

```
OpenSSL> genrsa -help
OpenSSL> genrsa 1024
La paire de clé est généré et affiché à l'écran, pour la sauvegarder dans
un fichier on utilise l'option -out
OpenSSL> genrsa -out ahmed.key 1024
Il vous ait demandé de visualiser le contenu du fichier ahmed.key
```

```
OpenSSL> genrsa -des3 -out ahmed.key 1024
la clé privé est chiffré ici avec un triple DES
Créer un fichier nomme "rand.txt" contenant n'importe quoi...
OpenSSL> genrsa -des3 -out ahmed.key -rand rand.txt 1024
```

```
Verification de la clé privée RSA :
OpenSSL> rsa -in ahmed.key
OpenSSL> rsa -in ahmed.key -check
OpenSSL> rsa -in ahmed.key -check -modulus
OpenSSL> rsa -in ahmed.key -check -modulus -text
```

```
Extraction de cle publique RSA :
OpenSSL> rsa -in ahmed.key -pubout -out ahmed.pub
```

```
Vérification de clé publique RSA :
OpenSSL> rsa -pubin -in ahmed.pub -text
```

Question 1:

Générer une paire de clé RSA d'une taille de 1024 bits.

Réponse :

```
OpenSSL> genrsa -aes256 -out ahmed.key 1024
```

Question 2 :

En utilisant la commande RSA analyser la paire de clés générée précédemment.

Réponse :

```
OpenSSL> rsa -in ahmed.key -text
```

Question 3 :

Extraire la clé publique de la paire de clé.

Réponse :

```
OpenSSL> rsa -in ahmed.key -pubout -out ahmed.pub
```

Partie 4 : Services à base de cryptographie :

Question 1 :

En utilisant la commande dgst et une clé privée, produire la signature d'un fichier. Analyser le résultat obtenu.

Réponse : ahmed.key représente ma clé privé

```
Openssl>dgst -sign ahmed.key -binary -out openssl.sig openssl.exe
```

Question 2 :

Vérifiez la signature précédente en utilisant la clé publique.

Réponse : ahmed.key représente ma clé privé et ahmed.pub ma clé publique

```
Openssl>dgst -verify ahmed.pub -signature openssl.sig openssl.exe
```

Question 3 :

Utiliser la commande speed pour établir un benchmark de l'api Openssl relatif à votre machine

Réponse :

```
Openssl> speed rsa1024 rsa2048
```