

Scénario

Deux étudiants Nour et Soul voulant communiquer entre eux sont observés par un pirate informatique, lui aussi étudiant de la même école, qui intercepte les messages envoyés via une application de messagerie où les messages ne sont pas chiffrés.

La version de l'OS du téléphone de Nour étant trop ancienne, il ne peut télécharger une nouvelle application.

Après une heure de conversation au contenu non sensible, Soul questionne Nour à propos de l'identité de sa petite-ami. Nour ne voulant pas révéler en public l'identité de sa bien-aimée, qui n'est d'autre que la directrice de l'établissement, décide de trouver un moyen de communiquer l'identité de cette dernière. Nour étant en voyage à l'étranger, il ne pourra pas rencontrer physiquement Soul avant 2030 ! Heureusement que ces derniers connaissent le programme Crypto Project.

Soul décide donc de générer une clé publique, qu'il enverra dans un premier temps à Nour. Le pirate ne peut rien faire avec ces informations sans la permutation et les entiers 'e' et 'n' que Soul aura gardé précieusement de son côté.

```
hab_i_a@MSI: /mnt/c/Users/
hab_i_a@MSI:/mnt/c/Users/habiy/Documents/ETNA/cryptoproject$ ./cryptoproject.php
CRYPTOPROEJCT

Faites votre choix :
1 - Génération de clé publique.
2 - Chiffrement d'un message.
3 - Déchiffrement d'un message
4 - Sortir du programme

choix: 1
Veuillez entrer la clé secrete
clé secrete: 1,2,5,10,20,50,100,200
Veuillez entrer le premier entier m :
m : 512
Veuillez entrer le deuxieme entier e:
e: 255

-----
e: 255, m: 512
Your secret key: "1, 2, 5, 10, 20, 50, 100, 200"
Your public key S': "251, 255, 312, 412, 462, 492, 502, 510"
Your permutation: "2, 8, 1, 7, 6, 5, 4, 3"
-----
```

Nour va donc chiffrer l'identité de sa petite-ami grâce à la clé publique de Soul et l'envoyer, avec également le nombre n qu'il aura choisi.

Nour envoie ainsi le message chiffré et le nombre n à Soul.

```
hab_i_a@MSI: /mnt/c/Users/habiy/Documents/ETNA/cryptoproject$ ./cryptoproject.php
CRYPTOPROJECT

Faites votre choix :
1 - Génération de clé publique.
2 - Chiffrement d'un message.
3 - Déchiffrement d'un message
4 - Sortir du programme

choix: 2
Veuillez entrer la clé publique S'
S' : 251,255,312,412,462,492,502,510
Veuillez entrer la chaine à chiffrer
Message: la directrice
Veuillez entrer l'entier n.
n : 6

-----
n: 6
Your crypted message: 1380 567 312 492 1125 567 1055 1209 1125 1029 975 1266 1186 1059 1055 998 1125 462
-----
```

Soul va alors déchiffrer le message de Nour via le nombre n et les paramètres qu'il aura gardé au chaud, et découvrira l'identité de la copine à Nour.

```
hab_i_a@MSI: /mnt/c/Users/habiy/Documents/ETNA/cryptoproject$ ./cryptoproject.php
CRYPTOPROJECT

Faites votre choix :
1 - Génération de clé publique.
2 - Chiffrement d'un message.
3 - Déchiffrement d'un message
4 - Sortir du programme

choix: 3
Veuillez entrer la clé secrete
clé secrete: 1,2,5,10,20,50,100,200
Veuillez entrer le premier entier m :
m : 512
Veuillez entrer le deuxieme entier e:
e: 255
Veuillez entrer la permutation P
P: 2,8,1,7,6,5,4,3
Veuillez entrer la chaine à dechiffrer
message: 1380 567 312 492 1125 567 1055 1209 1125 1029 975 1266 1186 1059 1055 998 1125 462
Veuillez entrer l'entier n.
n : 6

-----
The message: la directrice
-----
```

Le pirate ne connaissant que la clé publique de Soul, le message crypté et le nombre 'n', il ne peut déchiffrer le message :

```
hab_i_a@MSI: /mnt/c/Users/habiy/Documents/ETNA/cryptoproject$ ./cryptoproject.php
CRYPTOPROJECT

Faites votre choix :
1 - Génération de clé publique.
2 - Chiffrement d'un message.
3 - Déchiffrement d'un message
4 - Sortir du programme

choix: 3
Veuillez entrer la clé secrete
clé secrete: 1,2,4,10,40,100
Veuillez entrer le premier entier m :
m : 1222
Veuillez entrer le deuxieme entier e:
e: 127
Veuillez entrer la permutation P
P: 1,2,3,5,4,6
Veuillez entrer la chaine à dechiffrer
message: 1380 567 312 492 1125 567 1055 1209 1125 1029 975 1266 1186 1059 1055 998 1125 462
Veuillez entrer l'entier n.
n : 6

-----
The message:
-----
```

Le message est vide ! La réputation de Nour est donc sauvée et Soul a bien pris connaissance de l'information top secrète !