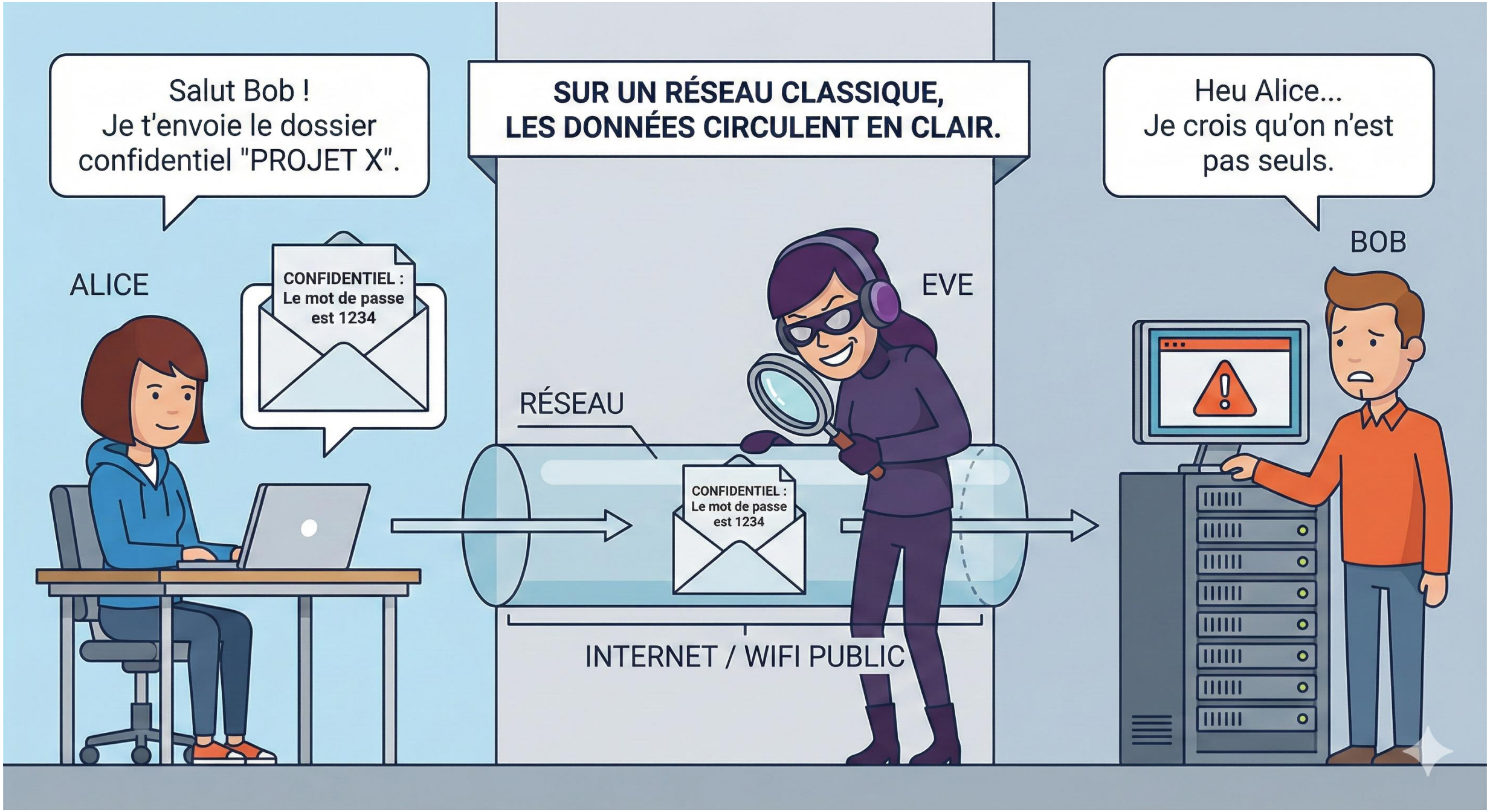

Salut Bob !
Je t'envoie le dossier confidentiel "PROJET X".
SUR UN RÉSEAU CLASSIQUE, LES DONNÉES CIRCULENT EN CLAIR.
Heu Alice...
Je crois qu'on n'est pas seuls.
ALICE
CONFIDENTIEL : Le mot de passe est 1234
EVE
BOB
RÉSEAU
CONFIDENTIEL : Le mot de passe est 1234
INTERNET / WIFI PUBLIC

PRINCIPE DU CHIFFREMENT

Je chiffre le message avant de l'envoyer.

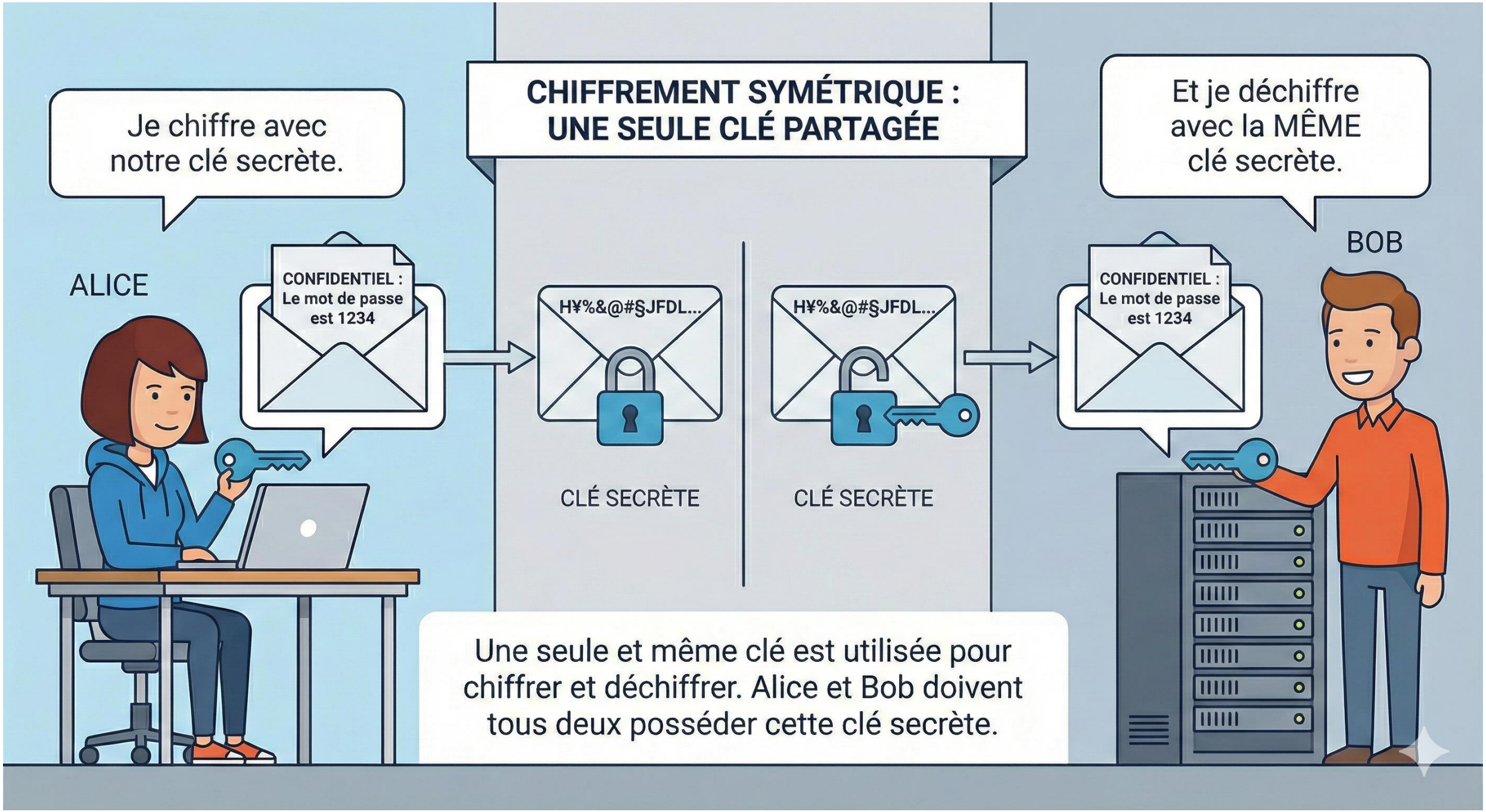
ALICE

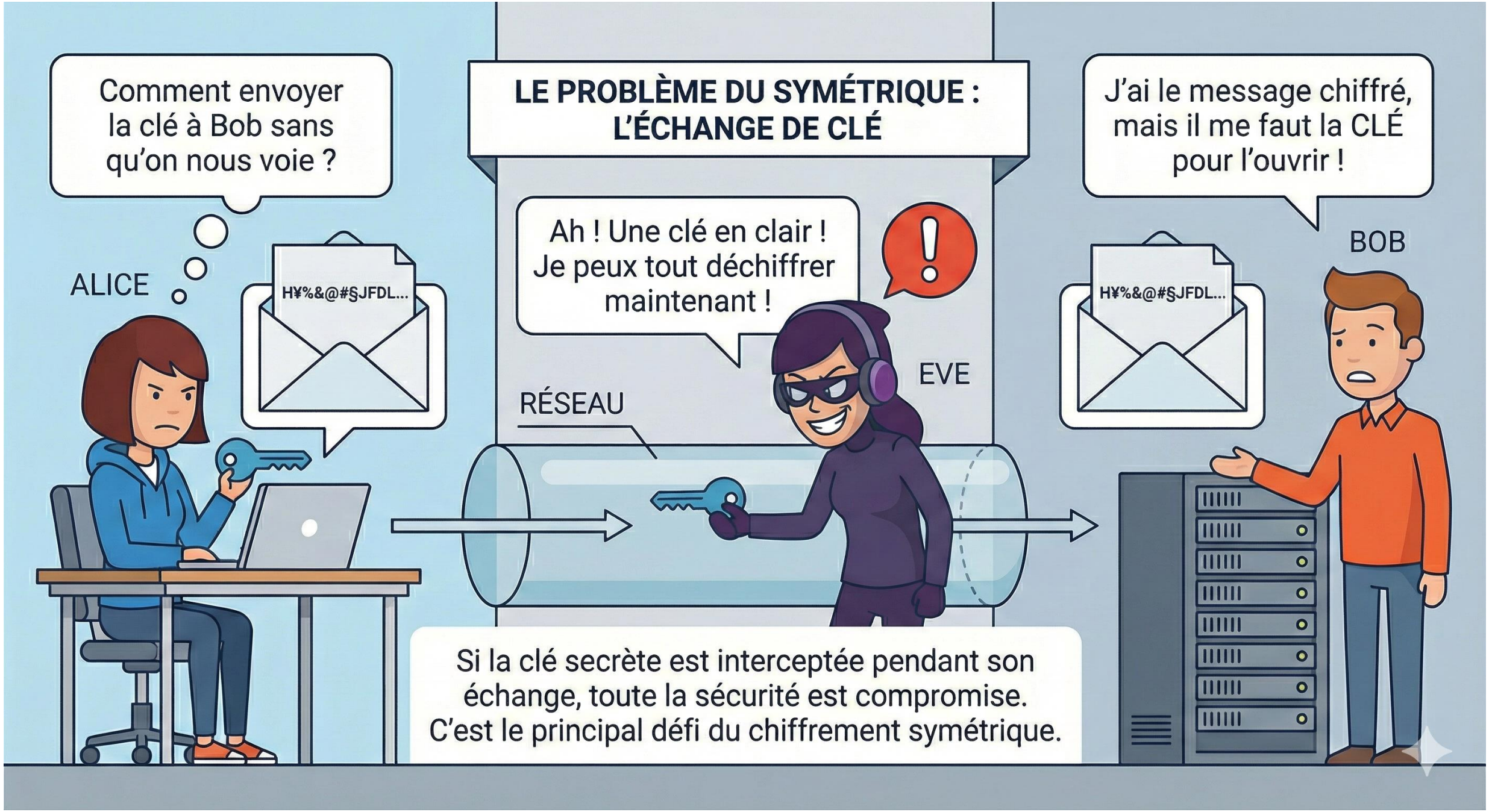
CONFIDENTIEL : Le mot de passe est 1234

CHIFFREMENT

H¥%&@#§JFDL KL$£€

Le chiffrement transforme les données en un format illisible (texte chiffré) pour les protéger. Seule une clé spécifique peut les déchiffrer.

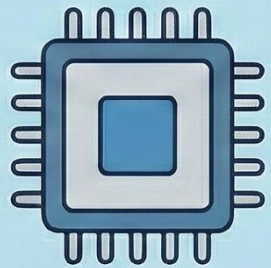

CHIFFREMENT SYMÉTRIQUE :
UNE SEULE CLÉ PARTAGÉE
Je chiffre avec notre clé secrète.
Et je déchiffre avec la MÊME clé secrète.
ALICE
BOB
CONFIDENTIEL : Le mot de passe est 1234
H¥%&@#§JFDL...
H¥%&@#§JFDL...
CONFIDENTIEL : Le mot de passe est 1234
CLÉ SECRÈTE
CLÉ SECRÈTE
Une seule et même clé est utilisée pour chiffrer et déchiffrer. Alice et Bob doivent tous deux posséder cette clé secrète.


LE PROBLÈME DU SYMÉTRIQUE : L'ÉCHANGE DE CLÉ
Comment envoyer la clé à Bob sans qu'on nous voie ?
ALICE
H¥%&@#§JFDL...
Ah ! Une clé en clair ! Je peux tout déchiffrer maintenant !
EVE
RÉSEAU
J'ai le message chiffré, mais il me faut la CLÉ pour l'ouvrir !
BOB
H¥%&@#§JFDL...
Si la clé secrète est interceptée pendant son échange, toute la sécurité est compromise. C'est le principal défi du chiffrement symétrique.

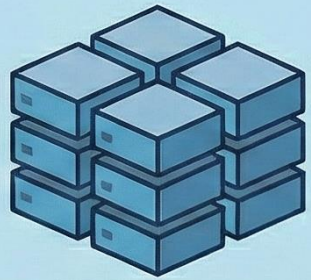
CHIFFREMENT SYMÉTRIQUE : AVANTAGES / INCONVÉNIENTS

AVANTAGES

RAPIDE



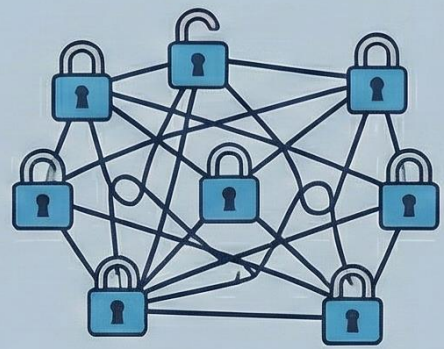
PEU COÛTEUX EN RESSOURCES



IDÉAL POUR GROS VOLUMES DE DONNÉES

INCONVÉNIENTS

PROBLÈME DE PARTAGE DE LA CLÉ



PEU PRATIQUE À GRANDE ÉCHELLE

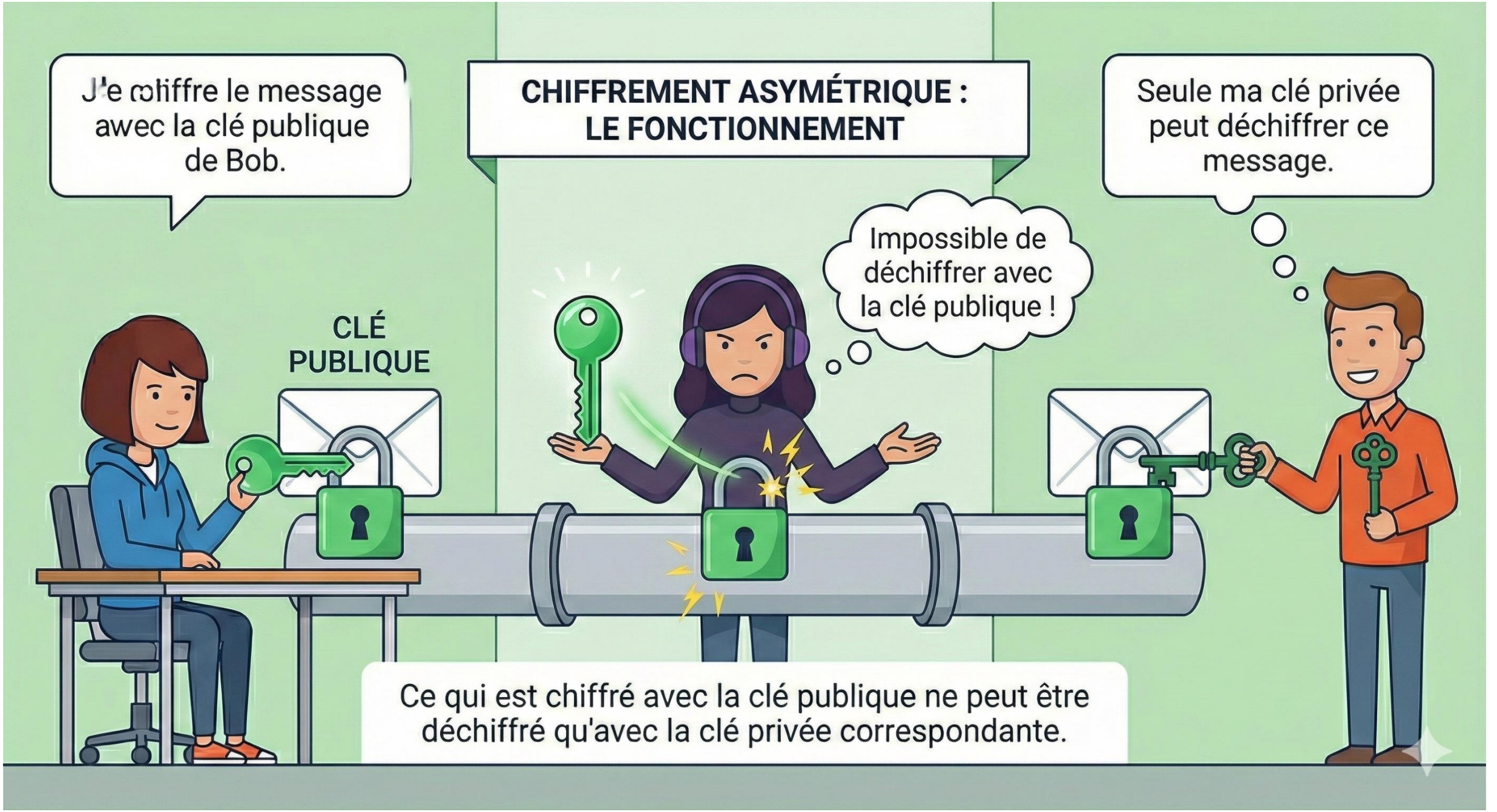
EXEMPLES D'ALGORITHMES

AES

DES (ancien)

ChaCha20


CHIFFREMENT ASYMÉTRIQUE :
UNE PAIRE DE CLÉS
Voici ma CLÉ PUBLIQUE ! Je la donne à tout le monde !
...Mais celle-ci est ma CLÉ PRIVÉE. Je la garde secrète.
BOB
≠
CLÉ PUBLIQUE
CLÉ PRIVÉE
Deux clés différentes mais liées mathématiquement.
L'une est publique, l'autre reste secrète.


CHIFFREMENT ASYMÉTRIQUE :
LE FONCTIONNEMENT
Je chiffre le message avec la clé publique de Bob.
CLÉ PUBLIQUE
Impossible de déchiffrer avec la clé publique !
Seule ma clé privée peut déchiffrer ce message.
Ce qui est chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante.

CHIFFREMENT ASYMÉTRIQUE : BILAN

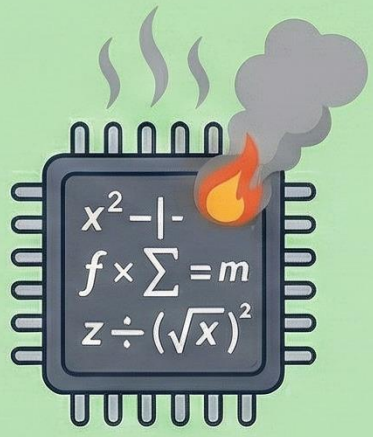
AVANTAGES

ÉCHANGE SÉCURISÉ DE (Pas de secret partagé)

BASE DE LA CONFIANCE (Authentification, Web)

INCONVÉNIENTS

LENT



COÛTEUX EN CALCUL / RESSOURCES

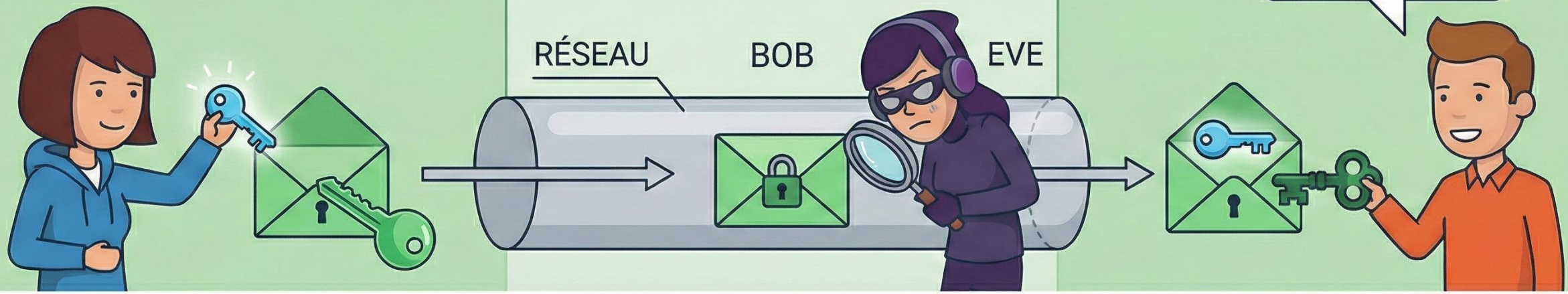
EXEMPLES D'ALGORITHMES

123 780 RSA

ECC (Courbes Elliptiques)

EN PRATIQUE : LES DEUX ENSEMBLE (HTTPS)

1. ASYMÉTRIQUE : ÉCHANGE SÉCURISÉ DE LA CLÉ



2. SYMÉTRIQUE : CHIFFREMENT RAPIDE DES DONNÉES

On combine les deux : l'asymétrique pour démarrer en sécurité, le symétrique pour la vitesse.

RÉSUMÉ VISUEL : SYMÉTRIQUE VS ASYMÉTRIQUE

	SYMÉTRIQUE (Bleu)	ASYMÉTRIQUE (Vert)
Nombre de clés	 **1** (Partagée)	 **2** (Paire)
Vitesse	 **RAPIDE**	 **LENT**
Partage de clé	 **DIFFICILE** (Risqué)	 **FACILE** (Sécurisé)
Usage principal	 **CHIFFREMENT DE DONNÉES**	 **ÉCHANGE DE CLÉS / AUTHENTIFICATION**

Le chiffrement est au cœur de la cybersécurité moderne.
On combine souvent les deux pour une sécurité optimale !