

CryptoProject !

Dans ce test, nous allons avoir plusieurs situations ainsi que leurs résultats.

Léa décide d'utiliser CryptoProject pour générer une clé publique pour que les gens puisse lui envoyé des messages secrets.

Léa décide donc de lancer CryptoProject.

```

Vous avez choisi l'option Chiffrement d'un message

      _____
     /         \
    /           \
   /             \
  /               \
 /                 \
/                   \
\                   /
 \                 /
  \               /
   \             /
    \           /
     \         /
      _____

      _____
     /         \
    /           \
   /             \
  /               \
 /                 \
/                   \
\                   /
 \                 /
  \               /
   \             /
    \           /
     \         /
      _____

Bien le bonjour chers amis. Avez-vous pensé à lire le mode d'emploi fourni avec ?

Appuyez sur 1, 2 ou 3 en fonction de votre choix puis validez en appuyant sur Entrer.
Que voulez-vous faire ?
1. Génération d'une clé publique
2. Chiffrement d'un message
3. Déchiffrement d'un message
Entrez "exit" pour quitter le programme

```

Elle décide donc de Générer sa propre clé publique elle sélectionne la premiere option.

Le Programme lui demande alors de rentrer sa suite-supercroissante.

Ensuite les nombres e et m (cf. doc).

Elle obtient ainsi sa clé publique.

```
1
> Vous avez choisi l'option génération d'une clé publique

Veillez entrer une suite super croissante
1,2,5,10,20,50,100,200
Veillez entrer le nombre e
255
Veillez entrer votre nombre m
512
P : 2,8,1,7,6,5,4,3
Clé publique : 251,255,312,412,462,492,502,510
```

Léa décide donc de donner sa clé publique à tous ses amis.

Florian veut envoyer un message crypté à léa.

Il lance le programme et sélectionne l'option 2.

Le programme lui demande alors d'entrer son texte à crypté, il écrit JETAIME.

Par la suite, il doit fournir la clé publique que lui a donner léa.

il devras ensuite donner un nombre n (cf. doc).

Le programme va donc lui donner son texte crypté.

```
2
> Veuillez entrer le texte que vous voulez crypter :
JETAIME
Veuillez entrer la clé publique
251,255,312,412,462,492,502,510
Veuillez entrer le nombre n
6
Le message crypté est : 717,804,1025,774,462,774,1055,975,713,462
```

Il donne donc son message crypté à léa ~~et s'enfuit en courant.~~

Léa curieuse veut savoir ce que florian lui à envoyer, elle sélectionne donc l'option 3 du programme.

Le programme lui demande ensuite le nombre e,m, le message crypté, la permutation P, sa clé secrète S et sa clé n que Florian lui à donner.

Le programme va décrypter le message et afficher le résultat.

```
2
> Veuillez entrer le texte que vous voulez crypter :
JETAIME
Veuillez entrer la clé publique
251,255,312,412,462,492,502,510
Veuillez entrer le nombre n
6
Le message crypté est : 717,804,1025,774,462,774,1055,975,713,462
```

Ce résultat est La version parfaite de l'application.