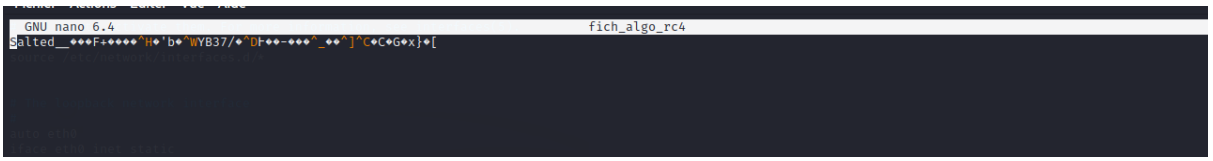
Bayrem HAMDI SAE8

L’algorithme RC4

1)



Vérifier alors que le message déchiffré est bien identique au fichier initial

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl enc -RC4 -d -in fich_algo_rc4  -out fich_dechiff_rc4
enter RC4 decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿Attaquant)-[~]
└─$ diff fich_algo_rc4 fich_dechiff_rc4
1c1
< Salted__◆◆◆F+◆◆◆◆'b◆YB37/◆├◆◆-◆◆◆◆◆◆C◆G◆x}◆[
\ Pas de fin de ligne à la fin du fichier
---
> hello this message is to test cypto

┌──(kali㉿Attaquant)-[~]
└─$ nano fich_dechiff_rc4

┌──(kali㉿Attaquant)-[~]
└─$ diff fich.txt  fich_dechiff_rc4

┌──(kali㉿Attaquant)-[~]
└─$
```

L’algorithme DES
Pour chiffrer le fichier fichier_nom_eleve avec l’algorithme DES avec clé explicite

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl enc -des -in fich.txt  -out fichier_chiff_des -k 0123456789ABCDEF
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```

```
┌──(kali㉿kali)-[~]
└─$ openssl des -rc4 -in clair.txt  -out resulta4 -k 0123456789ABCDEF
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~]
└─$ openssl enc -des -in clair.txt  -out resulta5 -k 0123456789ABCDEF
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~]
└─$ openssl enc -des -d -in resulta5 -out dechiffre5
enter DES-CBC decryption password:
bad password read

┌──(kali㉿kali)-[~]
└─$ openssl des -des -d -in resulta5 -out dechiffre5
enter DES-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~]
└─$ diff clair.txt dechiffre5
```

RSA

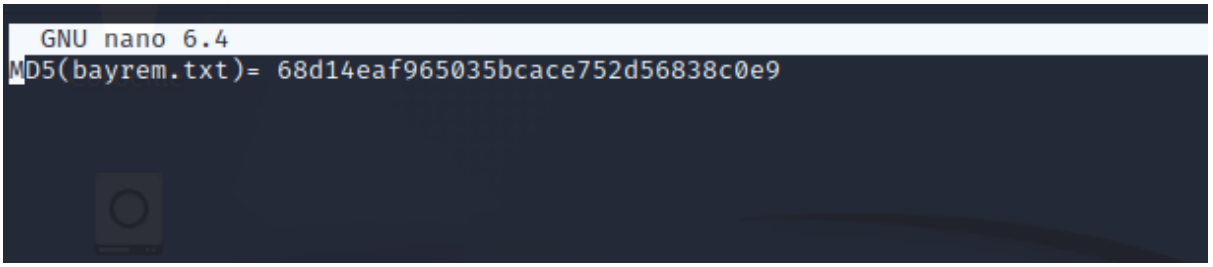
```
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -inkey rsakey.pem -in fichier-chiffr-Rsa -decrypt -out fi
chier-dechiffr-Rsa
```

```
└─$ diff  fichier-dechiffr-Rsa clair.txt
```

3 - **signature numerique**

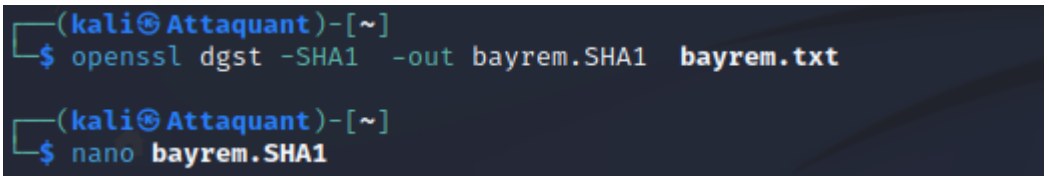
- Calculer la valeur de l'empreinte du fichier fichier_nom_eleve avec l'algorithme MD5 et la mettre dans un fichier fichier_nom_eleve.md5.

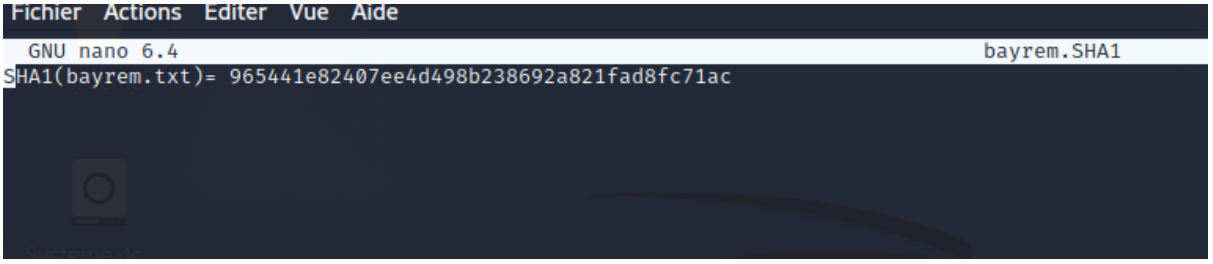
```
┌──(kali㉿Attaquant)-[~]
└─$ openssl dgst -md5  -out bayrem.md5  bayrem.txt

┌──(kali㉿Attaquant)-[~]
└─$ nano bayrem.md5
```



la taille de l'empreinte est 128 bits

Calculer la valeur de l'empreinte du même fichier avec l'algorithme SHA1 et la mettre dans un fichier fichier_nom_eleve.sha1.

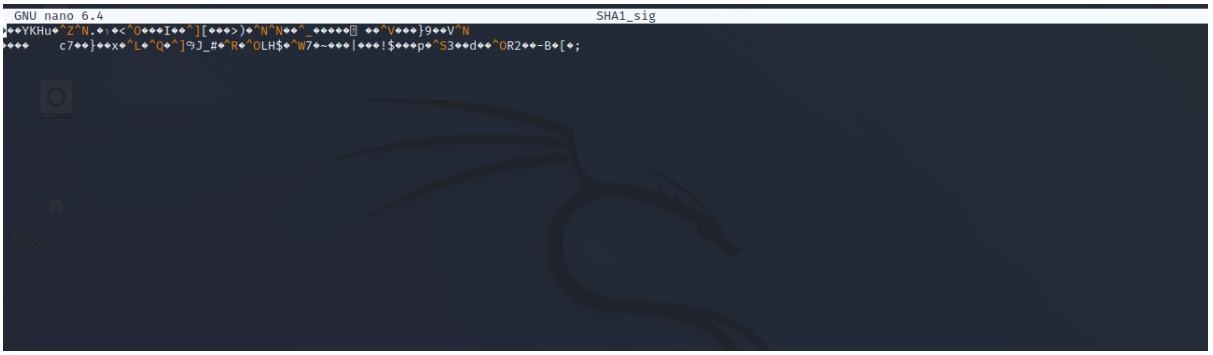




taille d'empreinte 160

l'algorithme md5 donne une empreinte de taille inferieure au algo sha1 donc on peut conclure que SHA1 est plus resistant au attaques de collision

signature d'un fichier
signature de SHA1



quel est la clé que vous devez utiliser pour signer ? cle privee

verif de signature

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl pkeyutl  -verify -in bayrem.SHA1   -pubin -inkey rsapubkey.pem -sigfile SHA1_sig
Signature Verified Successfully
```

Quel est la clé que vous devez utiliser pour vérifier la signature du fichier fichier_sig? le cle publique

4. CERTIFICAT NUMERIQUE

Créer un fichier de demande de signature de certificat (CSR Certificate Signing Request)

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl req -new -key serveur_cle.pem -out serveur_cert.pem
Could not open file or uri for loading private key from serveur_cle.pem
40070DE48E7F0000:error:16000069:STORE routines:ossl_store_get0_loader_int:unregistered scheme:../crypto/store/store_register.c:237:scheme=file
40070DE48E7F0000:error:80000002:system library:file_open:No such file or directory:../providers/implementations/storemgmt/file_store.c:267:calling stat(serveur_cle
.pem)

┌──(kali㉿Attaquant)-[~]
└─$ openssl req -new -key server_cle.pem -out server_cert.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:tunis
Locality Name (eg, city) []:tunis
Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:wassim
Email Address []:bayrem.hamdi@esprit.tn

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:bouselem
An optional company name []:.
```

Auto signature d'un certificat

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl req -new -x509 -days 365 -key server_cle.pem -out server_cert.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:tunis
Locality Name (eg, city) []:tunis
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ESPRIT
Organizational Unit Name (eg, section) []:ESPRIT
Common Name (e.g. server FQDN or YOUR name) []:bayrem
Email Address []:bayrem.hamdi@esprit.tn

┌──(kali㉿Attaquant)-[~]
└─$ openssl x509 -in server_cert.crt -text -noout
Certificate:
```

```
ertificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            45:b2:5d:34:10:d0:1a:f5:2b:5d:37:a8:65:81:5d:d3:05:55:03:63
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = TN, ST = tunis, L = tunis, O = ESPRIT, OU = ESPRIT, CN = bayrem, emailAddress = bayrem.hamdi@esprit.tn
        Validity
            Not Before: Feb 18 15:24:21 2023 GMT
            Not After : Feb 18 15:24:21 2024 GMT
        Subject: C = TN, ST = tunis, L = tunis, O = ESPRIT, OU = ESPRIT, CN = bayrem, emailAddress = bayrem.hamdi@esprit.tn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:cd:6f:e8:3a:25:8d:90:b1:59:66:6f:5d:8e:68:
                    fb:af:dc:3f:be:65:34:c0:db:a1:2e:98:a0:b6:82:
                    d0:e2:e5:2b:c8:68:67:6e:85:2d:dd:5f:fe:e1:95:
                    15:01:7c:4f:59:0b:7f:c5:74:8e:91:49:8e:78:d7:
                    b7:fa:5b:eb:f2:36:30:ac:81:70:8f:18:1c:c9:80:
                    36:11:64:20:2f:06:23:08:ac:f7:64:78:8c:a4:3c:
                    4f:76:e5:04:21:92:0d:89:29:7e:b9:26:a7:5d:18:
                    0d:a2:9c:45:c3:78:59:c7:20:0b:71:ec:d7:1c:3f:
                    a2:b6:d4:b2:86:fa:48:c7:2f
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                08:CD:E5:AC:69:77:EE:E4:AB:36:4D:A3:A8:2F:2A:9E:94:52:F9:2E
            X509v3 Authority Key Identifier:
                08:CD:E5:AC:69:77:EE:E4:AB:36:4D:A3:A8:2F:2A:9E:94:52:F9:2E
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        70:b3:ba:6e:a6:16:6c:9d:27:79:42:94:ba:69:bf:35:e8:20:
```

Signature par une autorité de certification (AC)

clé privée RSA pour l'AC de taille 2048
Générer un certificat pour l'AC ayant une période de validité 730 jours

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl genrsa -out cakey.pem 2048

┌──(kali㉿Attaquant)-[~]
└─$ openssl req -new -x509 -days 730 -key cakey.pem -out ca_crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:tunis
Locality Name (eg, city) []:tunis
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ESPRIT
Organizational Unit Name (eg, section) []:ESPRIT
Common Name (e.g. server FQDN or YOUR name) []:BAYREM
Email Address []:bayrem.hamdi@esprit.tn
```

Signer la demande du certificat du serveur

```
┌──(kali㉿Attaquant)-[~]
└─$ openssl x509 -req -in server_cert.pem  -out server.crt -CA ca_crt -CAkey cakey.pem -CAcreateserial -CAserial ca.srl
Certificate request self-signature ok
subject=C = TN, ST = tunis, L = tunis, CN = wassim, emailAddress = bayrem.hamdi@esprit.tn

┌──(kali㉿Attaquant)-[~]
└─$
```