CRYPTOPROJECT

BUT DE CE PROJET :

Créer un programme en ligne de commande, permettant de tester l'algorithme de *Merkle-Hellman.*
3 parties sont requises :

- Génération d'une clé publique
- Chiffrement d'un message
- Déchiffrement d'un message

LANCEMENT DES DIFFÉRENTES PARTIES :

```
 _____ _______    _______ _______ ____  _____  _____   ____      _ _____ _____ _______
/ ____|__   __\ \  / /  __ \__   __/ __ \|  __ \|  __ \ / __ \    | |  ____/ ____|__   __|
| |       | |   \ \/ /| |__) | | | |  | | |__) | |__) | |  | |   | | |__ | |       | |
| |       | |    > < |  ___/  | | | |  | |  ___/|  _  /| |  | |_  | |  __|| |       | |
| |____   | |   / . \| |      | | | |__| | |    | | \ \| |__| | |__| | |___| |____   | |
 \_____|  |_|  /_/ \_\_|      |_|  \____/|_|    |_|  \_\\____/ \____/|_____\_____|  |_|
Bienvenue sur le Crypto Project.
Faites votre choix :
1 - Génération de clé publique.
2 - Chiffrement d'un message.
3 - Déchiffrement d'un message
exit - Sortir du programme
>Votre choix :
```

PARAMÈTRES À FOURNIR :

```
> Votre choix : 1
Veuillez entrer le premier entier e.
PS : (cet entier est supérieur à 1 tout en étant inférieur et premier à 'm'):
>Premier entier e :
```

```
> Votre choix : 2
Veuillez entrer la clè S' sous le format x,y,z. (Ex : 1,2,5)
>Clé publique S' :
```

SCÉNARIO :

Les unites Américaines Bravo et Charlie sont sur le front Allemand durant la seconde guerre mondiale, elle ne peuvent parler que par radio mais les Allemands risquent de les espionner et de récupérer des informations capitales.

Pour eviter de perdre la guerre, elles decident de communiquer en utilisant l'algorithme de *Merkle-Hellman.*