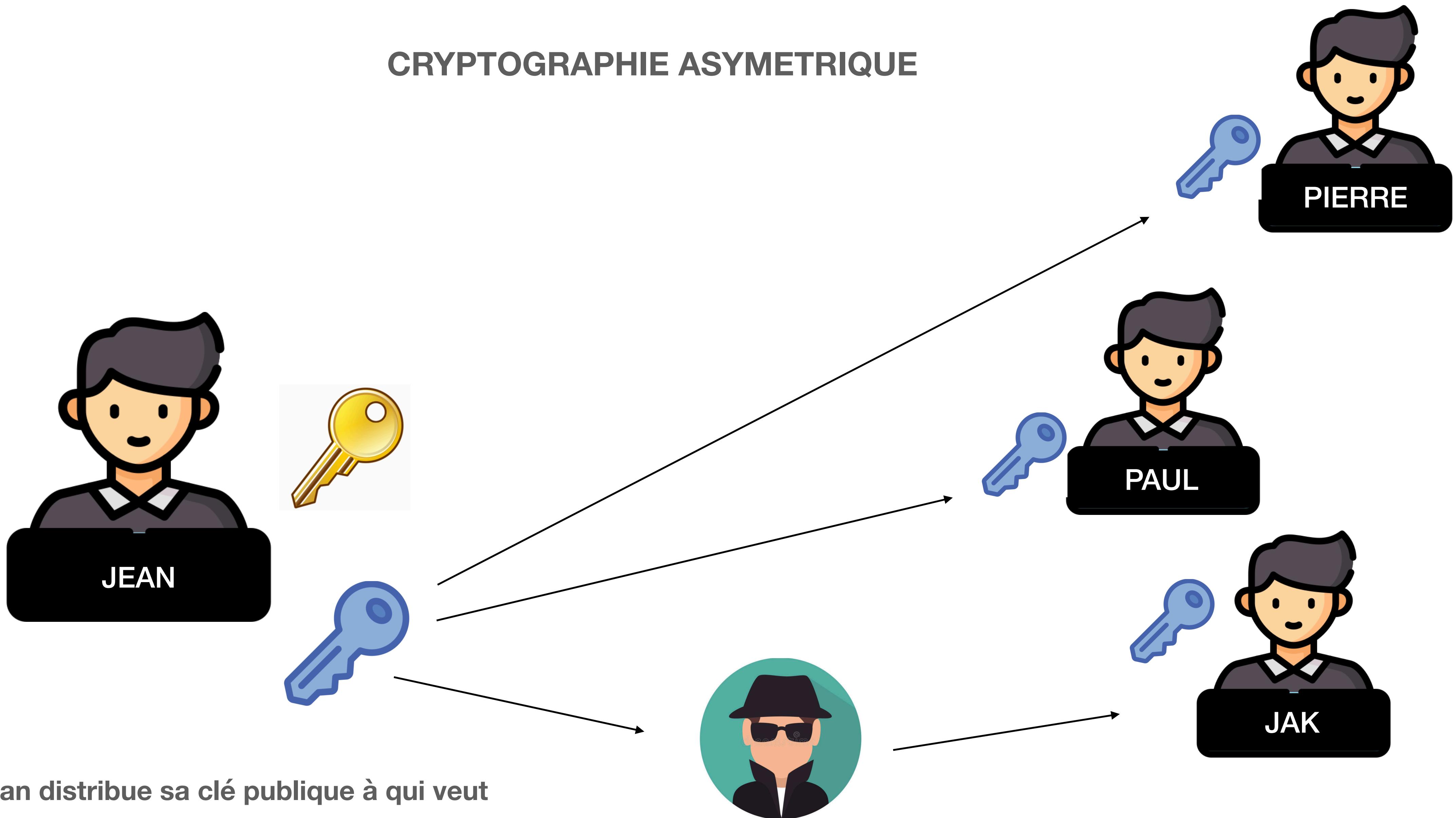
CE PROCÉDÉ ASSURE LA CONFIDENTIALITÉ DE L'ÉCHANGE, **MAIS !!!**

CRYPTOGRAPHIE ASYMETRIQUE



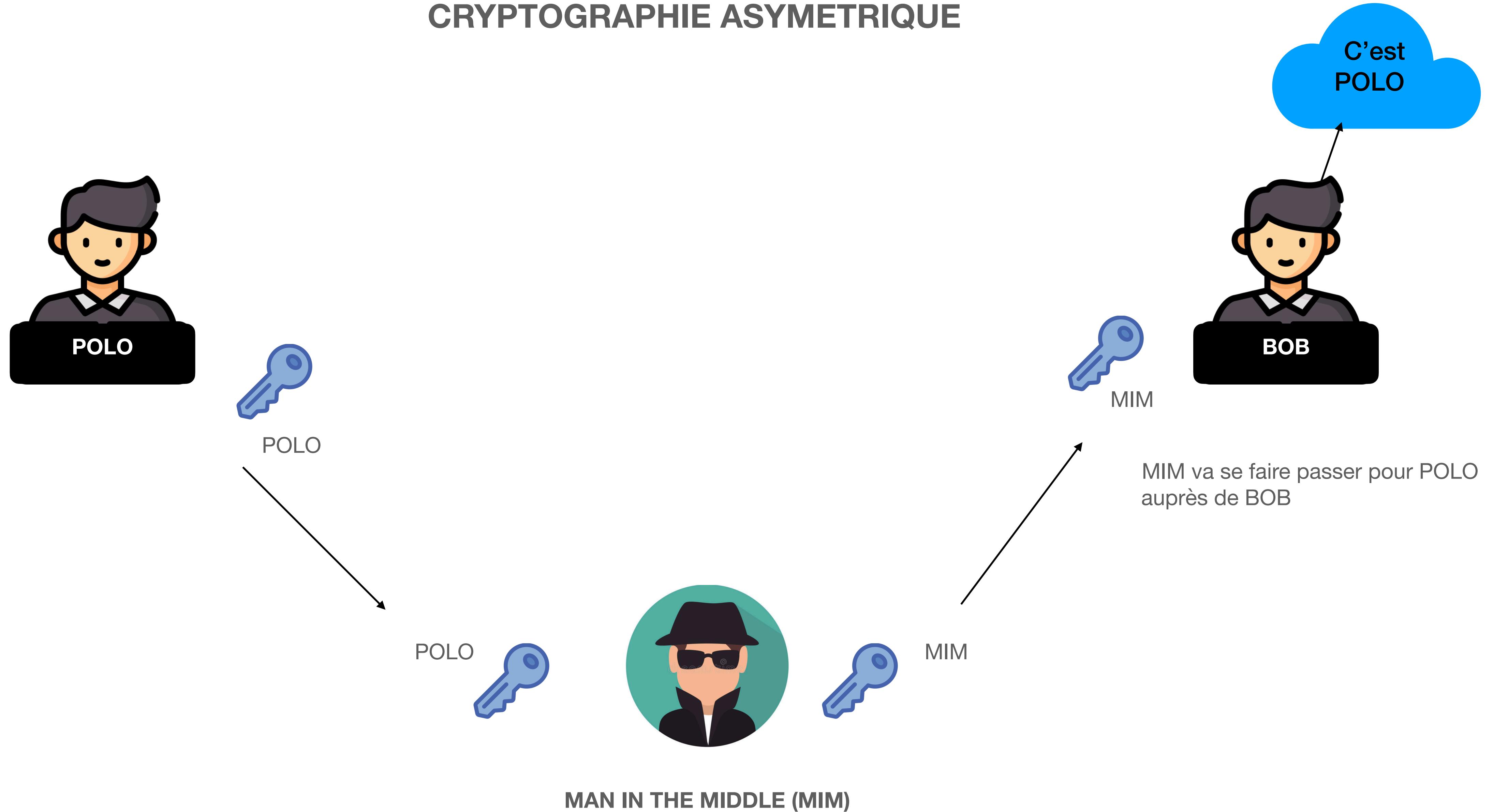
Jean distribue sa clé publique

CRYPTOGRAPHIE ASYMETRIQUE

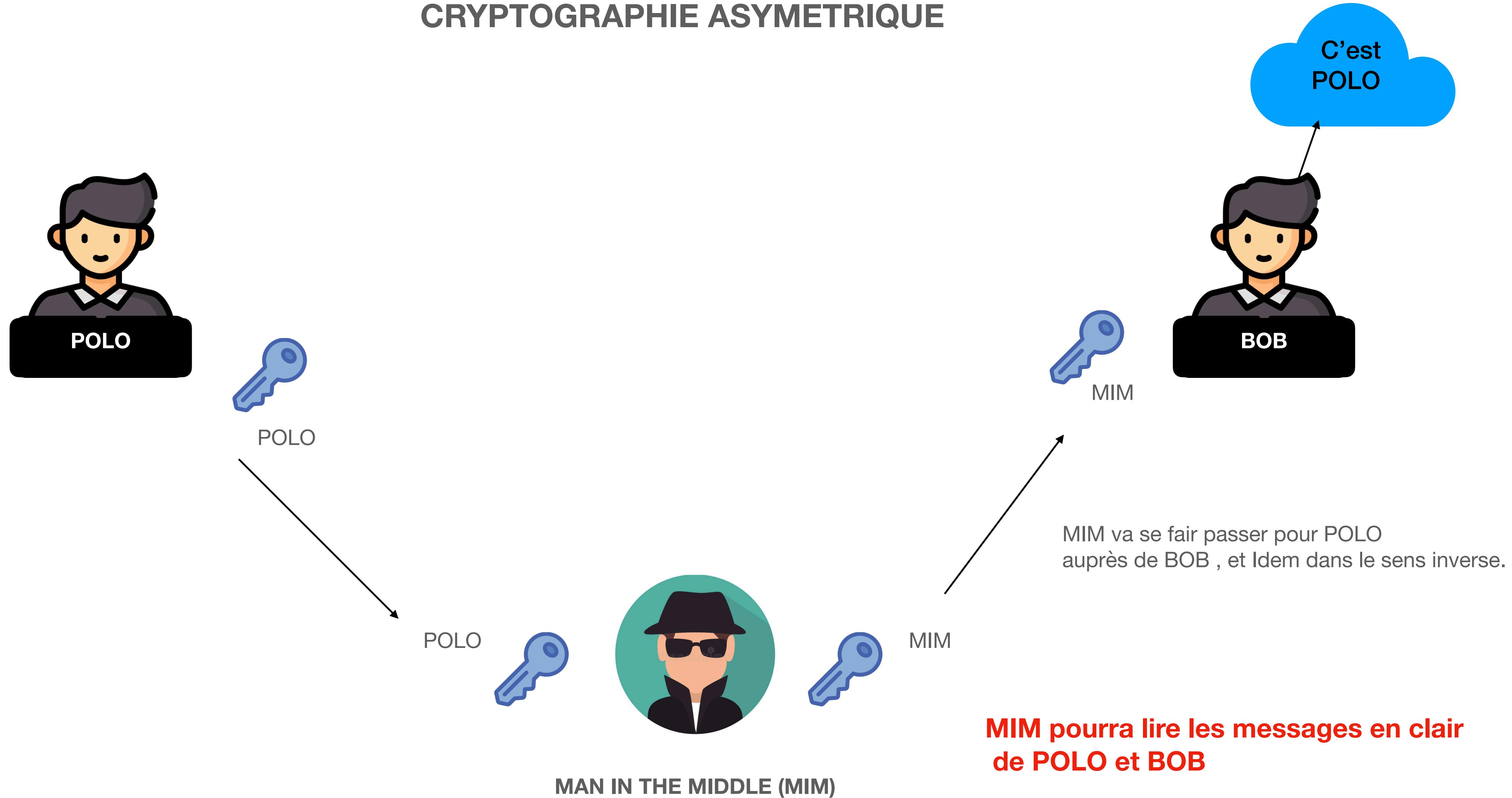


MAN IN THE MIDDLE

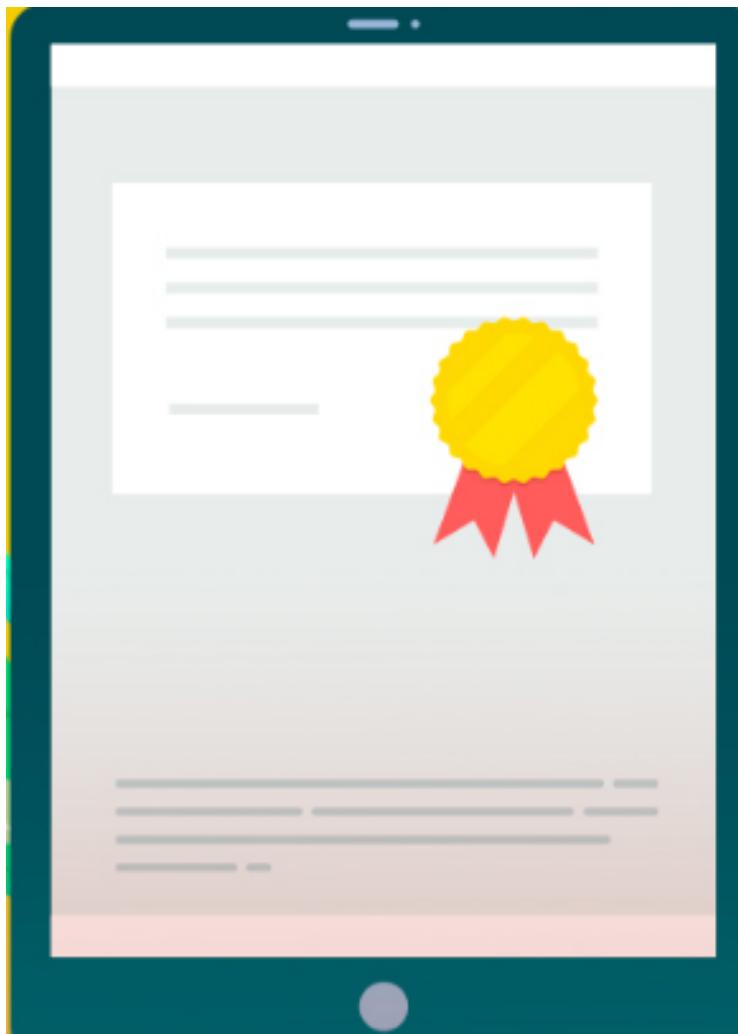
CRYPTOGRAPHIE ASYMETRIQUE



CRYPTOGRAPHIE ASYMETRIQUE



CERTIFICAT



POUR IDENTIFIER LA PERSONNE ON UTILISE UN CERTIFICAT.

LE CERTIFICAT EST UN FICHIER CONTENANT:

Une clé publique 

Des informations sur la personne (nom, prénom, adresse...etc...)



Informations sur le certificat (date de validité entre autres)

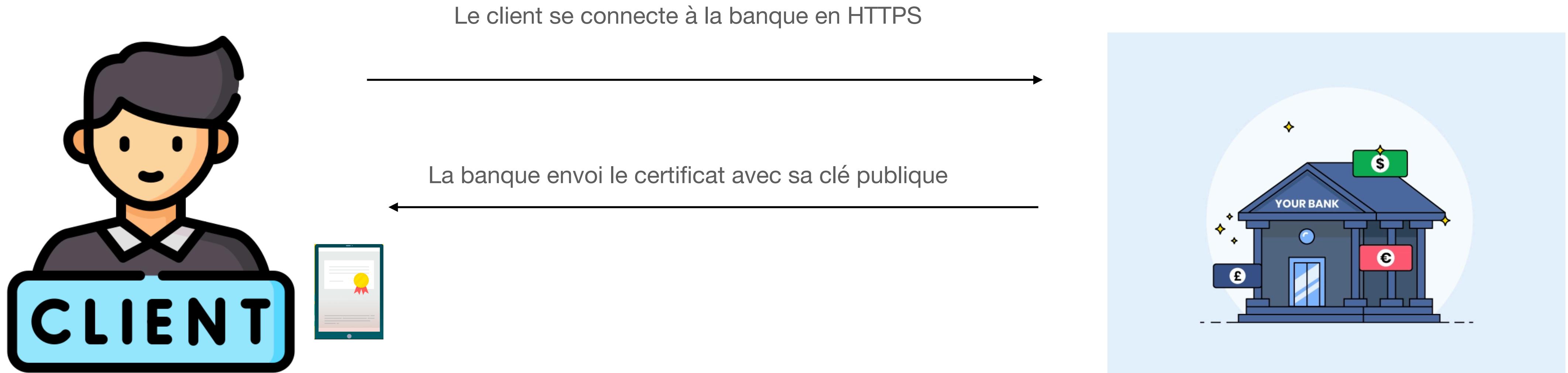
Signature électronique d'une autorité de certification.

Le certificat est délivré par une autorité de certification payante.

La personne désirant se certifier doit donner sa clé publique des informations sur elle.

Le certificat prouve que la clé publique appartient bien à cette personne,
ça évite la faille du Man In the Middle.

CHIFFREMENT SSL/TLS

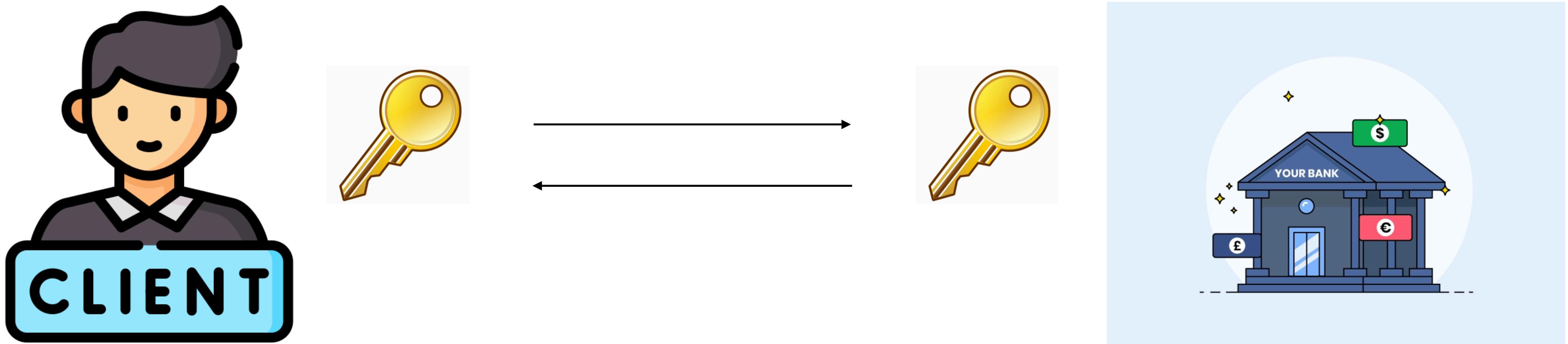


Le navigateur possède un BDD avec les clés publiques des autorités de certification

TLS : Transport Layer Security

SSL : Secure Socket Layer

CHIFFREMENT SSL/TLS



Le client et la banque négocient pour obtenir une clé commune comme pour le chiffrement symétrique