

## ACTIVITÉ 2 : chiffrement asymétrique

**Objectif :** en exécutant « à la main » un algorithme de **chiffrement asymétrique**, déterminer les avantages et les inconvénients de cette méthode de chiffrement.

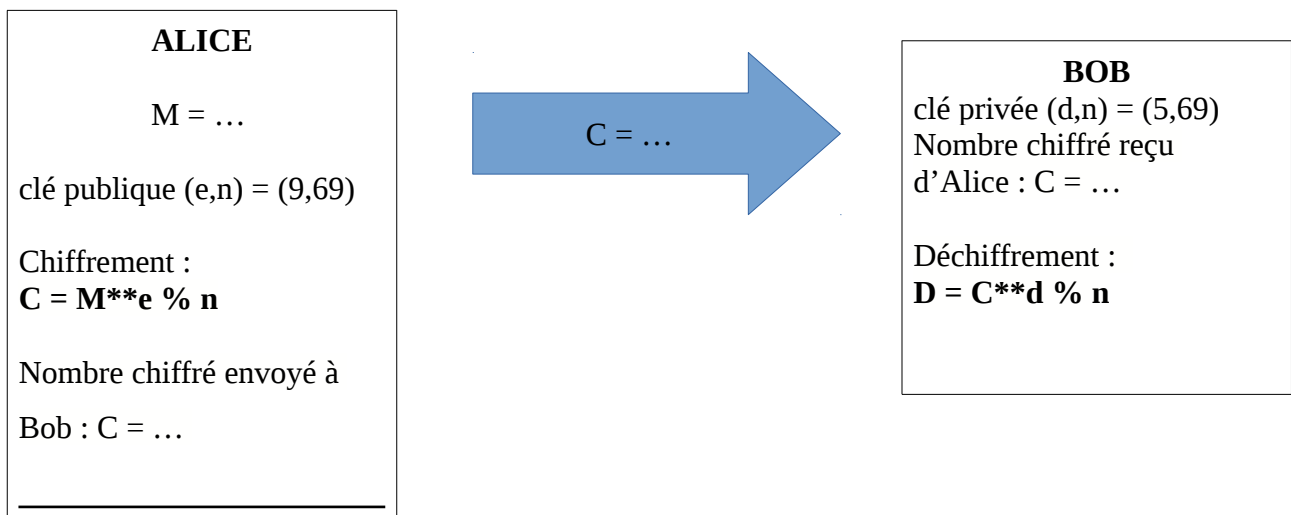
On utilise dans ce chiffrement la **clé publique**  $(e,n) = (9,69)$  et la **clé privée**  $(d,n) = (5,69)$ .  
Le principe du chiffrement asymétrique RSA est décrit dans la fiche méthode.

1. Par binôme :

- choisir un nombre entier M à chiffrer.** M doit être compris entre 0 et 68. Commencer par choisir un nombre entre 2 et 10, surtout si les calculs sont effectués à la calculatrice. Une fois les calculs terminés, il est possible de recommencer avec un nombre plus grand.
- Répartir les rôles dans le binôme :
  - Alice travaille uniquement avec la **clé publique (9,69)**,
  - Bob travaille avec la **clé privée (5,69)**

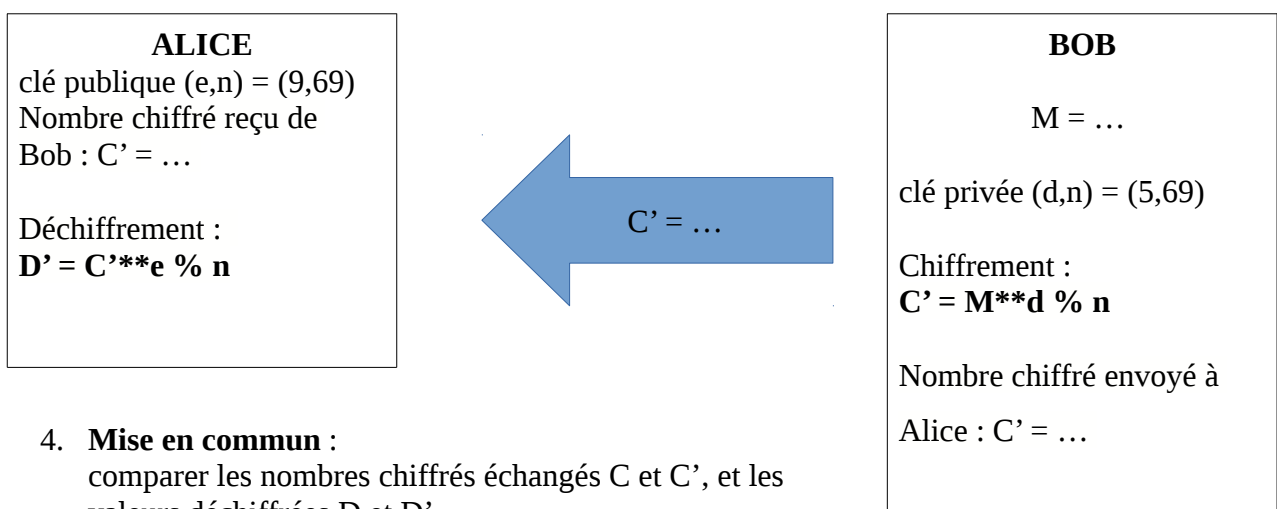
2. D'Alice vers Bob

- Alice chiffre le nombre M avec la clé publique et envoie le résultat C à Bob
- de son côté Bob déchiffre avec sa clé privée le nombre chiffré C reçu d'Alice.



3. De Bob vers Alice

- Bob chiffre le même nombre M avec sa clé privée et envoie le résultat C' à Alice
- Alice déchiffre avec la clé publique le nombre chiffré C' reçu de Bob



4. Mise en commun :

comparer les nombres chiffrés échangés C et C', et les valeurs déchiffrées D et D'.

	Avantage(s)	Inconvénient(s)
chiffrement symétrique		