Travaux pratiques de Réseau

TP SMTP-TLS/SSL

indications de correction

Q2 .chiffrement clé secrète

chiffrer un fichier avec le mot de passe dans la ligne de commande (avec l'option -pass) :
openssl enc -des3 -salt -in fic1 -out fic1.des3 -pass pass:aaaa

déchiffrement (mot de passe avec l'option -pass) :
openssl enc -des3 -d -salt -in fic1.des3 -out file.txt -pass pass:aaaa

Q3. paramètre (salt) : citation de la doc openssl

Without the -salt option it is possible to perform efficient dictionary attacks on the password and to attack stream cipher encrypted data. The reason for this is that without the salt the same password always generates the same encryption key. When the salt is being used the first eight bytes of the encrypted data are reserved for the salt: it is generated at random when encrypting a file and read from the encrypted file when it is decrypted.

Q4 chiffrement Clé publique-clé privé

```
openssl genrsa -out test_priv.pem 1024
openssl rsa -in test_priv.pem -pubout -out test_pub.pem
openssl rsautl -encrypt -in test.txt -inkey test_pub.pem -pubin -out se-
cret.txt
openssl rsautl -decrypt -in secret.txt -inkey test_priv.pem -out decr.txt
```

Q5. Signature numerique

on commence par gerer les clés privées et publiques comme indiquées plus haut puis on met les différents fichiers dans chaque répertoire puis on applique les fonctions de creation et de génération.

creation : openssl dgst -binary -out **sig.sig** -sign **privatekey.pem clair.txt**
vérif :openssl dgst -signature **sig.sig** -verify **publickey.pem clair.txt**