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

ALICE

M = …

clé publique (e,n) = (9,69)

Chiffrement :
C = Me % n**

Nombre chiffré envoyé à Bob : C = …

C = …

BOB
clé privée (d,n) = (5,69)
Nombre chiffré reçu d'Alice : C = …

Déchiffrement :
D = Cd % n**

3. **De Bob vers Alice**
   a) Bob chiffre le même nombre M avec sa clé privée et envoie le résultat C' à Alice
   b) Alice déchiffre avec la clé publique le nombre chiffré C' reçu de Bob

ALICE
clé publique (e,n) = (9,69)
Nombre chiffré reçu de Bob : C' = …

Déchiffrement :
D' = C'e % n**

C' = …

BOB

M = …

clé privée (d,n) = (5,69)

Chiffrement :
C' = Md % n**

Nombre chiffré envoyé à Alice : C' = …

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		