# CryptoProject

## Documentation du projet CryptoProject




Réalisé par Florian DOUSSIN et Thomas NAKACHE

# Lancement du projet

## Comment démarrer ?

Pour démarrer le projet, exécutez la commande **php cryptoquest.php**

Cela va démarrer le programme. Un menu va apparaître ou vous allez pouvoir accéder à :

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

Il vous suffira d'entrer 1, 2 ou 3 en fonction de l'option que vous voudrez exécuter.

Si vous voulez quitter le programme à tout moment, il vous suffira d'entrer « exit ».

# Génération de clé publique

La clé publique vous servira ensuite pour chiffrer un message. Lorsque vous avez sélectionné l'option Génération clé publique, on vous demande d'entrer une suite super-croissante.

1. Vous aurez à entrer cette suite sous la forme : 1,2,3,4,5…

Une suite super-croissante est une suite dont l'addition des nombres précédents est toujours inférieur au nombre suivant.

Voici un exemple de suite super-croissante : 1,2,5,10,20,50,100,200.. (exemple avec des pièces de monnaie en Euro).

Vous entrez donc votre suite super-croissante avec chaque nombre séparé UNIQUEMENT par une **virgule** (voir l'exemple ci-dessus) puis appuyez sur Entrer.

2. Ensuite, vous aurez à entrer les nombres « E » et « M »

« E » doit être inférieur à « M » mais supérieur à 1.

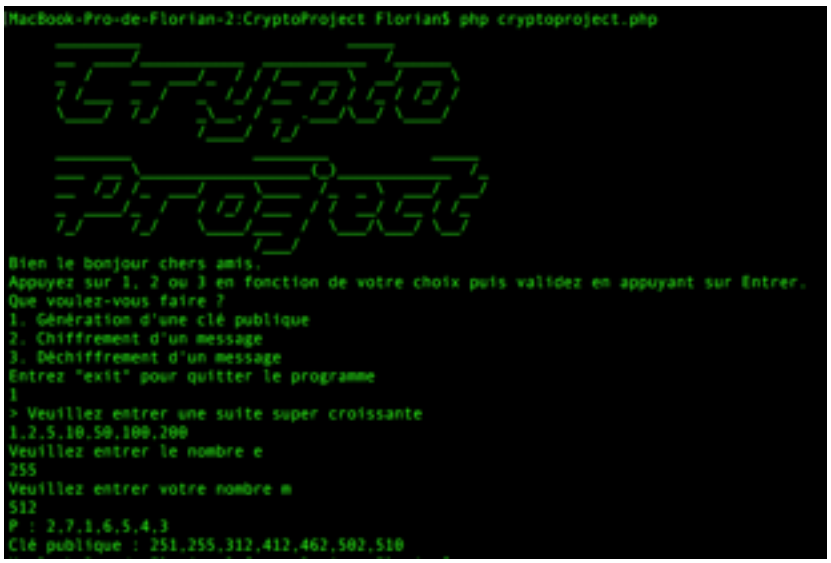
« M » doit être supérieur à l'addition de tous les termes de notre suite super-croissante.

De plus, « E » et « M » doivent toujours être **premiers entre eux**, c'est à dire que « M » et « E » doivent avoir leur plus grand diviseur commun égal à 1. En d'autres termes, ils ne doivent avoir aucun autre diviseur que 1 et -1 en commun.

Exemple : 255 et 512 sont premiers entre eux.

Une fois tout ceci entré, vous pourrez obtenir votre clé publique (pensez à la stocker !).

Voici un exemple illustrant l'utilisation du programme :



# Chiffrement d'un message

Vous avez choisi l'option Chiffrement d'un message en appuyant sur « 2 ». Ici, vous allez devoir entrer le message que vous voulez chiffrer pour le faire ressortir en message crypté.

Déroulement du programme :

Il vous est tout d'abord demandé de rentrer votre texte à chiffrer. À vous de rentrer ce que vous voulez.

Vous devez ensuite entrer votre clé publique. C'est la clé que vous avez récupéré précédemment (voilà l'importance de la stocker ou la mémoriser quelque part !) en créant une clé publique (oui c'est là qu'elle va vous servir !).

Enfin, vous devrez rentrer un nombre « n ». Le nombre « n » est un nombre utilisé pour le découpage du chiffrement du message. Le nombre « n » doit être compris entre 4 et le nombre de caractères compris dans votre texte à chiffrer. À vous de rentrer un chiffre compris entre ces chiffres là.

Voici un exemple du déroulement de l'exécution du programme :


Vous entrez le texte que vous voulez crypter, ici « PREPETNA » puis notre clé publique obtenue précédemment et enfin le nombre « n » et nous obtenons enfin le message crypter.

# Déchiffrement d'un message

Vous avez choisi l'option déchiffrement d'un message. Cette option permet de déchiffrer un message crypté grâce à notre algorithme. Vous devrez donc suivre un processus similaire à l'option Chiffrement d'un message mais pour le déchiffrement cette fois.

Vous arrivez sur l'écran et choisissez cette option en appuyant sur « 3 ».

On vous demande dans un premier temps de rentrer « e » et « m ». « e » et « m » comme pour la génération de la clé publique, doivent être premiers entre eux donc avoir un plus grand diviseur commun égal à 1. Vous pouvez réutiliser les même.

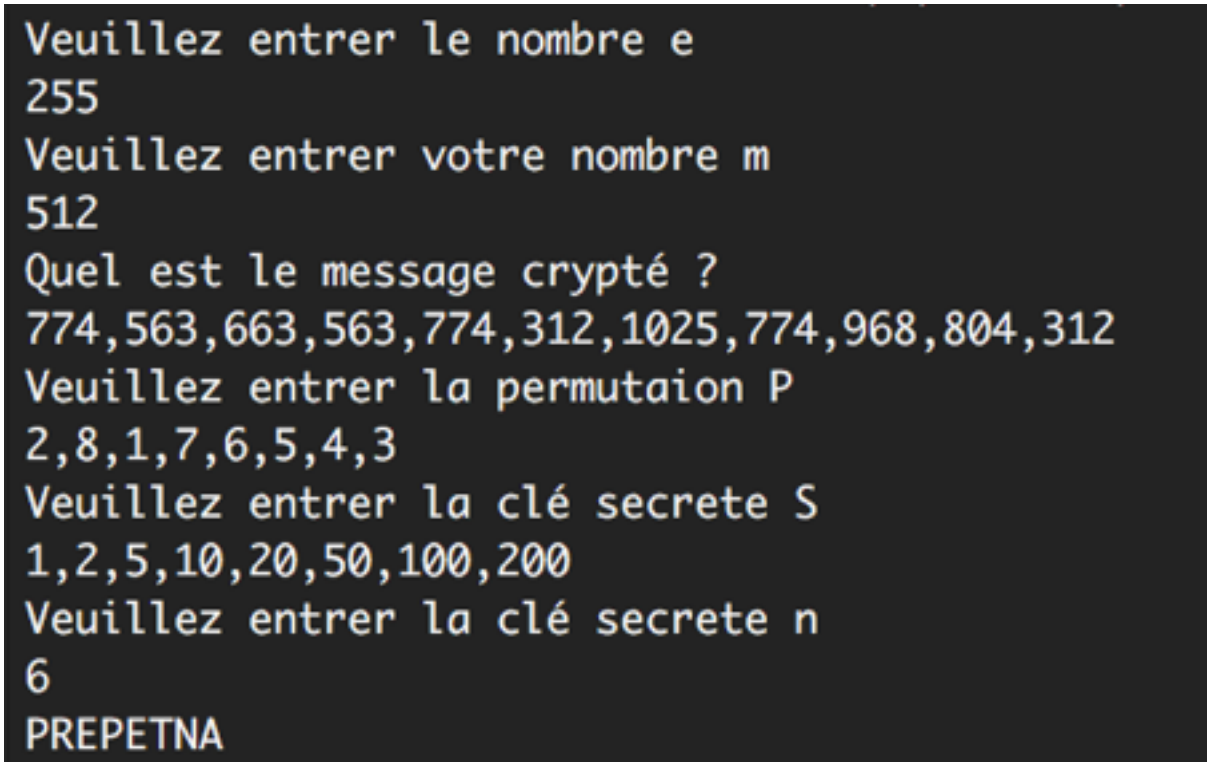
Ensuite, vous devrez rentrer le message crypté. Le message crypté à entrer est celui qui vous avez reçu depuis l'option Chiffrement d'un message et au même format.

Puis, vous aurez à rentrer la Permutation P. Cette permutation P a été obtenue lors de la Génération de la clé publique en même temps que la clé publique. Tout comme le message crypté, vous devez la rentrer au même format que le format obtenu (Nombre1,Nombre2,Nombre3,etc.)

Ensuite, il faut rentrer la clé secrète S. C'est la clé (super-croissante) qui a été utilisée pour la génération de la clé publique. À vous de la rentrer de nouveau !

Enfin, vous devrez rentrer votre clé secrète « n ». C'est le nombre « n » utilisé pour le chiffrement.

Une fois ceci rempli, vous allez obtenir votre message décrypté ! Comme ceci :




Pensez à bien respecter le format d'entrée des informations sinon cela ne marchera pas !

Bonne utilisation ;)