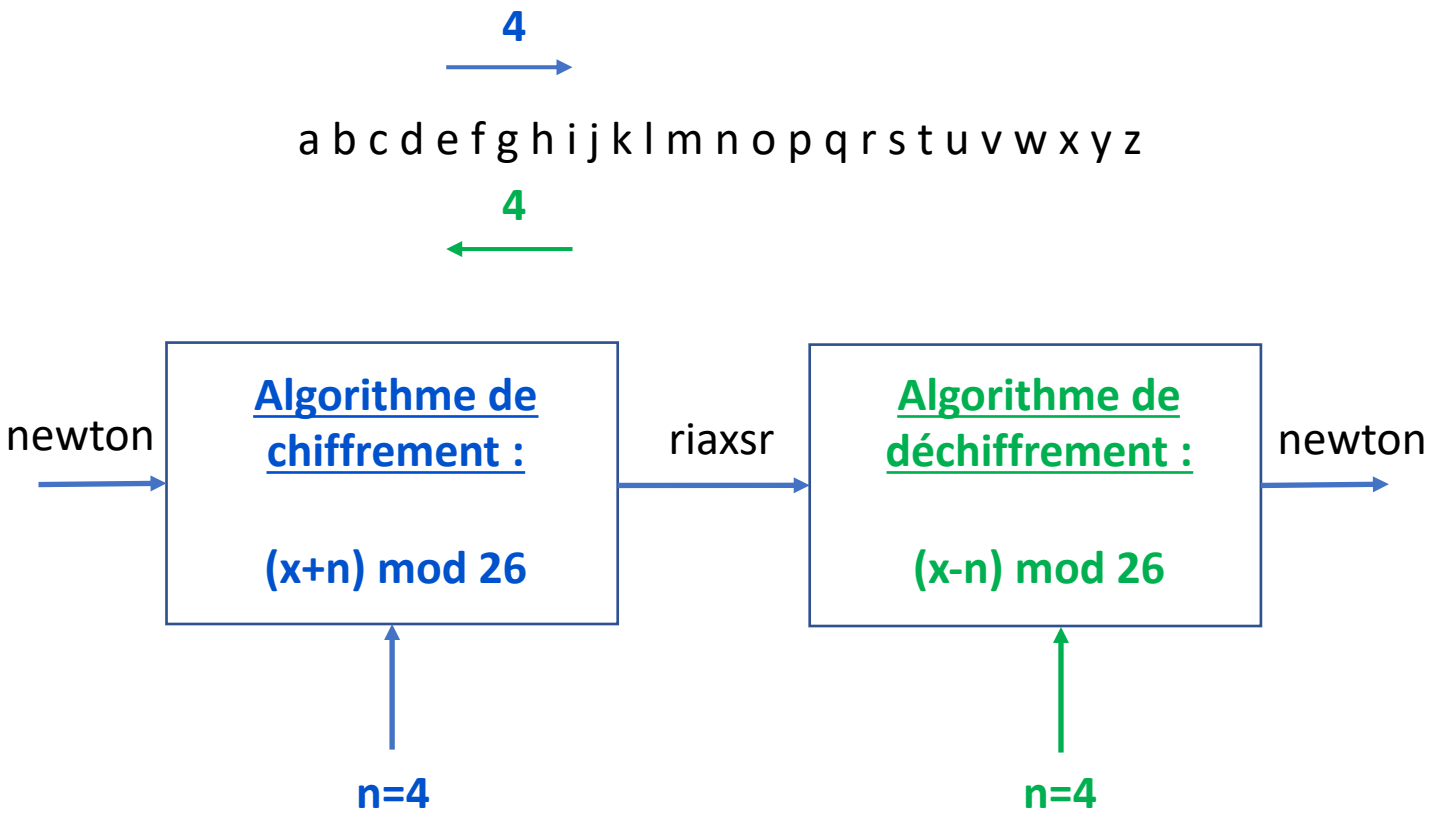
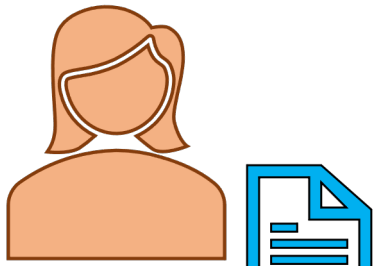
PRINCIPE DU CHIFFREMENT/DÉCHIFFREMENT SYMETRIQUE

On appelle ce chiffrement : code de césar ou chiffrement par décalage.

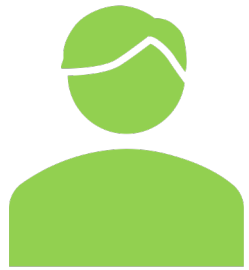


N est appelé la **clé de chiffrement**.
Dans le cas du chiffrement **symétrique**, la clé est identique pour le chiffrement et le déchiffrement.

CHIFFRAGE/DECHIFFRAGE SYMETRIQUE



ALICE



BOB

2. TRANSFERT DU FICHIER CHIFFRÉ

3. DECHIFFRAGE DU FICHIER AVEC LA CLÉ

1.CHIFFRAGE DU FICHIER AVEC LA CLÉ

CLÉ SYMÉTRIQUE UNIQUE

\+

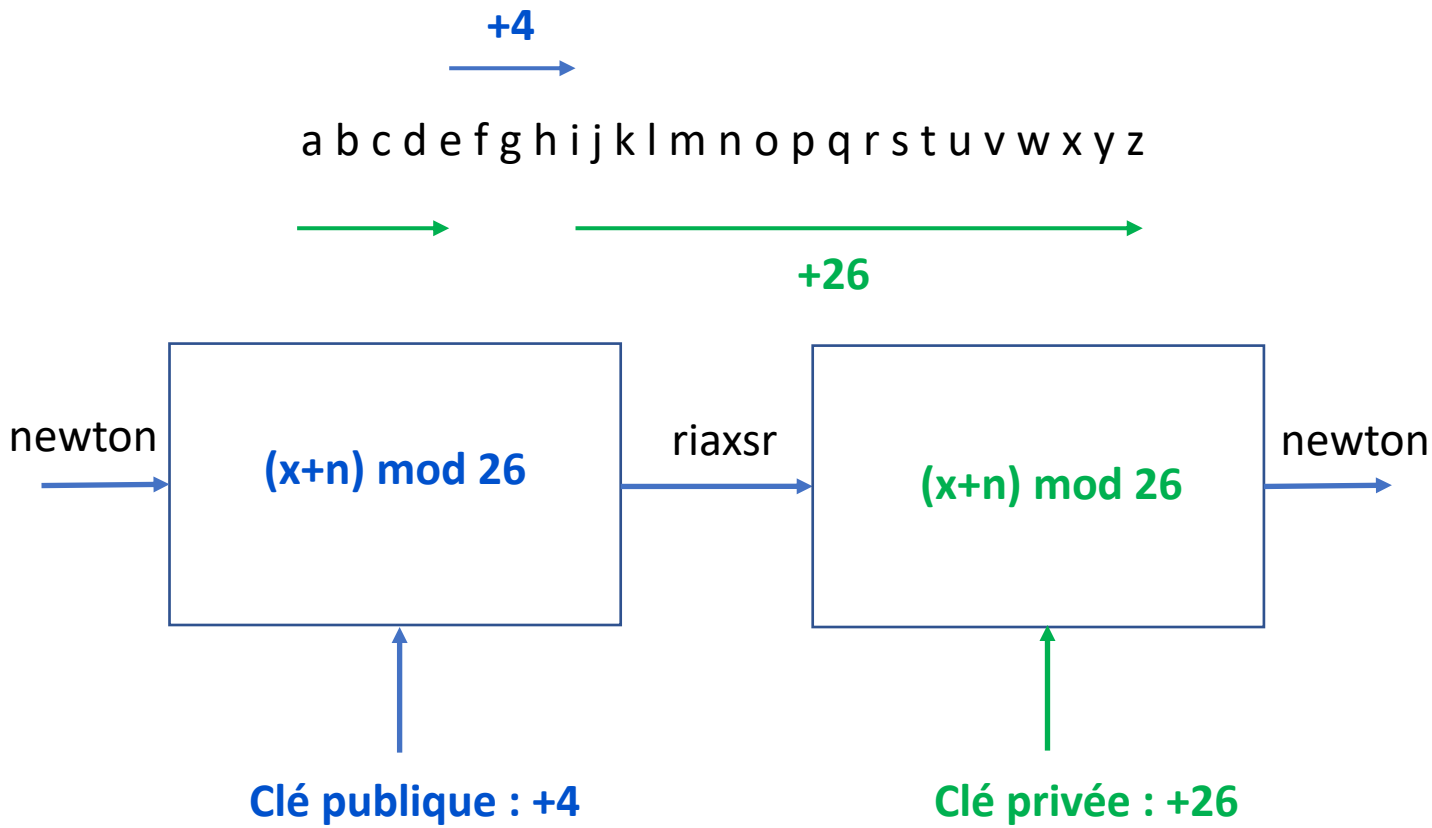
\+

CLÉ SYMÉTRIQUE UNIQUE

Cette technique est très simple, rapide et peu gourmande en ressource CPU.

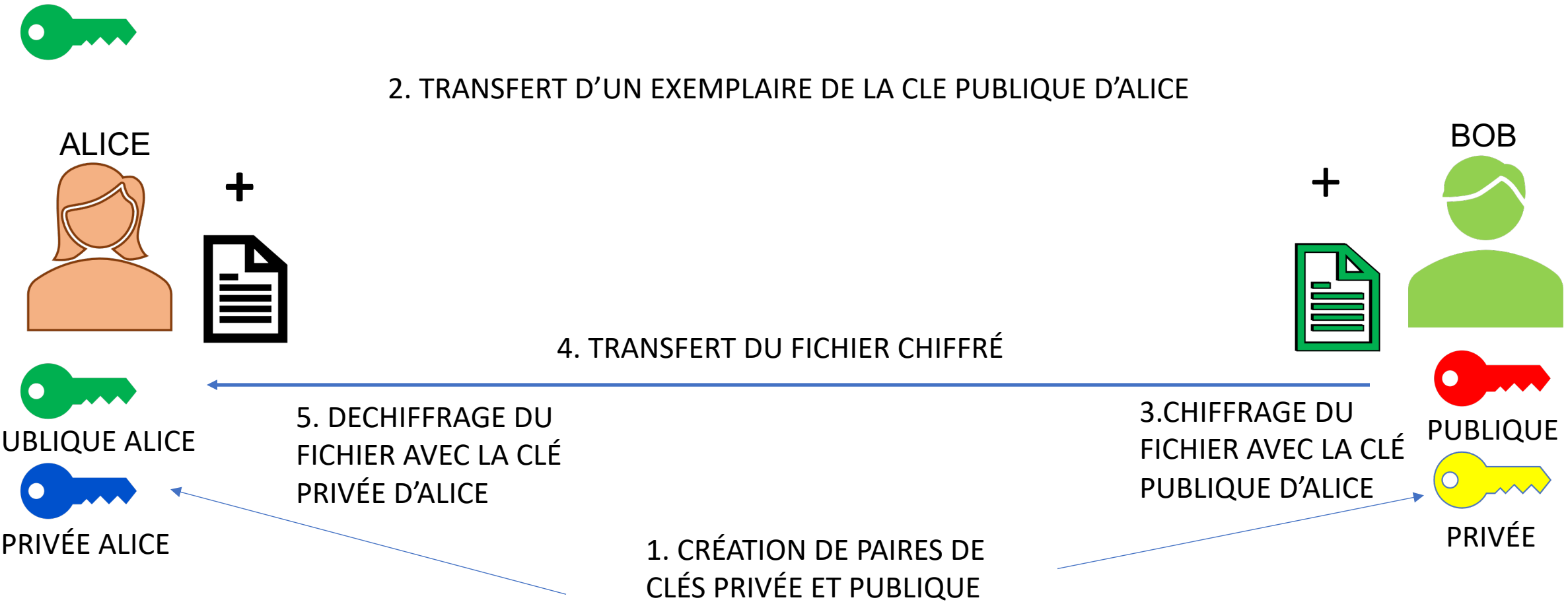
RISQUE DE VOL DE LA CLÉ DE CHIFFREMENT LORS DU PARTAGE DE LA CLÉ ENTRE LES 2 UTILISATEURS.

PRINCIPE DU CHIFFREMENT/DÉCHIFFREMENT ASYMETRIQUE



Les deux clés sont créées ensemble, on parle de paires de clé asymétriques

CHIFFRAGE/DECHIFFRAGE ASYMETRIQUE



Avantage : la technique de transfert est sécurisée. Seul la clé publique est visible. La clé privée n'est pas transmise.
Inconvénient : lent et gourmand en ressource CPU.