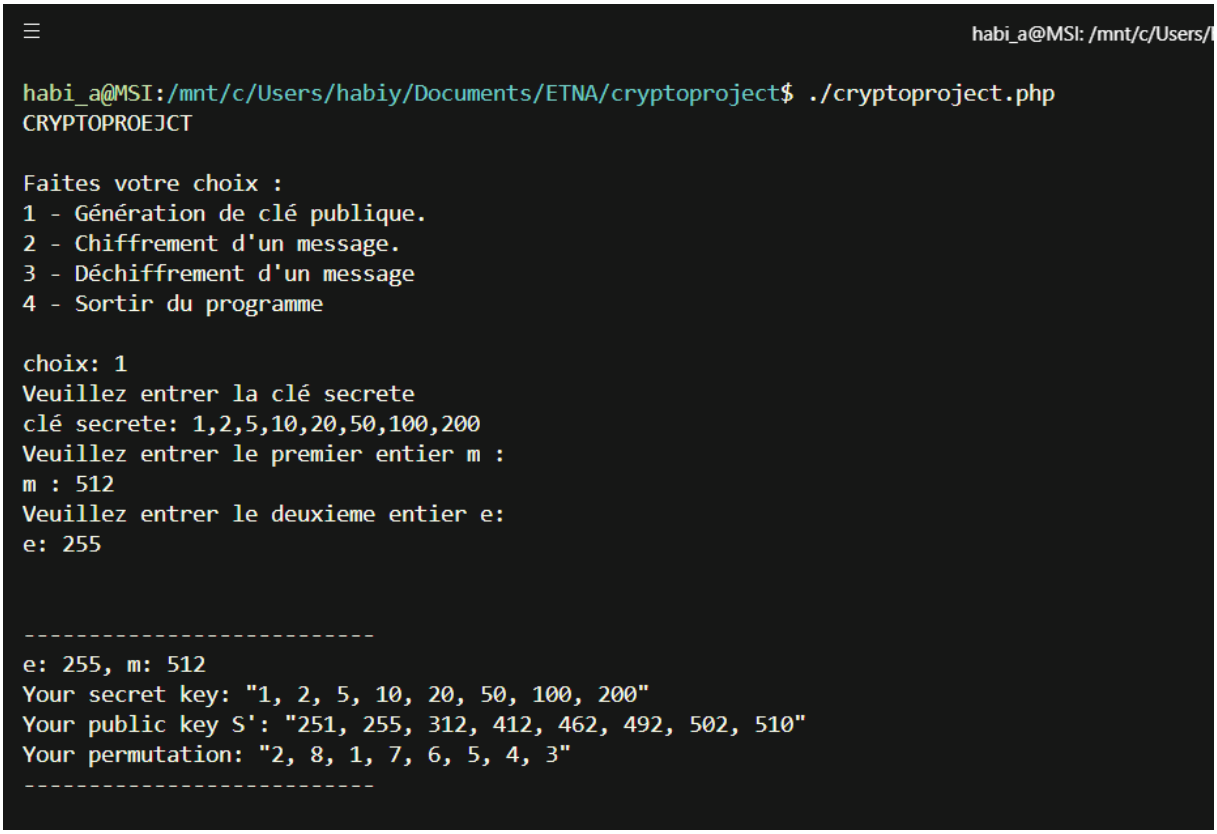
 # Scénario

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.

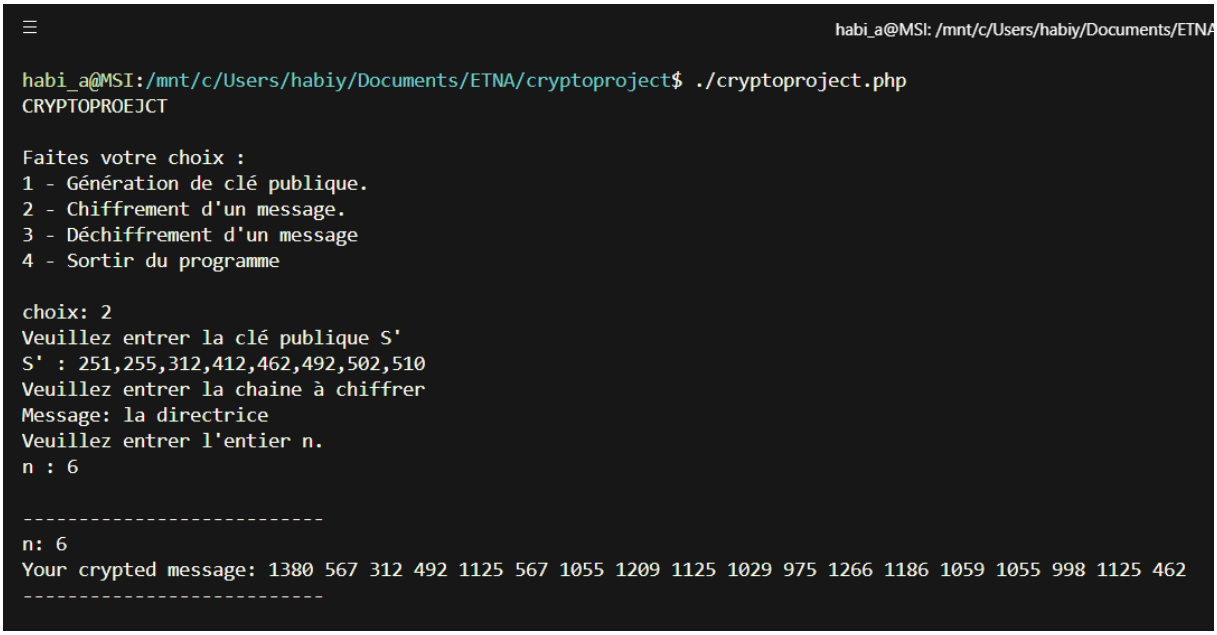
Après une heure de conversation au contenu non sensible, Soul questionne Nour à propos de l'identité de sa petite-ami. Nour ne voulant pas révéler en public l'identité de sa bien-aimée, qui n'est d'autre que la directrice de l'établissement, décidé de trouver un moyen de communiquer l'identité de cette 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.

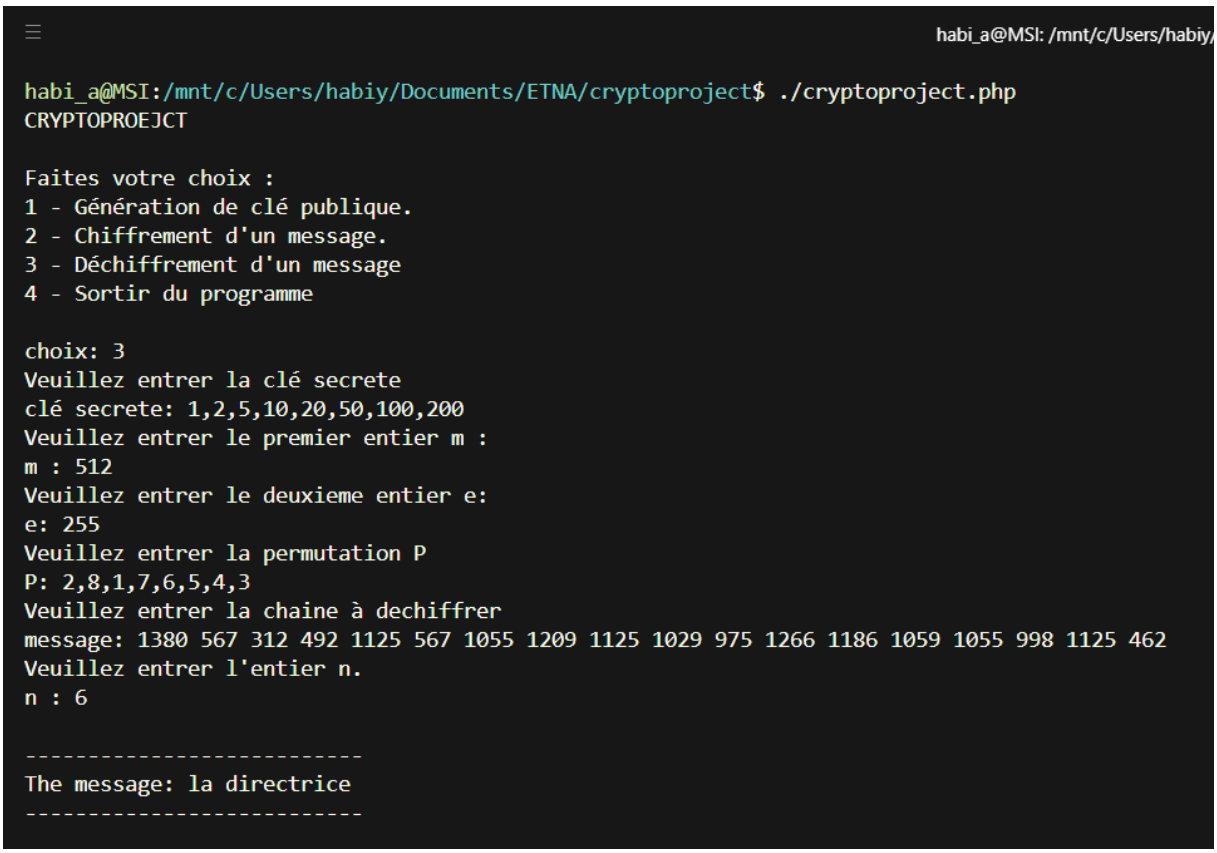


Nour va donc chiffrer l'identité de sa petite-ami grâce à la clé publique de Soul et l’envoyer, avec également le nombre n qu'il aura choisi.

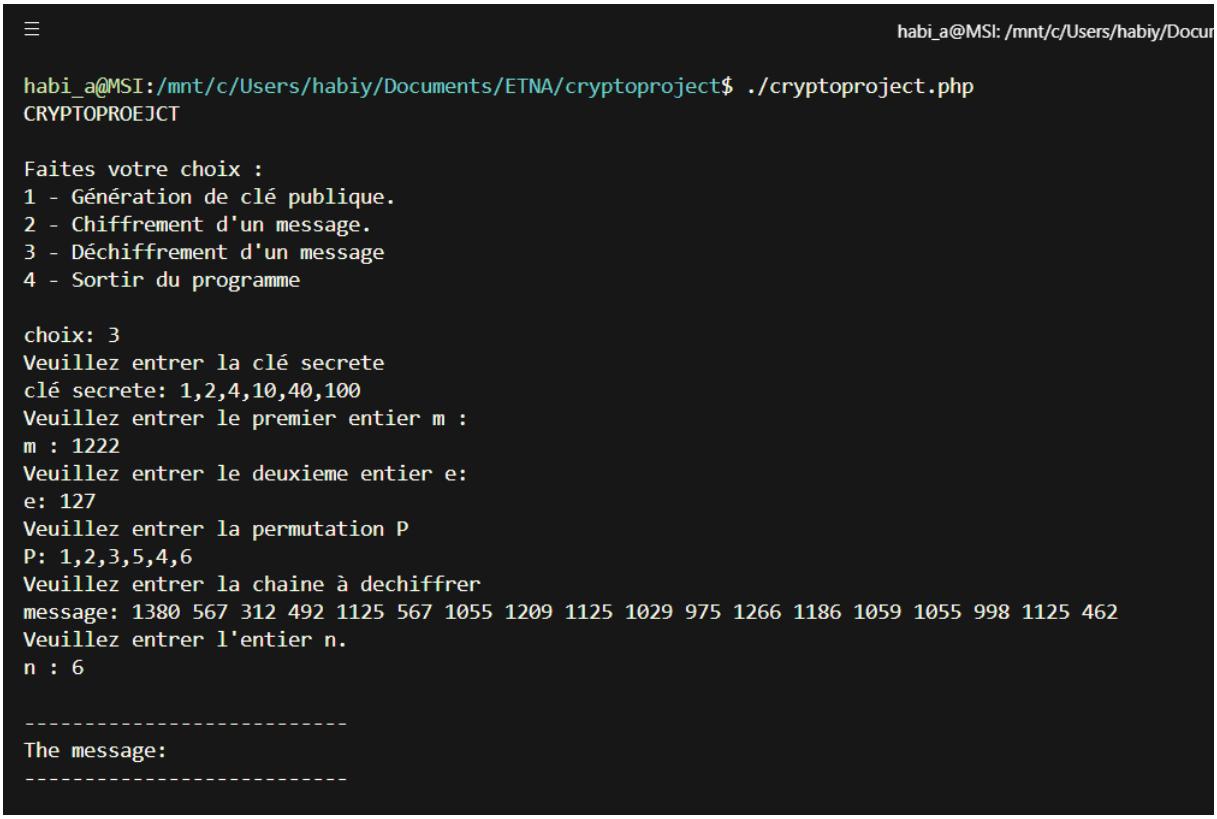
Nour envoie ainsi le message chiffré et le nombre n à Soul.



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.



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



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