CryptoProject

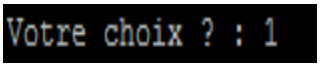
Bienvenue sur la documentation du projet de Nathan Van Hamelryck et de Laurent Gonnet. Ce dossier vous permettra d'utiliser notre interface étape par étape afin de pouvoir générer une clé, crypter/décrypter un message et de récupérer les clés privée et publique.

1. *L'interface*

Pour lancer le projet, il suffit de lancer le fichier cryptoproject.php en écrivant la ligne de commande suivante : php cryptoproject.php

Une fois cette commande effectuée, vous arriverez au menu du projet. Le menu est le suivant :

Il est donc possible via celui-ci de pouvoir choisir si on veut générer une clé publique, si on veut crypter un message ou si on veut le décrypter. Pour pouvoir choisir l'option qui nous intéresse, il suffit de taper le chiffre devant celle-ci. Par exemple, si nous voulons générer la clé publique, il suffit de taper « 1 » comme suit :



Ne pas oublier de taper sur la touche « Valider » pour confirmer votre choix.

2. *Génération d'une clé publique*

Pour générer la clé publique (choix n°1), plusieurs étapes sont nécessaires.

Etape n°1 : vous devez entrer une suite super croissante. Une suite super croissante est une suite où le $j^{ème}$ terme doit être plus grand que la somme des j-1 termes qui le précèdent dans la suite. Par exemple 1, 2, 5, 10, 20, 50, 100, 200 est une suite super croissante car :

- 1 + 2 < 5
- 1 + 2 + 5 < 10
- 1 + 2 + 5 + 10 < 20
- etc.

Tous les termes de la suite doivent être séparées par des espaces. Si les espaces ne sont pas présents ou si des lettres, caractères spéciaux, etc … sont présents, la suite ne sera pas validée. Voici ce que cela donne :

```
Entrer une suite super croissante séparé par des espaces (le jème terme doit être > que la somme des j-1 termes qui le précèdent dans la suite) : 1 2 5 10 20 100 200
```

Etape n°2 : vous devez entrer un terme m qui doit être supérieur à un certain terme. Dans le cas où vous avez choisi la super croissante ci-dessus, ce terme devra être supérieur à 338. Attention, si vous tapez un terme inférieur ou égal à 338 ou tout autre chose, cela vous affichera un message d'erreur :

```
Entrer m supérieur à 338 :
Chiffre incorect m doit être superieur a 338
Entrer m supérieur à 338 : 512
```

Etape n°3 : vous devez entrer un terme e qui doit être inférieur à 512 mais également différent de 0. Ce terme devra également être premier avec 512. Un nombre premier est un nombre qui est divisible par 1 et par lui-même. Un nombre premier « entre eux » sont deux nombres qui ne sont que divisibles par 1. Un exemple : 5 est un nombre premier car il n'est divisible que par 1 et par lui-même. Dans votre cas, et seulement si vous avez choisir la super croissante et le terme m ci-dessus, vous pouvez par exemple choisir 255 car 255 et 512 ne sont que divisibles par 1 :

```
Entrer e inférieur à 512 (!=0) de telle sort qu'il soit premier avec 512: 255
```

A la fin de ces trois étapes, vous devez voir afficher la clé intermédiaire (qui doit rester privée), la clé publique (que vous pouvez distribuer) et la permutation (à garder secret également). Vous devez également garder secret la suite super croissante et les termes e et m.

3. Chiffrement d'un message

Pour générer le chiffrement d'un message, vous devez également passer par plusieurs étapes.

Etape n°1 : vous devez entrer une clé publique (termes séparés par un espace) :

```
Entrer la clef public séparé par des espaces (ex: 512 888 965 1258) : 512 88 965
```

Etape n°2 : vous devez entrer le message qui doit être crypté (caractères minuscules et majuscules uniquement) :

```
Entrer le message a crypter : test
```

Etape n°3 : vous devez entrer un terme compris entre deux termes (par exemple : 2 et 3) :

```
Entrer un nombre comprit entre 2 et 3 inclus : 3
```

A la fin de ces trois étapes, vous devez avoir votre message crypté et un nombre n pour les packages.

4. *Déchiffrement d'un message*

Pour le déchiffrement d'un message, vous devez passer par plusieurs étapes. Attention, pour le déchiffrement, vous devez obligatoirement passer par la génération d'une clé publique (voir partie 2) et par le chiffrement du message (voir partie 3).

Etape n°1 : vous devez entrer la clé secret (la suite super croissante, séparée par des espaces)

Etape n°2 : vous devez entrer le terme e qui a été choisi durant la génération de la clé publique

Etape n°3 : vous devez entrer le terme m qui a été choisi durant la génération de la clé publique

Etape n°3 : vous devez entrer la permutation qui vous a été donné durant la génération de la clé publique (toujours séparé par des espaces)

Etape n°4 : vous devez entrer le nombre n qui correspond au découpage des paquets qui vous a été donné durant le chiffrement du message

Etape n°5 : vous devez entrer le message crypté (les termes numériques, séparés par des espaces) qui vous a été donné durant le chiffrement du message

Bien évidemment, si d'autres termes sont donnés ou si les termes ne sont pas conformes aux intitulés (lettres aux lieu de chiffres par exemple), un message d'erreur apparaitra.