TP : Cryptographie RSA et protocole HTTPS

Les modules Python os et subprocess permettent sur les systèmes d'exploitation **windows** et **linux** d'agir sur eux avec différentes méthodes qu'ils proposent. Par exemple :

Le module os

Le moduleos permet dans un script Python d'exécuter des commandes au niveau système. La documentation complète est à l'adresse "https://docs.python.org/fr/3/library/os.html"

— La méthode system() permet d'exécuter une commande ou une application. Par exemple, l'ouverture de bloc-notes

```
1 os.system("C:/windows/notepad.exe")
```

— La méthode getcwd() renvoie le répertoire courant.

```
1 directory = os.getcwd()
```

— La méthode startfile() ouvre le fichier spécifié en paramètre avec l'application dédiée par défaut.

```
1 os.startfile("..\code_cesar.pdf")
```

— La méthode listdir() renvoie le contenu du répertoire passé en paramètre dans une liste. Le répertoire courant si aucun argument passé.

```
1 os.listedir("C:/Users/eleve/")
```

Le module subprocess

Le module subprocess permet dans un script Python d'exécuter des commandes au niveau système. La documentation complète est à l'adresse "https://docs.python.org/fr/3/library/subprocess.html"

— La méthode run(args) permet d'exécuter un programme. Le paramètre args est une liste contenant le programme à exécuter et les éventuels options à ajouter.

```
1 subprocess.run(["mspaint","C:\\Users\\bob\\gary.png"])
```

— La méthode Popen(args) permet d'exécuter un programme. Le paramètre args est une liste contenant le programme à exécuté et les éventuels options à ajouter.

```
1 subprocess.Popen(["mspaint","C:\\Users\\bob\\gary.png"])
```

Partie A

1) Dans la console Python, lancez avec le module os le programme de dessin de windows.

2) Dans la console Python, lancez avec le module subprocess le bloc-notes de windows.

Partie B

1) Aller sur le site www.python.org avec un navigateur de votre choix.

a) Le protocole utilisé est-il sécurisé ? Justifier.

b) Quelle est l'autorité de certification du site ?

c) Quel est l'algorithme utilisé pour chiffrer la communication ?

d) Quel est la taille de la clef publique utilisée ?

2) Le certificat est un fichier d'extension pem.

a) Télécharger ce fichier.

b) Quelle est la première et la dernière ligne de ce fichier ?

3) Le navigateur affiche toutes les données contenues dans le certificat. Il est possible d'extraire ces données avec un logiciel dédié comme OpenSSL

a) Si OpenSSL est installé, tapez en console la commande :

```
openssl x509 -in "fichier" -noout -text
```

Si tout ce passe bien, vous obtenez les même informations que dans le navigateur.

b) On peut aussi extraire la clé publique du certificat avec la commande :

```
openssl x509 -in "fichier" -noout -pubkey
```

4) Écrire les commandes en Python et obtenez les mêmes valeurs.