SCÉNARIO :

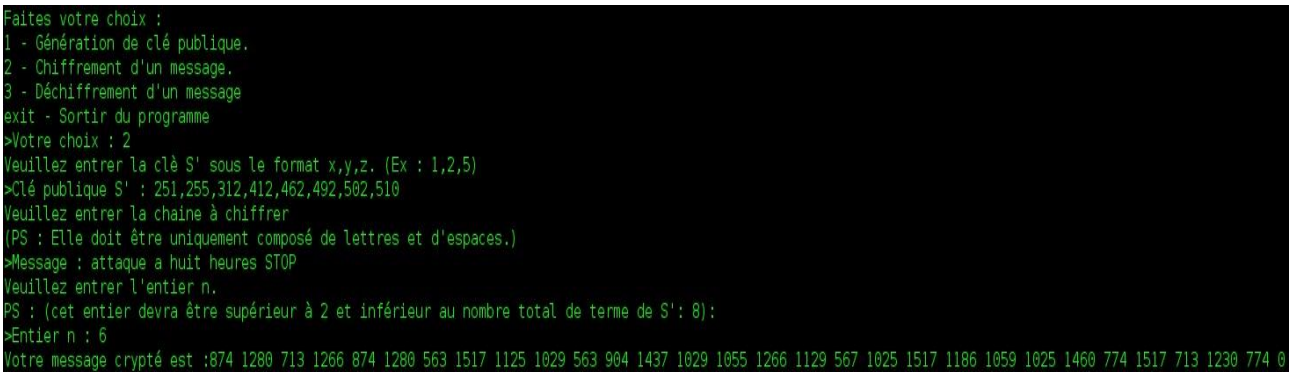
CRYPTOPROJECT

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

Pour eviter de perdre la guerre, elles decident 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 :

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



Charlie le récupère le décode et a donc l’heure