

SCÉNARIO :

CRYPTOPROJECT

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

Pour éviter de perdre la guerre, elles décident de communiquer en utilisant l'algorithme de Merkle-Hellman.

Bravo veut envoyer un message à Charlie contenant l'heure de l'offensive, impossible de le dire clairement à la radio.

Les Allemands les piégeraient et les pertes seraient considérables.

Charlie doit donc générer une clé :

```
CRYPTOPROJECT
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 : 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 : 255
Veuillez entrer le second entier m :
>Second entier m : 512
Veuillez entrer la clé secrète S sous le format x,y,z. (Ex : 1,2,5)
>Clé super croissante S : 1,2,5,10,20,50,100,200
Génération de la clé publique
Clé publique générée !
La clé publique est : 251,255,312,412,462,492,502,510
```

Charlie envoie donc la clé à Bravo. Bravo crypte le message avec la clé envoyée grâce au programme.

```
Faites votre choix :
1 - Génération de clé publique.
2 - Chiffrement d'un message.
3 - Déchiffrement d'un message
exit - Sortir du programme
>Votre choix : 2
Veuillez entrer la clé S' sous le format x,y,z. (Ex : 1,2,5)
>Clé publique S' : 251,255,312,412,462,492,502,510
Veuillez entrer la chaîne à chiffrer
(PS : Elle doit être uniquement composée de lettres et d'espaces.)
>Message : attaque a huit heures STOP
Veuillez entrer l'entier n.
PS : (cet entier devra être supérieur à 2 et inférieur au nombre total de terme de S': 8):
>Entier n : 6
Votre message crypté est :874 1280 713 1266 874 1280 563 1517 1125 1029 563 904 1437 1029 1055 1266 1129 567 1025 1517 1186 1059 1025 1460 774 1517 713 1230 774 0
```

Charlie le récupère le décode et a donc l'heure