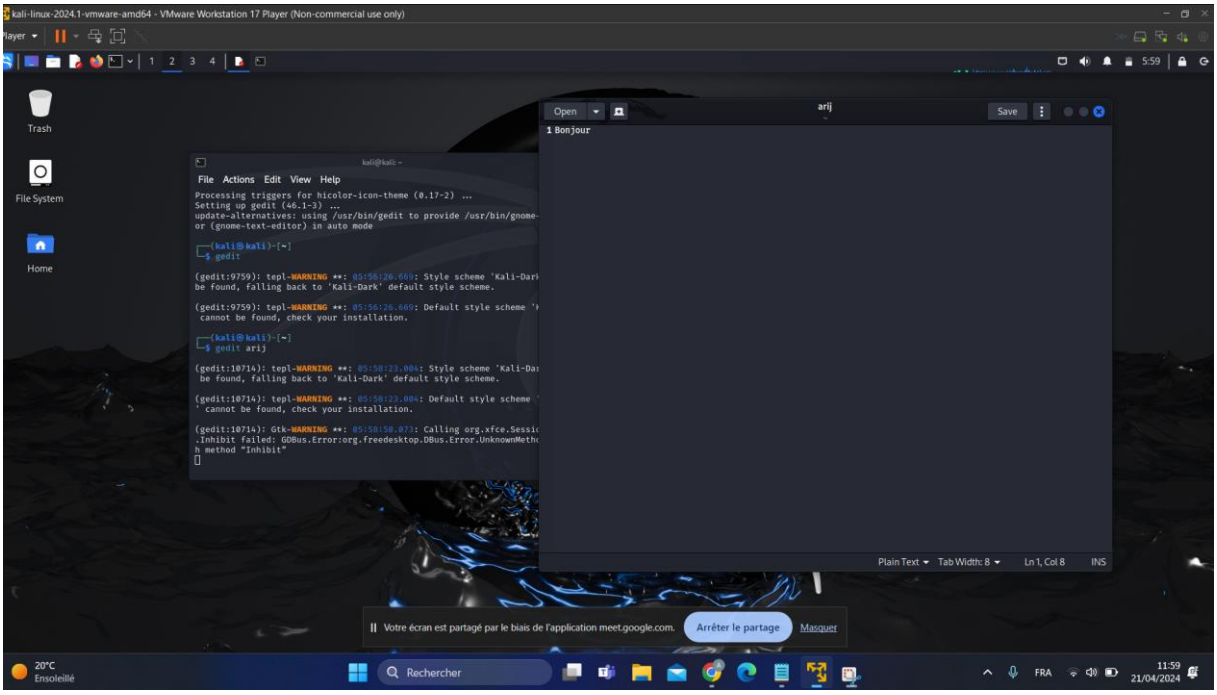
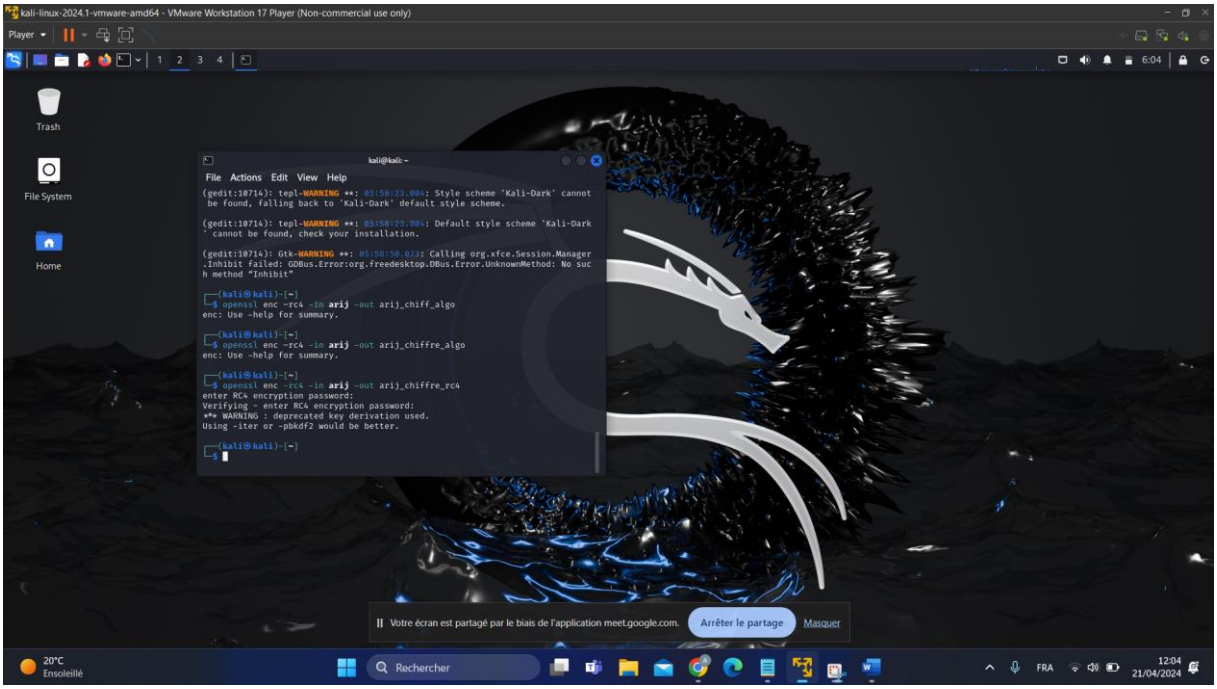
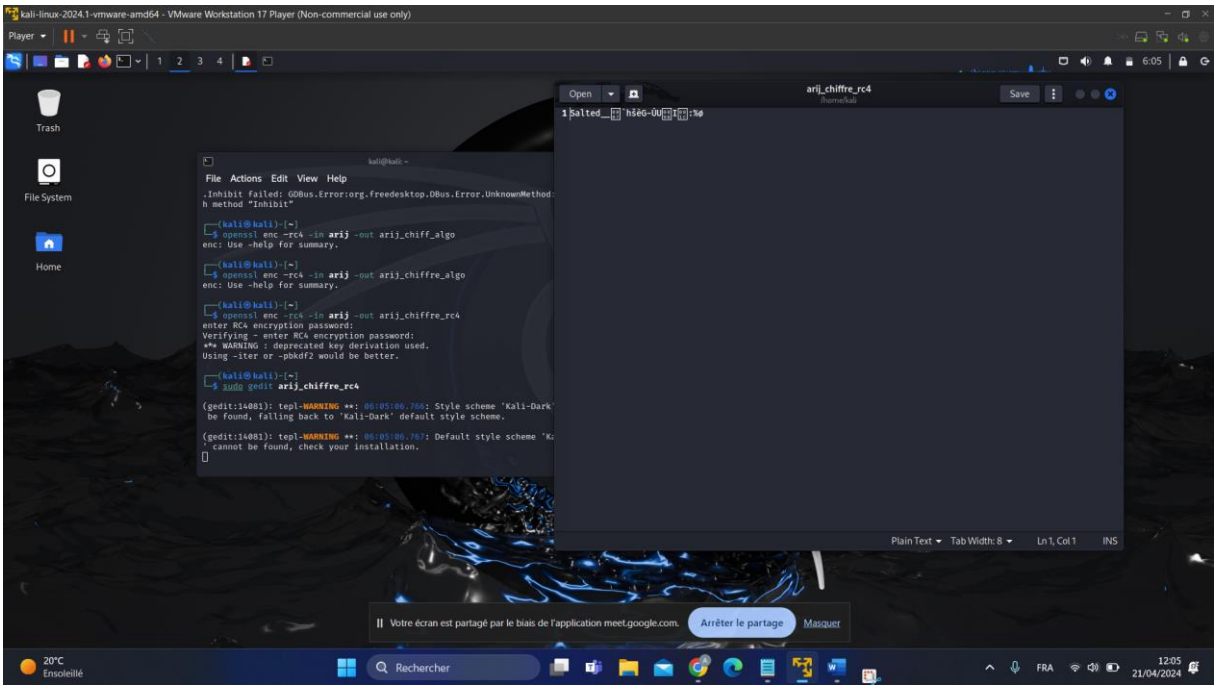
LAB 3 : La Cryptographie avec OpenSSL

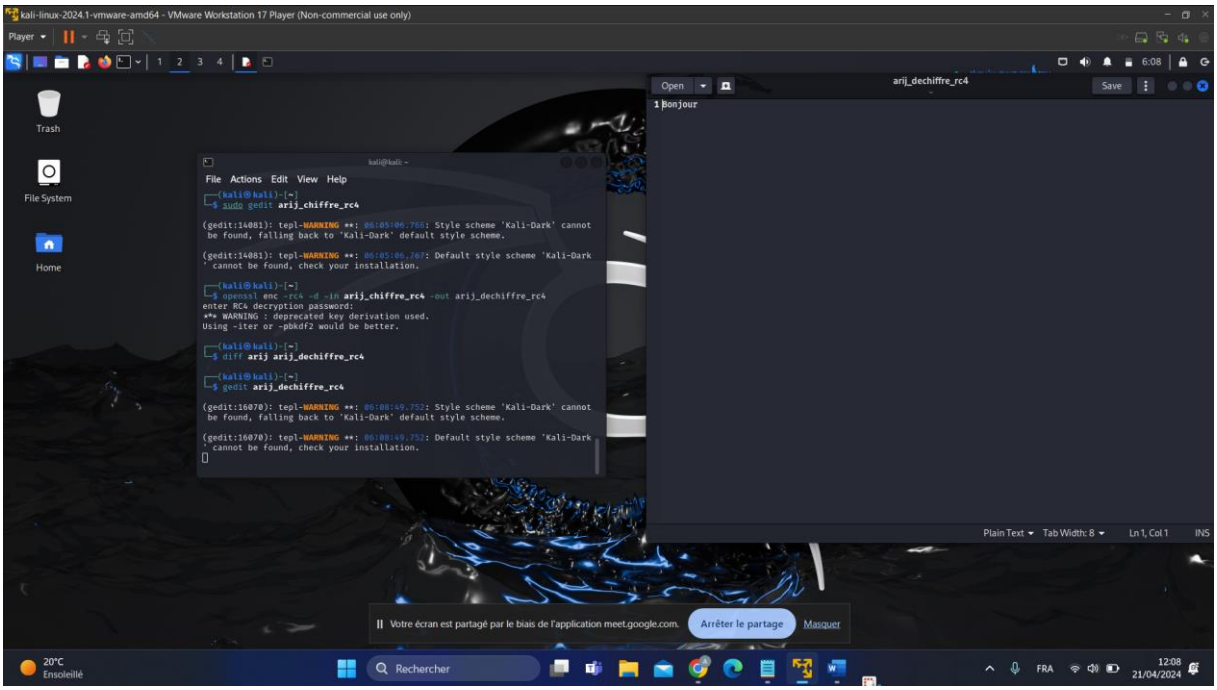
1. CHIFFREMENT SYMETRIQUE

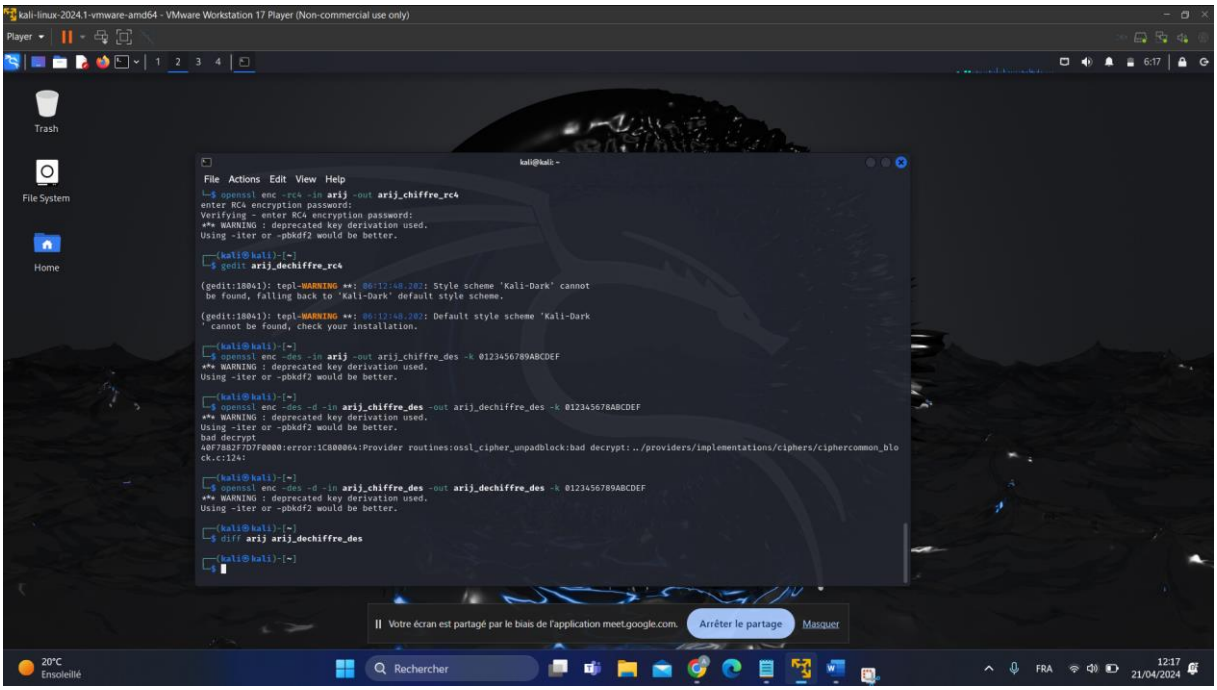




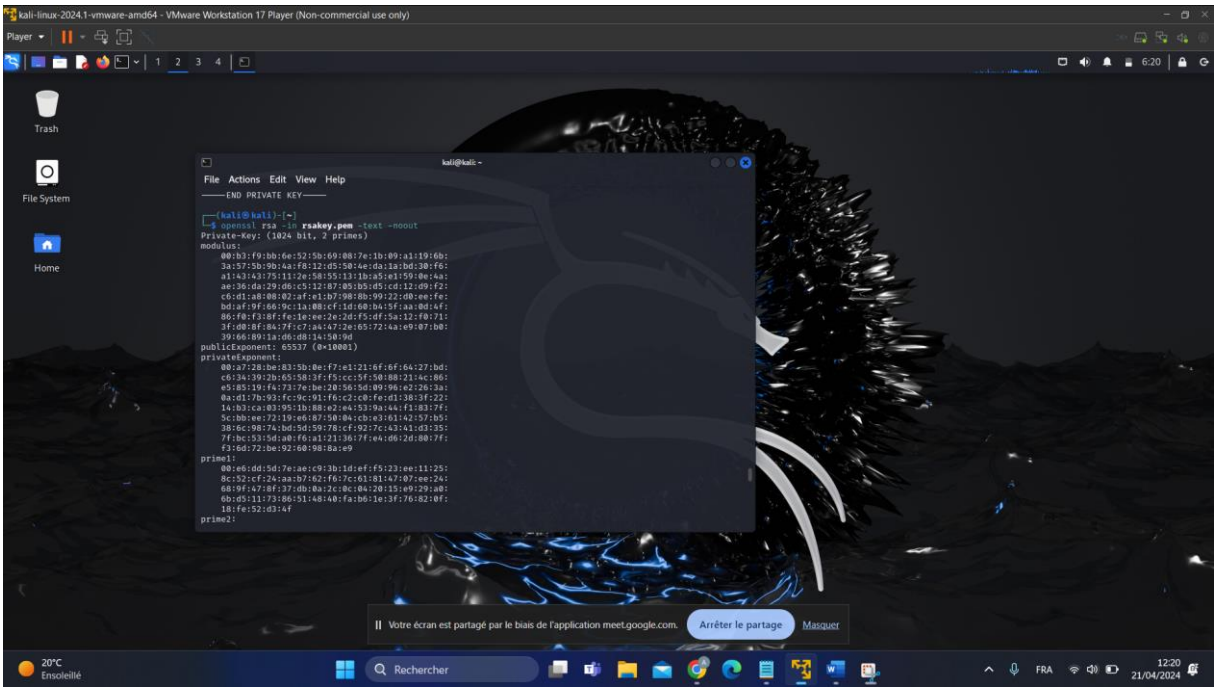


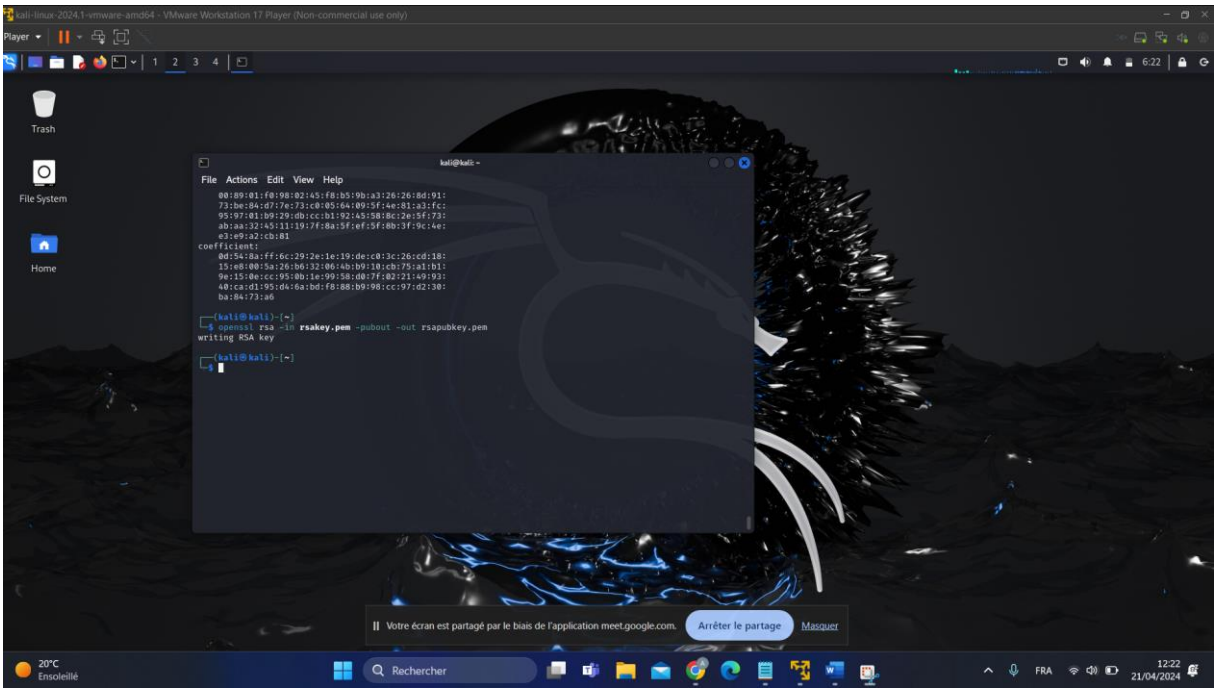
L’algorithme DES



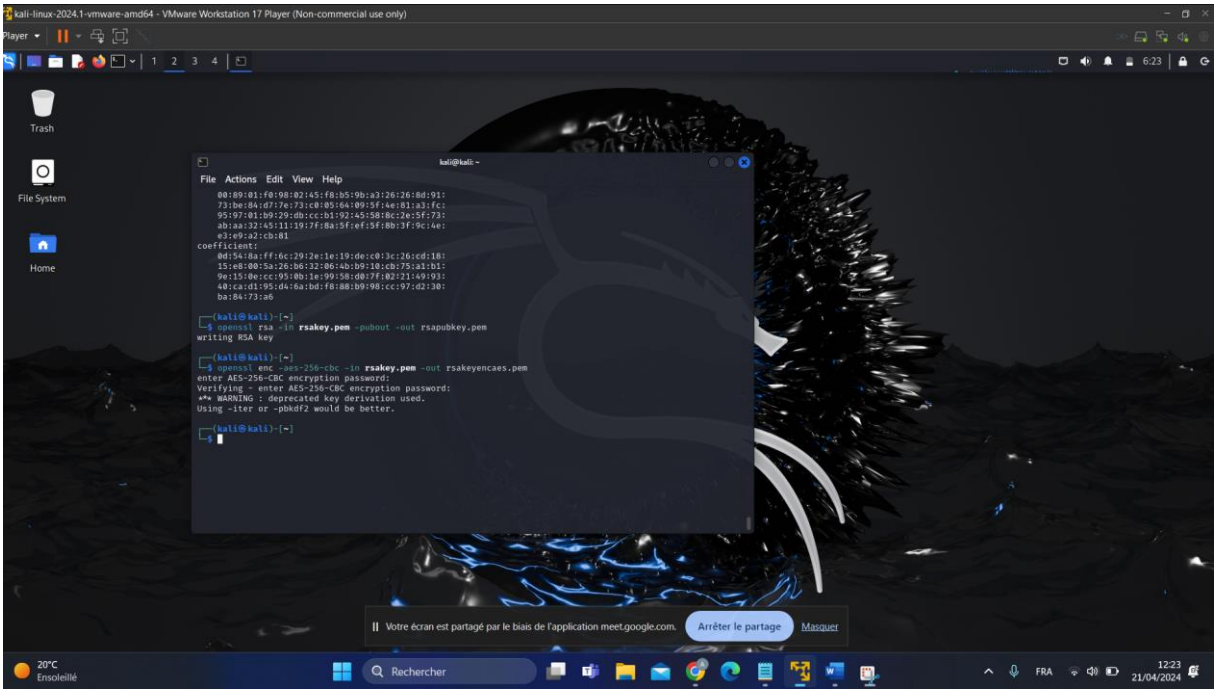


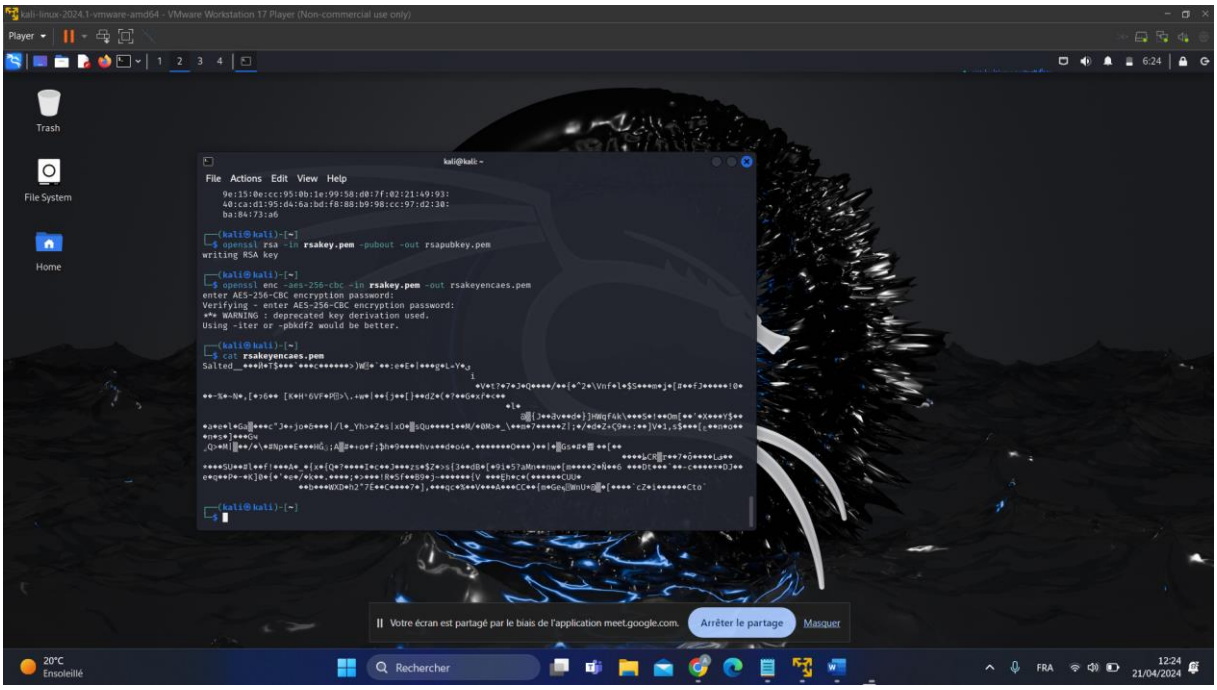
2. CHIFFREMENT ASYMETRIQUE

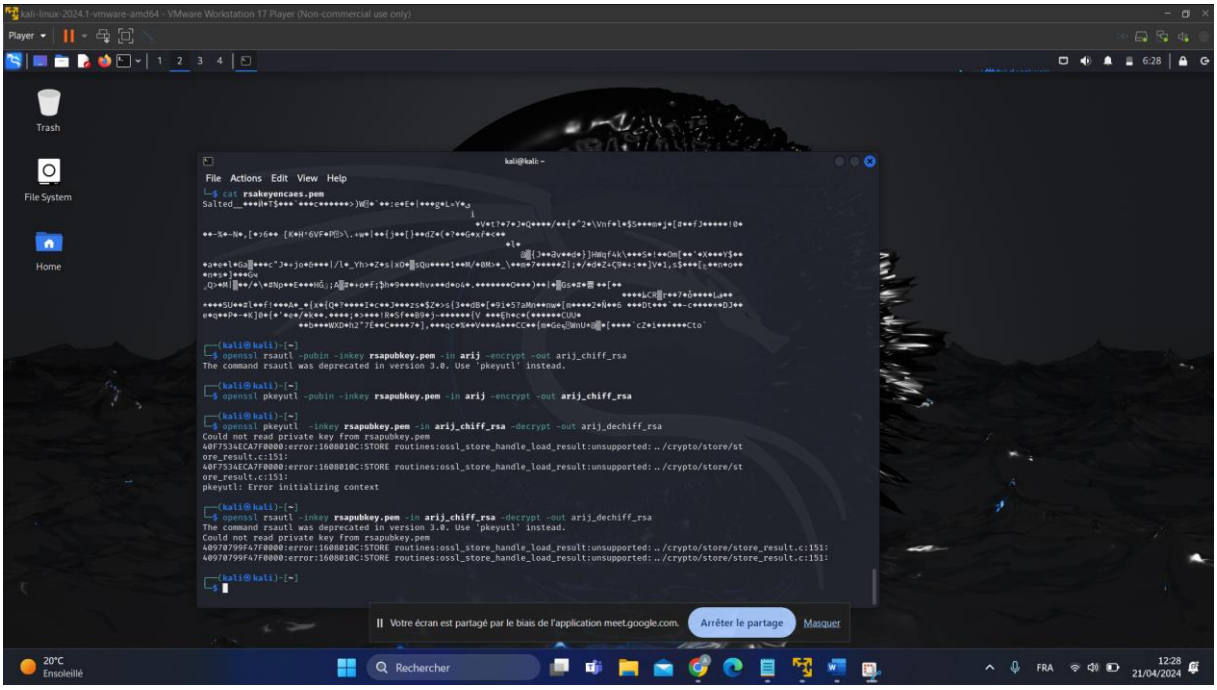



kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
00:89:01:f0:98:02:45:f8:b5:9b:a3:26:26:8d:91:
73:be:84:d7:7e:73:c0:05:64:09:5f:4e:81:a3:fc:
95:97:01:b9:29:db:cc:b1:92:45:58:8c:2e:5f:73:
ab:aa:32:45:11:19:7f:8a:5f:ef:5f:8b:3f:9c:4e:
e3:e9:a2:cb:81
coefficient:
0d:54:8a:ff:6c:29:2e:1e:19:de:c0:3c:26:cd:18:
15:e8:00:5a:26:b6:32:06:4b:b9:10:cb:75:a1:b1:
9e:15:0e:cc:95:0b:1e:99:58:d0:7f:02:21:49:93:
40:ca:d1:95:d4:6a:bd:f8:88:b9:98:cc:97:d2:30:
ba:84:73:a6
(kali@kali)-[~]
$ openssl rsa -in rsakey.pem -pubout -out rsapubkey.pem
writing RSA key
(kali@kali)-[~]
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
12:22
21/04/2024

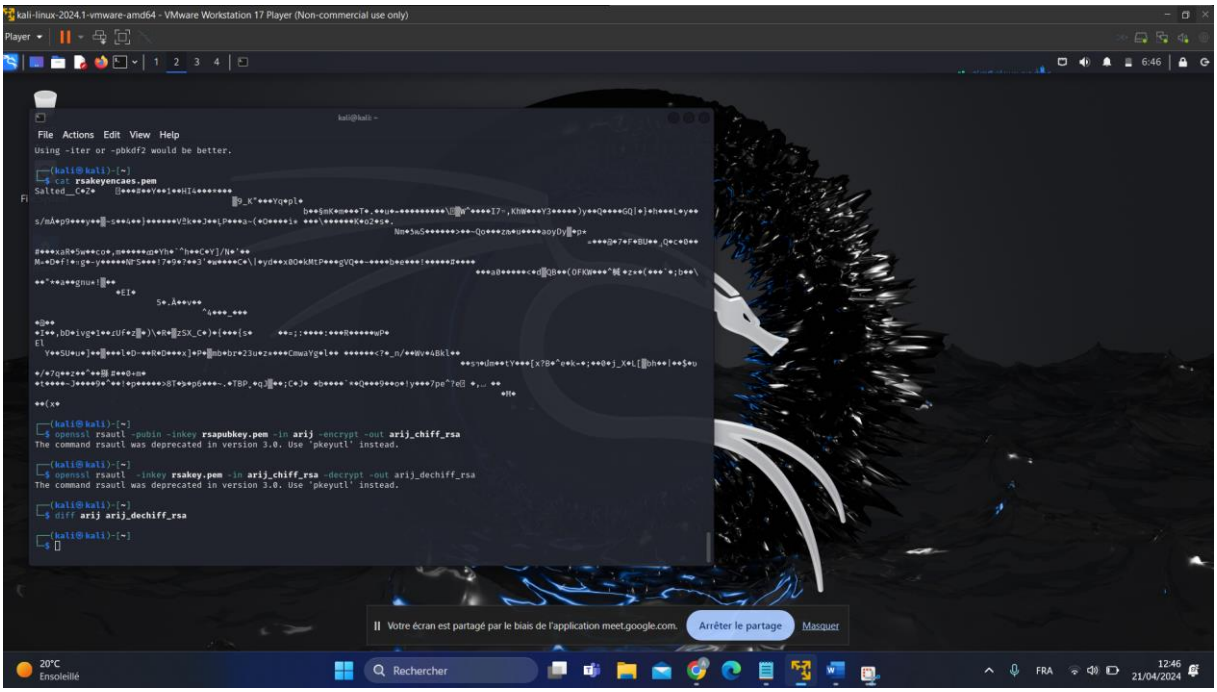
8_____


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
00:89:01:f0:98:02:45:f8:b5:9b:a3:26:26:8d:91:
73:be:84:d7:7e:73:c0:05:64:09:5f:4e:81:a3:fc:
95:97:01:b9:29:db:cc:b1:92:45:58:8c:2e:5f:73:
ab:aa:32:45:11:19:7f:8a:5f:ef:5f:8b:3f:9c:4e:
e3:e9:a2:cb:81
coefficient:
0d:54:8a:ff:6c:29:2e:1e:19:de:c0:3c:26:cd:18:
15:e8:00:5a:26:b6:32:06:4b:b9:10:cb:75:a1:b1:
9e:15:0e:cc:95:0b:1e:99:58:d0:7f:02:21:49:93:
40:ca:d1:95:d4:6a:bd:f8:88:b9:98:cc:97:d2:30:
ba:84:73:a6
(kali@kali)-[~]
$ openssl rsa -in rsakey.pem -pubout -out rsapubkey.pem
writing RSA key
(kali@kali)-[~]
$ openssl enc -aes-256-cbc -in rsakey.pem -out rsakeyencaes.pem
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(kali@kali)-[~]
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
12:23
21/04/2024

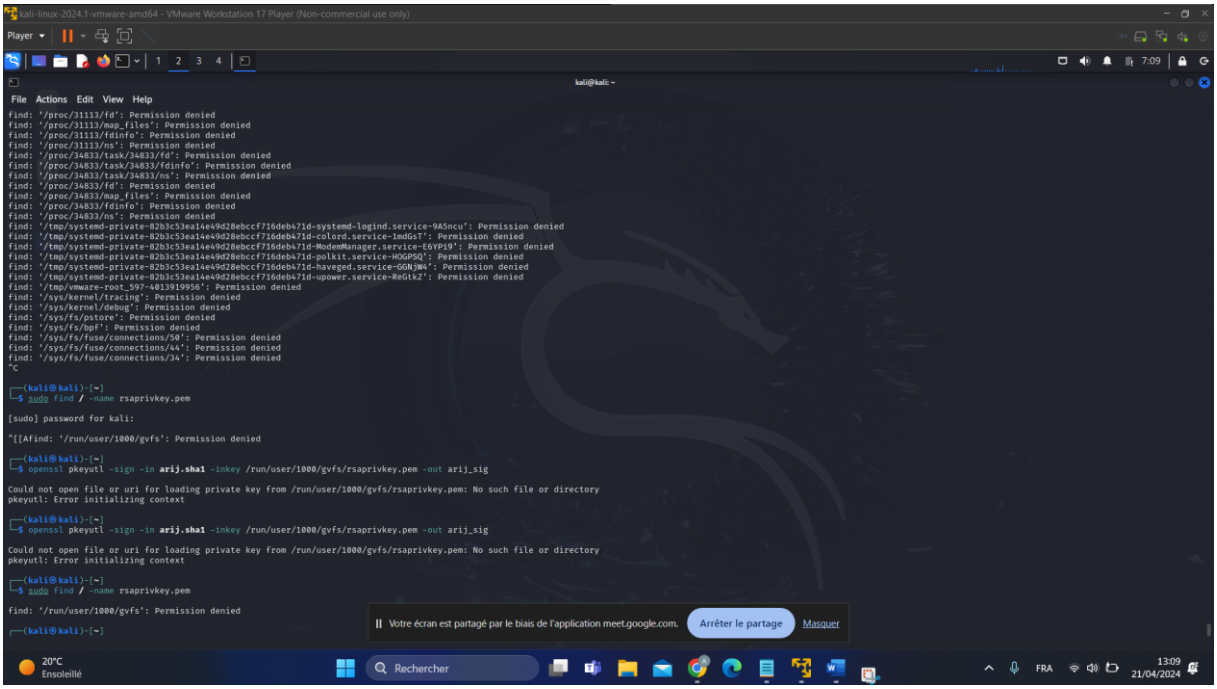

kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
12:24
21/04/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
12:28
21/04/2024

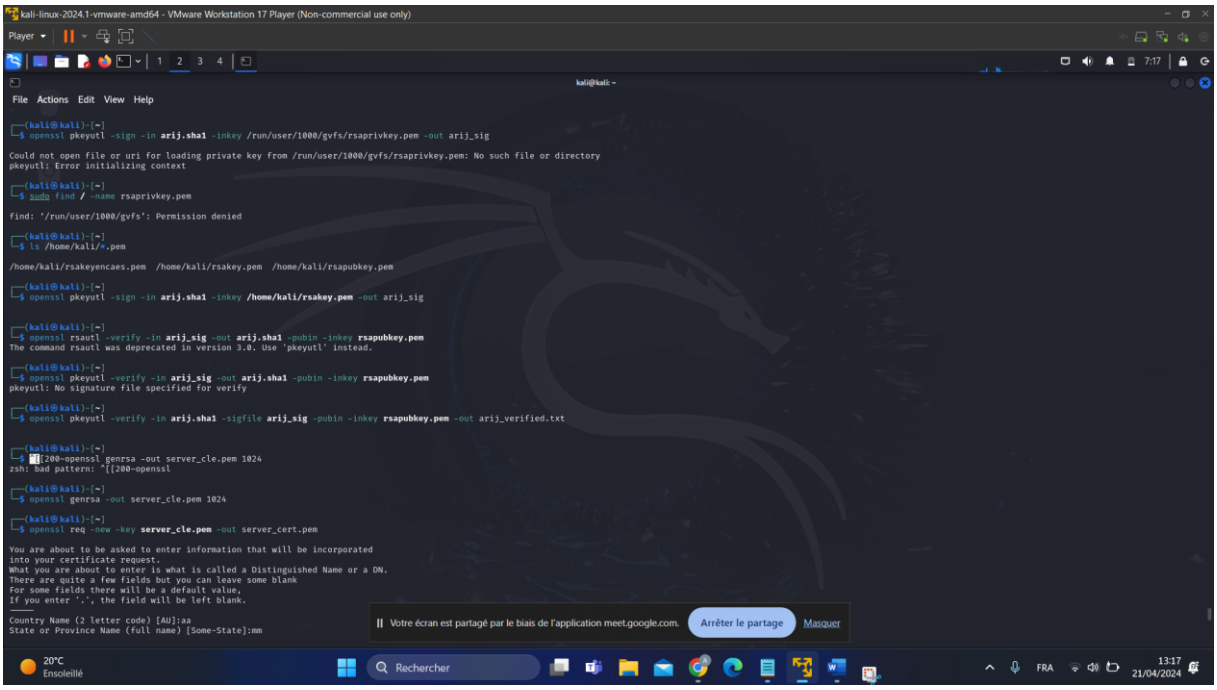
8_____

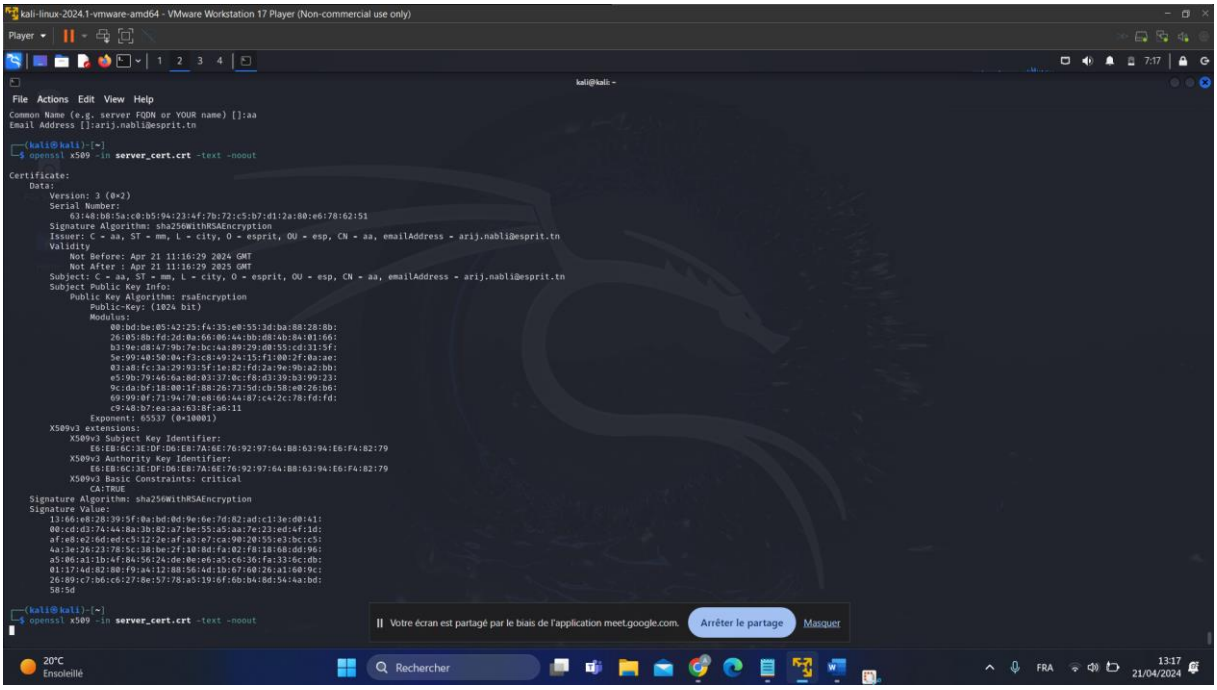


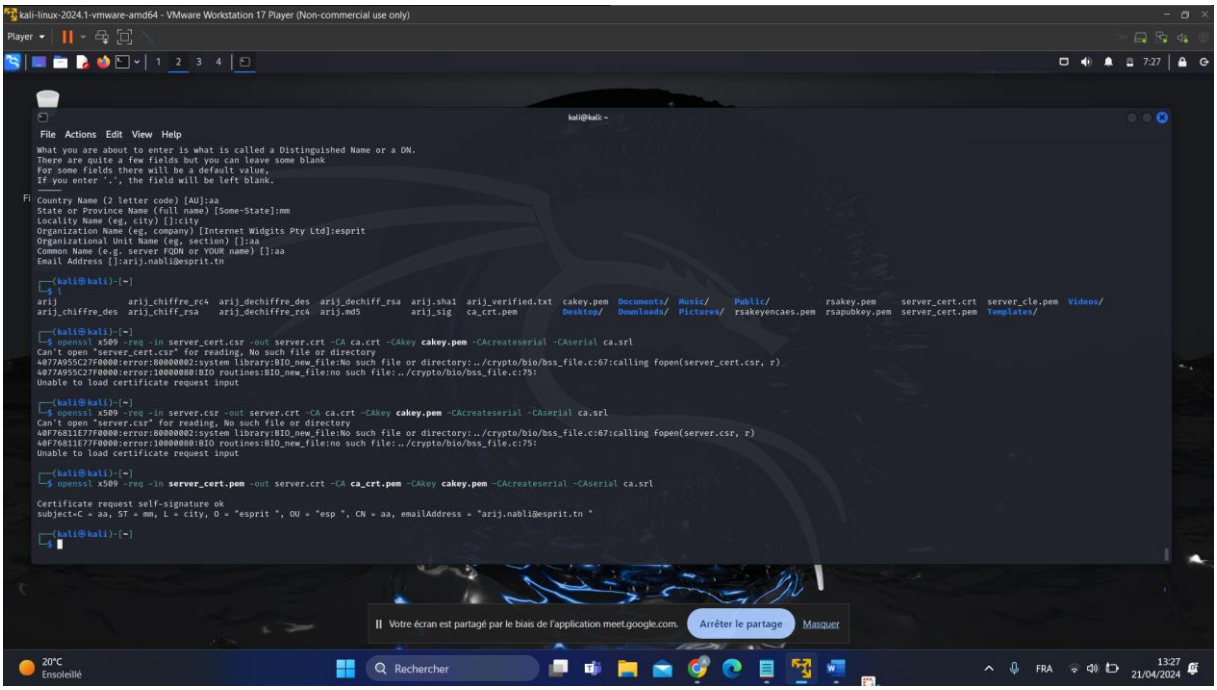
3. SIGNATURE NUMERIQUE



4-CERTIFICAT NUMERIQUE


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -sign -in arij.sha1 -inkey /run/user/1000/gvfs/rsaprivkey.pem -out arij_sig
Could not open file or uri for loading private key from /run/user/1000/gvfs/rsaprivkey.pem: No such file or directory
pkeyutl: Error initializing context
┌──(kali㉿kali)-[~]
└─$ sudo find / -name rsaprivkey.pem
find: '/run/user/1000/gvfs': Permission denied
┌──(kali㉿kali)-[~]
└─$ ls /home/kali/*.pem
/home/kali/rsakeyencaes.pem /home/kali/rsakey.pem /home/kali/rsapubkey.pem
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -sign -in arij.sha1 -inkey /home/kali/rsakey.pem -out arij_sig
┌──(kali㉿kali)-[~]
└─$ openssl rsautl -verify -in arij_sig -out arij.sha1 -pubin -inkey rsapubkey.pem
The command rsautl was deprecated in version 3.0. Use 'pkeyutl' instead.
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -verify -in arij_sig -out arij.sha1 -pubin -inkey rsapubkey.pem
pkeyutl: No signature file specified for verify
┌──(kali㉿kali)-[~]
└─$ openssl pkeyutl -verify -in arij.sha1 -sigfile arij_sig -pubin -inkey rsapubkey.pem -out arij_verified.txt
┌──(kali㉿kali)-[~]
└─$ [illegible]200~openssl genrsa -out server_cle.pem 1024
zsh: bad pattern: ^[[200~openssl
┌──(kali㉿kali)-[~]
└─$ openssl genrsa -out server_cle.pem 1024
┌──(kali㉿kali)-[~]
└─$ 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]:aa
State or Province Name (full name) [Some-State]:mm
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
13:17
21/04/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~
Common Name (e.g. server FQDN or YOUR name) []:aa
Email Address []:arij.nabli@esprit.tn
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in server_cert.crt -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
63:48:b8:5a:c0:b5:94:23:4f:7b:72:c5:b7:d1:2a:80:e6:78:62:51
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = aa, ST = mm, L = city, O = esprit, OU = esp, CN = aa, emailAddress = arij.nabli@esprit.tn
Validity
Not Before: Apr 21 11:16:29 2024 GMT
Not After : Apr 21 11:16:29 2025 GMT
Subject: C = aa, ST = mm, L = city, O = esprit, OU = esp, CN = aa, emailAddress = arij.nabli@esprit.tn
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
Modulus:
00:bd:be:05:42:25:f4:35:e0:55:3d:ba:88:28:8b:
26:05:8b:fd:2d:8a:66:06:44:bb:d8:4b:84:01:66:
b3:9e:d8:47:9b:7e:bc:4a:89:29:d8:55:cd:31:5f:
5e:99:40:50:04:f3:c8:49:24:15:f1:00:2f:0a:ae:
83:a8:fc:3a:29:93:5f:1e:82:fd:2a:9e:9b:a2:bb:
e5:9b:79:46:6a:8d:03:37:0c:f8:d3:39:b3:99:23:
9c:da:bf:18:00:1f:88:26:73:5d:cb:58:e0:26:b6:
69:99:0f:71:94:70:e8:66:44:87:c4:2c:78:fd:fd:
c9:48:b7:ea:aa:63:8f:a6:11
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
E6:EB:6C:3E:DF:D6:EB:7A:6E:76:92:97:64:B8:63:94:E6:F4:82:79
X509v3 Authority Key Identifier:
E6:EB:6C:3E:DF:D6:EB:7A:6E:76:92:97:64:B8:63:94:E6:F4:82:79
X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
13:66:e8:28:39:5f:0a:bd:0d:9e:6e:7d:82:ad:c1:3e:d0:41:
00:cd:d3:74:44:8a:3b:82:a7:be:55:a5:aa:7e:23:ed:4f:1d:
af:e8:e2:6d:ed:c5:12:2e:af:a3:e7:ca:90:20:55:e3:bc:c5:
4a:3e:26:23:78:5c:38:be:2f:10:8d:fa:02:f8:18:68:dd:96:
a5:06:a1:1b:4f:84:56:24:de:0e:e6:a5:c6:36:fa:33:6c:db:
01:17:4d:82:80:f9:a4:12:88:56:4d:1b:67:60:26:a1:60:9c:
26:89:c7:b6:c6:27:8e:57:78:a5:19:6f:6b:b4:8d:54:4a:bd:
58:5d
┌──(kali㉿kali)-[~]
└─$ openssl x509 -in server_cert.crt -text -noout
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
13:17
21/04/2024


kali-linux-2024.1-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
kali@kali: ~
File Actions Edit View Help
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]:aa
State or Province Name (full name) [Some-State]:mm
Locality Name (eg, city) []:city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:esprit
Organizational Unit Name (eg, section) []:aa
Common Name (e.g. server FQDN or YOUR name) []:aa
Email Address []:arij.nabli@esprit.tn
arij arij_chiffre_rc4 arij_dechiffre_des arij_dechiff_rsa arij.sha1 arij_verified.txt cakey.pem Documents/ Music/ Public/ rsakey.pem server_cert.crt server_cle.pem Videos/
arij_chiffre_des arij_chiff_rsa arij_dechiffre_rc4 arij.md5 arij_sig ca_crt.pem Desktop/ Downloads/ Pictures/ rsakeyencaes.pem rsapubkey.pem server_cert.pem Templates/
$ openssl x509 -req -in server_cert.csr -out server.crt -CA ca.crt -CAkey cakey.pem -CAcreateserial -CAserial ca.srl
Can't open "server_cert.csr" for reading, No such file or directory
4077A955C27F0000:error:80000002:system library:BIO_new_file:No such file or directory:../crypto/bio/bss_file.c:67:calling fopen(server_cert.csr, r)
4077A955C27F0000:error:10000080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:75:
Unable to load certificate request input
$ openssl x509 -req -in server.csr -out server.crt -CA ca.crt -CAkey cakey.pem -CAcreateserial -CAserial ca.srl
Can't open "server.csr" for reading, No such file or directory
40F76811E77F0000:error:80000002:system library:BIO_new_file:No such file or directory:../crypto/bio/bss_file.c:67:calling fopen(server.csr, r)
40F76811E77F0000:error:10000080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:75:
Unable to load certificate request input
$ openssl x509 -req -in server_cert.pem -out server.crt -CA ca_crt.pem -CAkey cakey.pem -CAcreateserial -CAserial ca.srl
Certificate request self-signature ok
subject=C = aa, ST = mm, L = city, O = "esprit ", OU = "esp ", CN = aa, emailAddress = "arij.nabli@esprit.tn "
Votre écran est partagé par le biais de l'application meet.google.com.
Arrêter le partage
Masquer
20°C
Ensoleillé
Rechercher
FRA
13:27
21/04/2024