



**Ecole nationale supérieure de l'intelligence
artificielle et sciences des données
Taroudant.**

Filière : SITCN

Cryptographie appliquée

Thème :

TP N1 : OpenSSL

Réaliser par:

Zouhair GUERTAOU

Encadré par:

Mr. Hasnae Al-amrani

Objectif

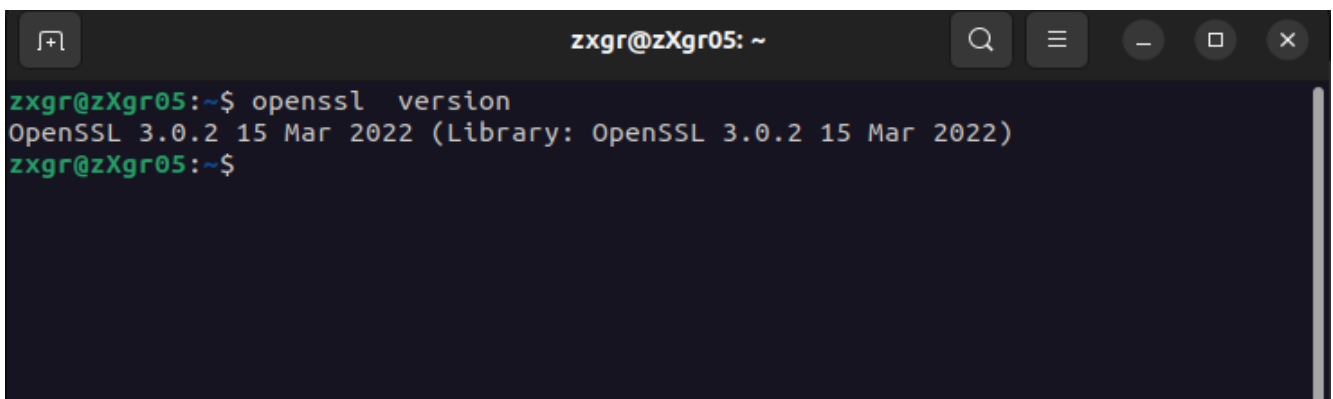
- Se familiariser avec les fonctionnalités et la bibliothèque openssl
- Génération et utilisation des Clés secrètes
- Chiffrement de données via les commandes de la bibliothèque openssl

Outils

- Système Windows ou Linux
- Bibliothèque openssl

Préparation de l'environnement de travail

Verification de l'existence du bibliotheque openssl sur **Ubuntu** :

A terminal window with a dark background. The title bar shows 'zxgr@zXgr05: ~' and standard window controls. The terminal text shows the command 'openssl version' being executed, resulting in the output 'OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)'. The prompt 'zxgr@zXgr05:~\$' is visible before and after the command.

```
zxgr@zXgr05:~$ openssl version
OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
zxgr@zXgr05:~$
```

Sur Windows

- Sur la machine Windows du lab de test (virtual box) ou sur votre machine :
- Telecharger la bibliothèque openssl .
- Une fois téléchargé, décompressé le dossier et placer le sur le disque C:\
- Ajouter le chemin : C:\OpenSSL\bin au variable utilisateur path

Variables d'environnement

Variables utilisateur pour HP

Variable	Valeur
OneDrive	C:\Users\HP\OneDrive
Path	C:\Users\HP\AppData\Local\Microsoft\WindowsApps;C:\User...
PTSHOME	C:\Program Files (x86)\Packet Tracer 5.2
TEMP	C:\Users\HP\AppData\Local\Temp
TMP	C:\Users\HP\AppData\Local\Temp

Nouvelle...

Modifier...

Supprimer

Variables système

Variable	Valeur
ComSpec	C:\Windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
JAVA_HOME	C:\Program Files\Java\jdk-23
NUMBER_OF_PROCESSORS	12
OS	Windows_NT
Path	C:\Program Files\Common Files\Oracle\Java\javapath;C:\Prog...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64

Nouvelle...

Modifier...

Supprimer

OK

Annuler

Modifier la variable d'environnement

%USERPROFILE%\AppData\Local\Microsoft\WindowsApps

C:\Users\HP\AppData\Local\Programs\Microsoft VS Code\bin

C:\Users\HP\AppData\Local\Programs\MiKTeX\miktex\bin\x6...

C:\OpenSSL\bin

Nouveau

Modifier

Parcourir...

Supprimer

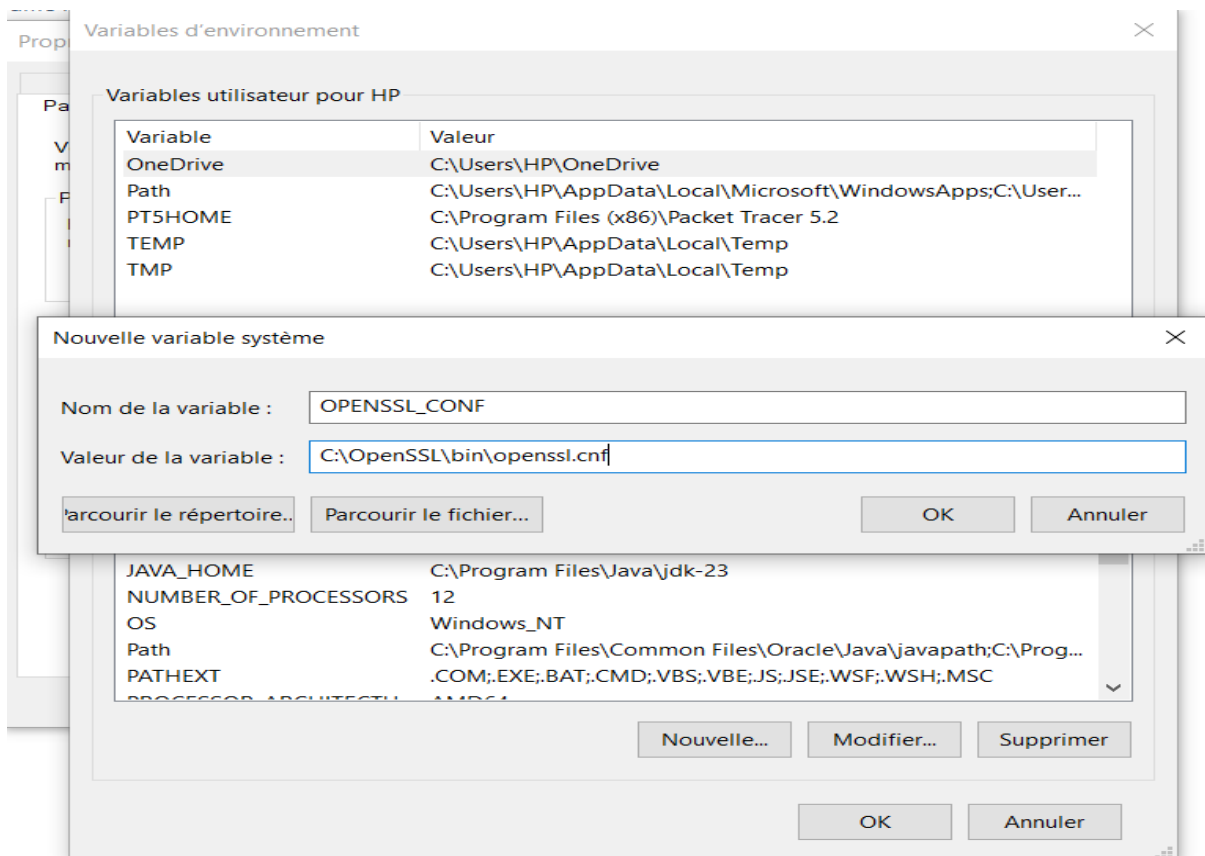
Déplacer vers le haut

Déplacer vers le bas

Modifier le texte...

OK

Annuler



Invite de commandes

```
Microsoft Windows [version 10.0.19045.5487]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\HP>openssl version
OpenSSL 1.0.2j-fips 26 Sep 2016

C:\Users\HP>
```

Fonctionnalités OpenSSL

La bibliothèque OpenSSL est une implémentation libre des protocoles SSL et TLS qui offre un ensemble d'outils en ligne de commande permettant, le chiffrement et le déchiffrement (RSA, DES, IDEA, RC2, RC4, Blowfish, etc.)...La syntaxe générale pour utiliser les fonctionnalités d'OpenSSL en mode shell est la suivante : **openssl <commande> <options>**

Chiffrement d'un fichier

➔ **Chiffrement avec AES-256-cpc :**

```
zxgr@zXgr05: ~/Desktop
zxgr@zXgr05:~/Desktop$ cat fichier.txt
SITCN
zxgr@zXgr05:~/Desktop$ openssl enc -aes-256-cbc -in fichier.txt -out fichier_chiffre_aes.enc -k aes256
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
zxgr@zXgr05:~/Desktop$ cat fichier_chiffre_aes.enc
Salted__L***N~.Wa1***Szxgr@zXgr05:~/Desktop$
```

➔ **Dechiffrement avec AES-256-CPC :**

```
zxgr@zXgr05:~/Desktop$ openssl enc -aes-256-cbc -d -in fichier_chiffre_aes.enc -out fichier_dechiffre_aes.enc -k aes256
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
zxgr@zXgr05:~/Desktop$ cat fichier_dechiffre_aes.enc
SITCN
zxgr@zXgr05:~/Desktop$
```

➔ **Chiffrement avec 3DES :**

```
zxgr@zXgr05: ~/Desktop
zxgr@zXgr05:~/Desktop$ openssl enc -des-ede3-cbc -in fichier.txt -out fichier_chiffre_3des.enc -k 3des
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
zxgr@zXgr05:~/Desktop$ cat fichier_chiffre_3des.enc
Salted__***1/SRy***Mzxgr@zXgr05:~/Desktop$
```

➔ **Dechiffrement avec 3DES :**

```
zxgr@zXgr05: ~/Desktop
zxgr@zXgr05:~/Desktop$ openssl enc -des-ede3-cbc -d -in fichier_chiffre_3des.enc
-out fichier_dechiffre_3des.txt -k 3des
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
zxgr@zXgr05:~/Desktop$ cat fichier_dechiffre_3des.txt
SITCN
zxgr@zXgr05:~/Desktop$
```