Aide-Mémoire

Comme il s'agit d'une API assez vaste (mais cohérente), il faudra bien utiliser la documentation ci-dessous :

Système : station DORANCO ou VM Kali-Linux avec openssl

Ligne de commande : https://www.madboa.com/geek/openssl/

Guide pratique sur les certificats : https://guidespratiques.traduc.org/vf/SSL-Certificates-HOWTO.html

Syntaxe générale :

```
openssl commande -option -in fichierentree -out fichiersortie
```

Il est possible de faire travailler sur l'entrée standard (noter le -n pour ne pas avoir de \n rajouté)

```
echo -n "message à encoder" | openssl enc -base64
```

Algorithmes de base

Encodage

Encoder vos prénom et nom de famille en

- Hexadécimal
- Binaire
- Base64

Hachage

Hacher vos prénom et nom de famille en

- MD5
- SHA-1
- SHA-256
- RIPE-MD160

Certificats X509

Certificats CNRS et le Certificat de Godard

Effectuer les commandes suivantes.

```
openssl x509 -text -in CNRS2.pem
```

```
openssl verify -CAfile CNRS2.pem -purpose any CNRS2.pem
```

```
openssl x509 -text -in CNRS2-Standard.pem
```

```
openssl verify -CAfile CNRS2.pem -purpose any CNRS2-Standard.pem
```

```
openssl verify -CAfile CNRS2.pem -purpose any godard.pem
```

```
openssl verify -CAfile CNRS2-Standard.pem -purpose any godard.pem
```

```
cat CNRS2.pem CNRS2-Standard.pem > chaine.pem
```

```
openssl verify -CAfile chaine.pem -purpose any godard.pem
```

Expliquer.

La clé publique de Godard est-elle authentique ?