المدرسة الوطنية العليا للذكاء الاصطناعي وعلوم المعطيات - تارودانت
ÉCOLE NATIONALE SUPÉRIEURE DE L'INTELLIGENCE ARTIFICIELLE
ET SCIENCES DES DONNÉES - TAROUDANT

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

Filière : SITCN

Cryptographie appliquée

Thème :

TP N1 : OpenSSL

Réaliser par:

Zouhair GUERTAOUI

Encadré par:

Mr. Hasnae Al-amrani

Année Universitaire : 2024 / 2025

Objectif

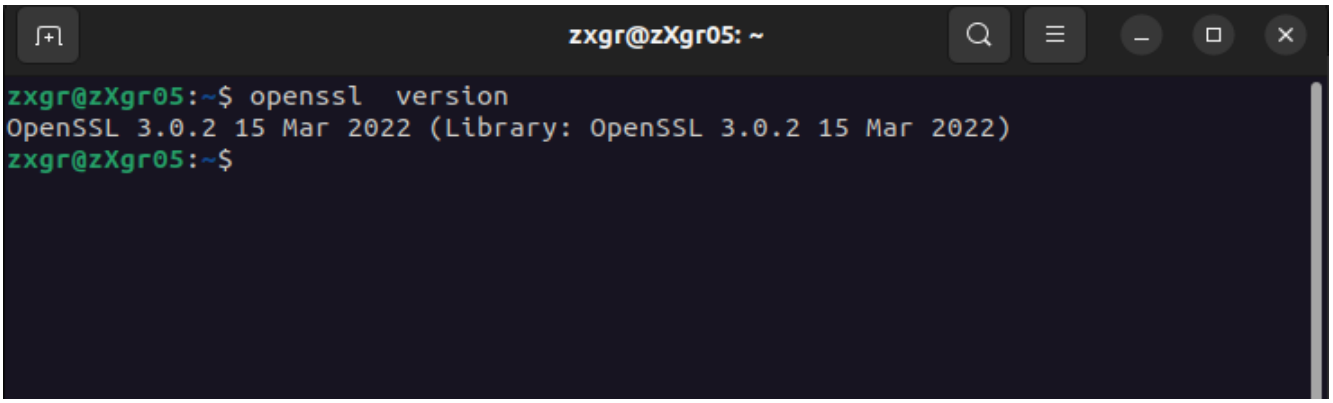
- Se familiariser avec les fonctionnalités et la bibliothèque openSSL
- Génération et utilisation des Clés secrètes
- Chiffrement de données via les commandes de la bibliothèque openSSL

Outils

- Système Windows ou Linux
- Bibliothèque openSSL

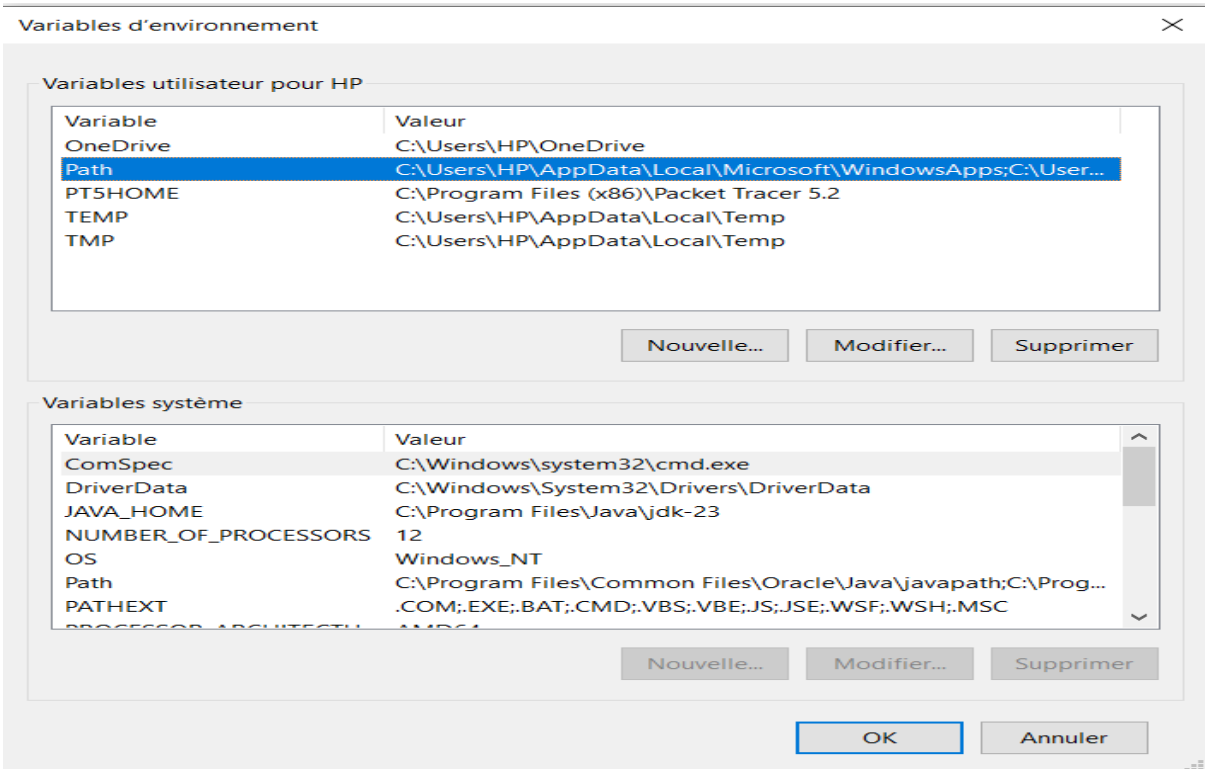
Préparation de l'environnement de travail

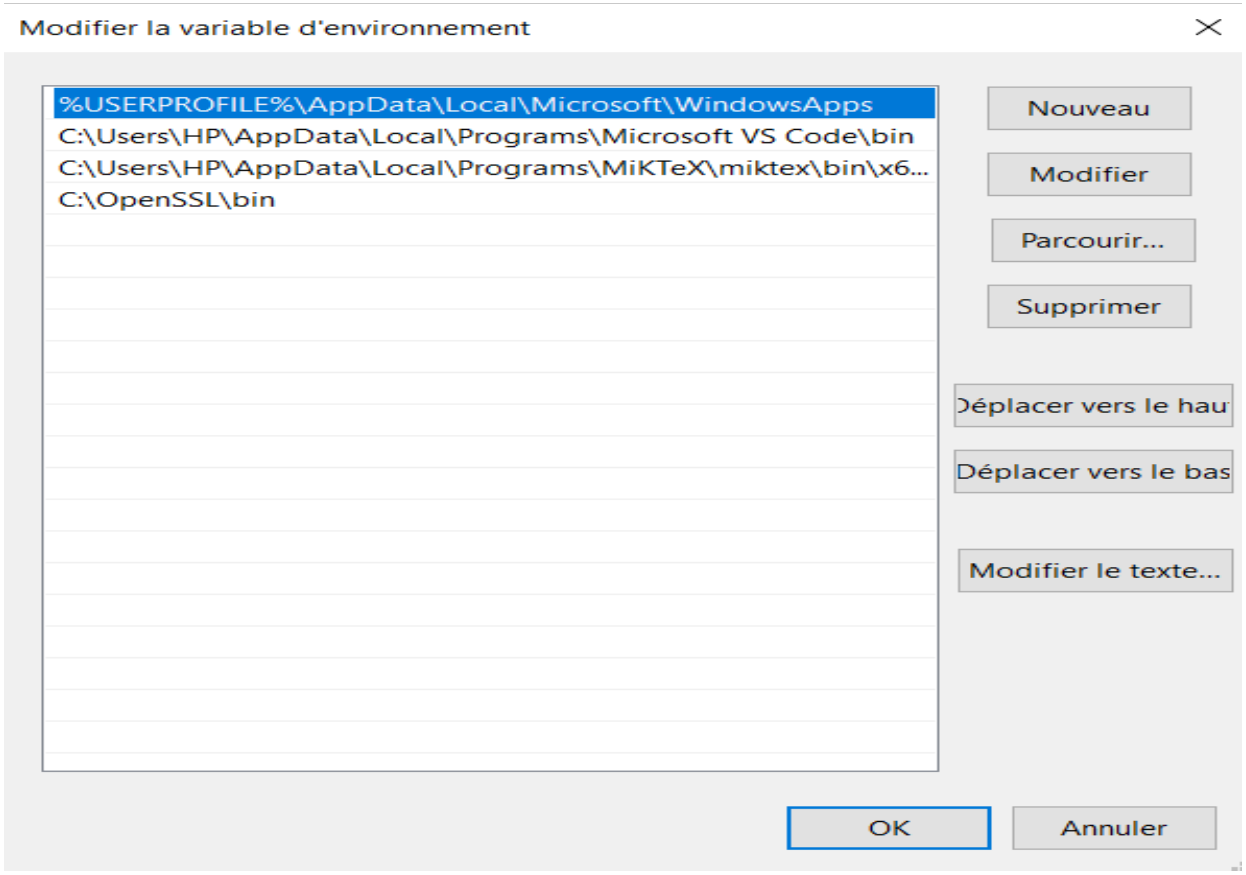
Verification de l'existence du bibliotheque openssl sur **Ubuntu** :

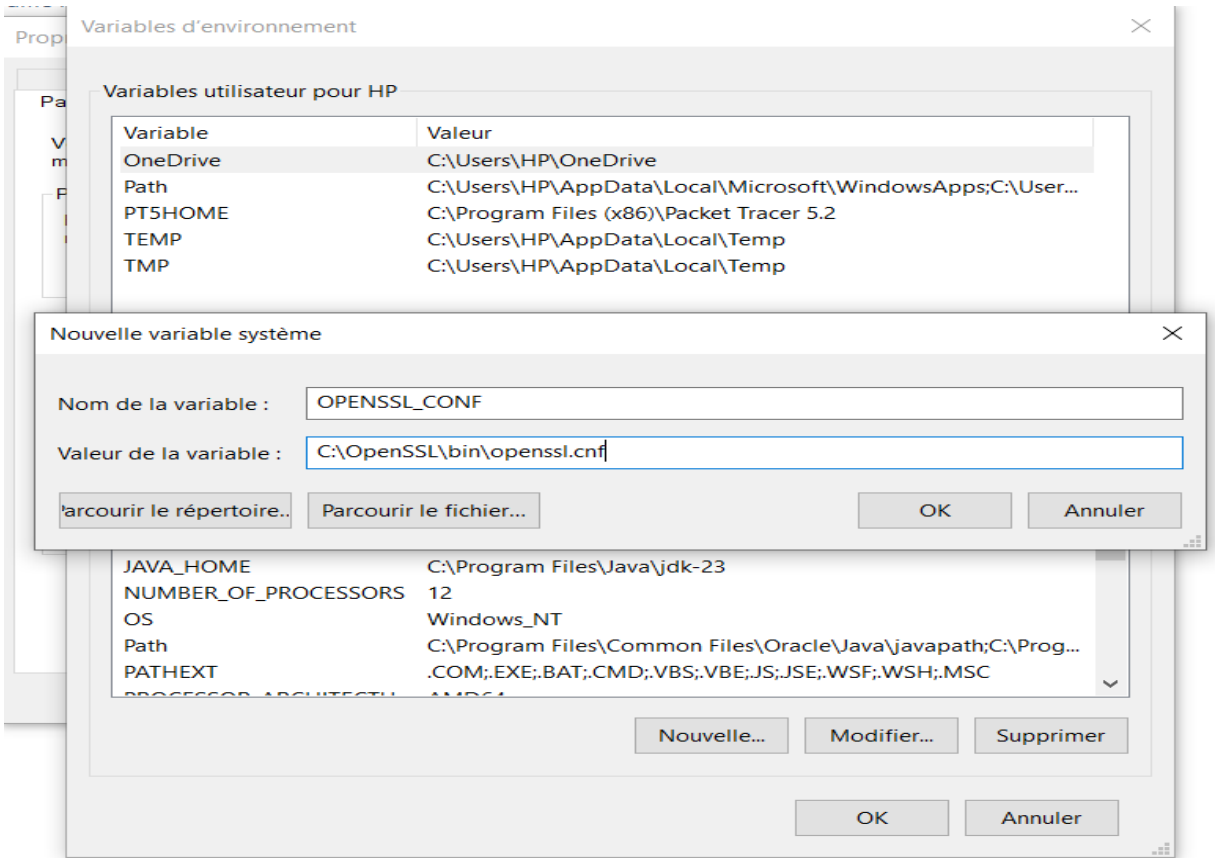


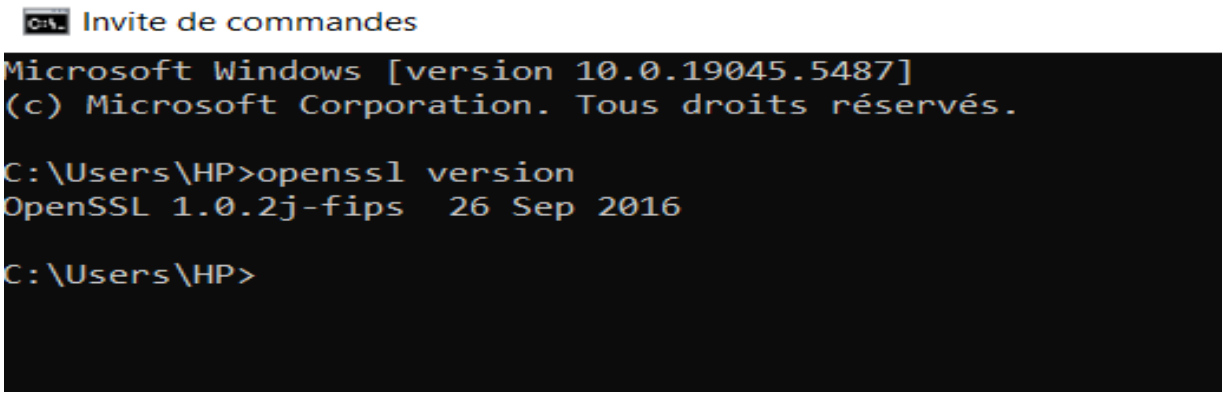
Sur Windows

- 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...
PT5HOME
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
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 hau
Déplacer vers le bas
Modifier le texte...
OK
Annuler



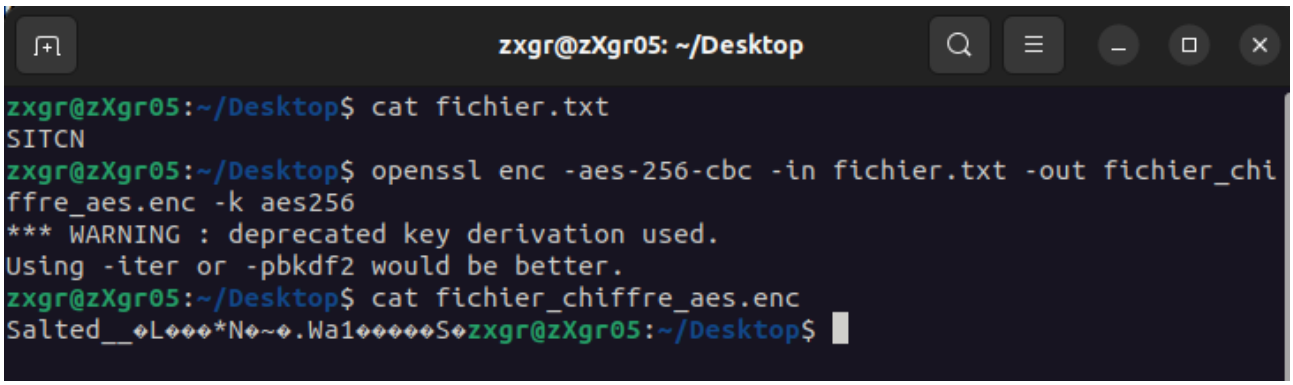


Fonctionnalités OpenSSL

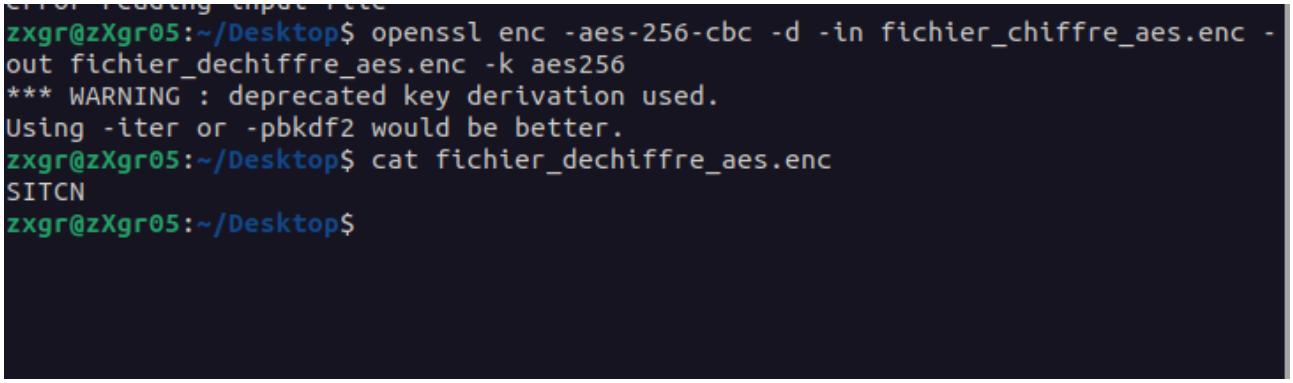
La bibliothèque OpenSSL est une implémentation libre des protocoles SSL et TLS qui offre un ensemble d'outils en ligne de commande permettant, le chiffrement et le déchiffrement (RSA, DES, IDEA, RC2, RC4, Blowfish, etc.)...La syntaxe générale pour utiliser les fonctionnalités d'OpenSSL en mode shell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

Chiffrement d'un fichier

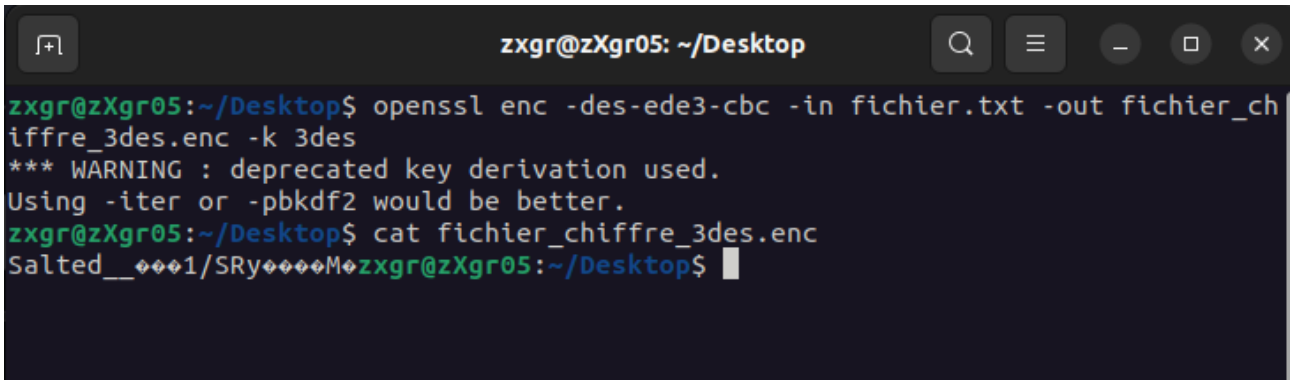
➔ **Chiffrement avec AES-256-cpc :**



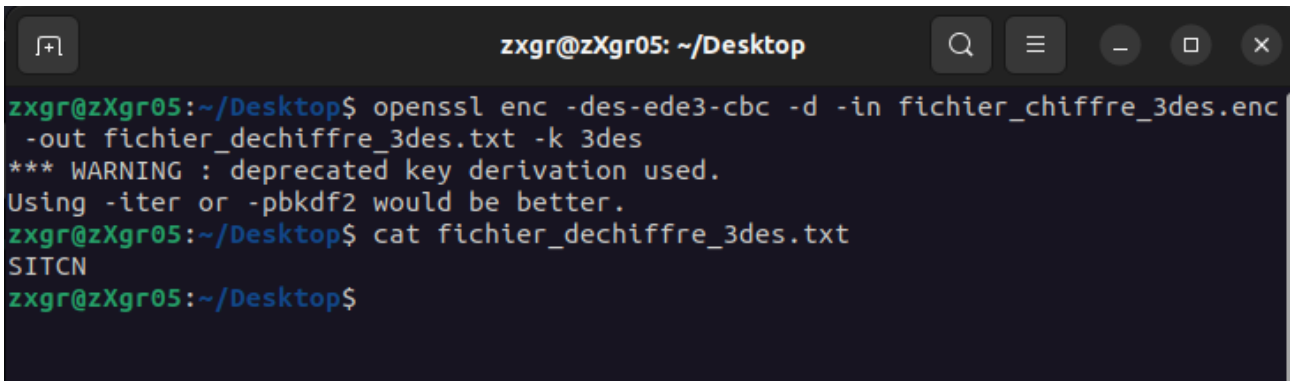
➔ **Dechiffrement avec AES-256-CPC :**



➔ **Chiffrement avec 3DES :**



➔ **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$