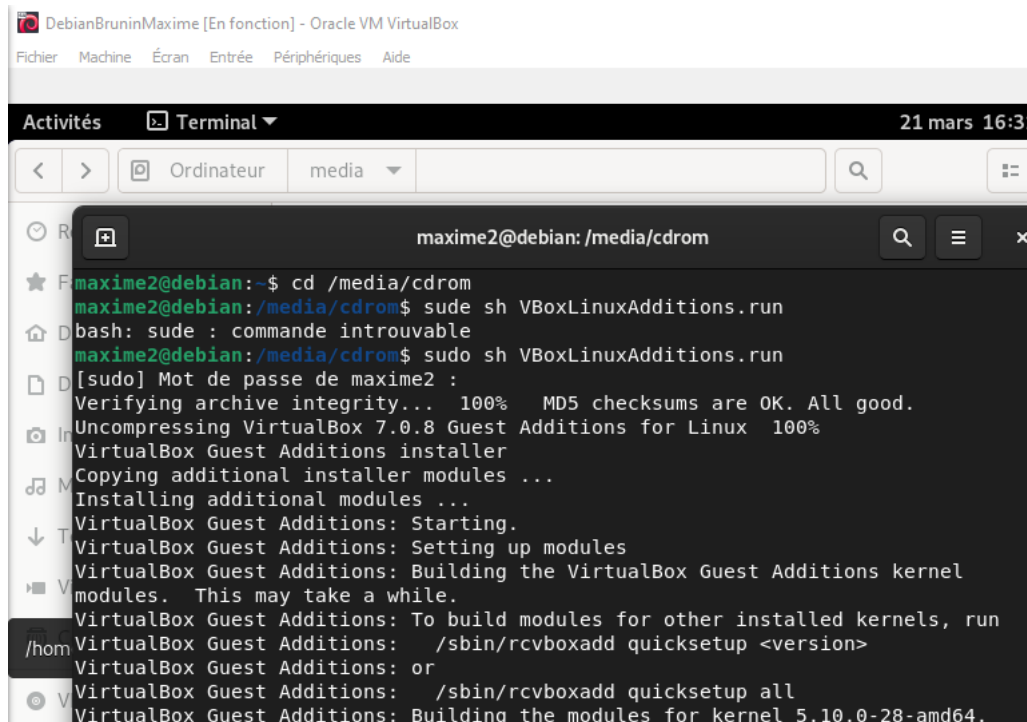
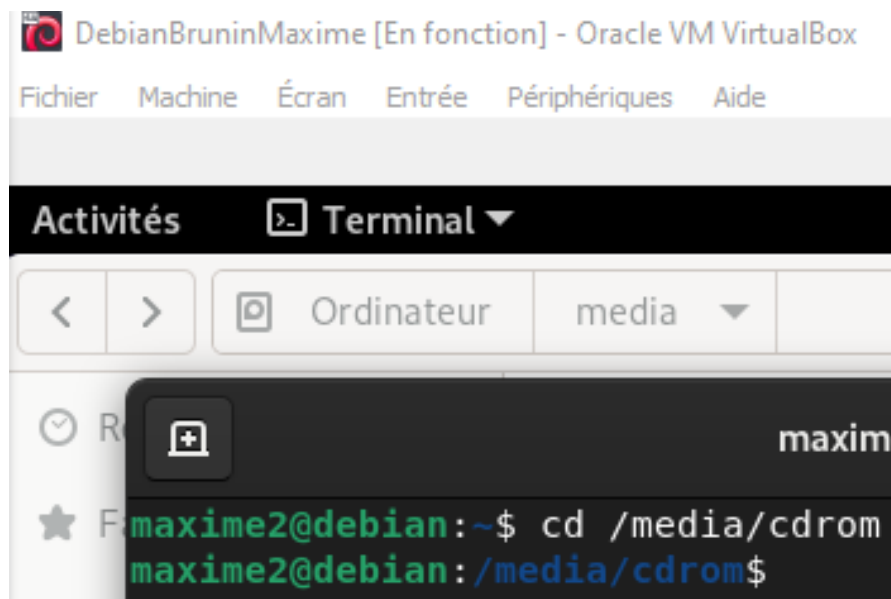
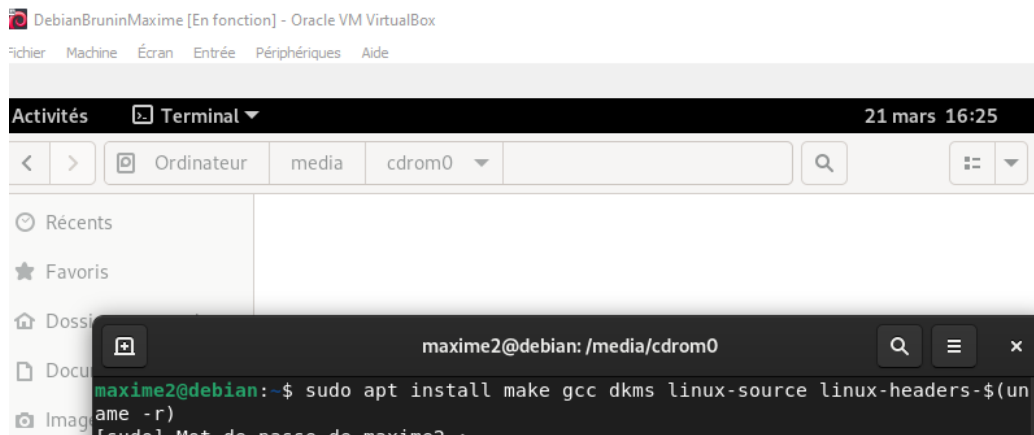
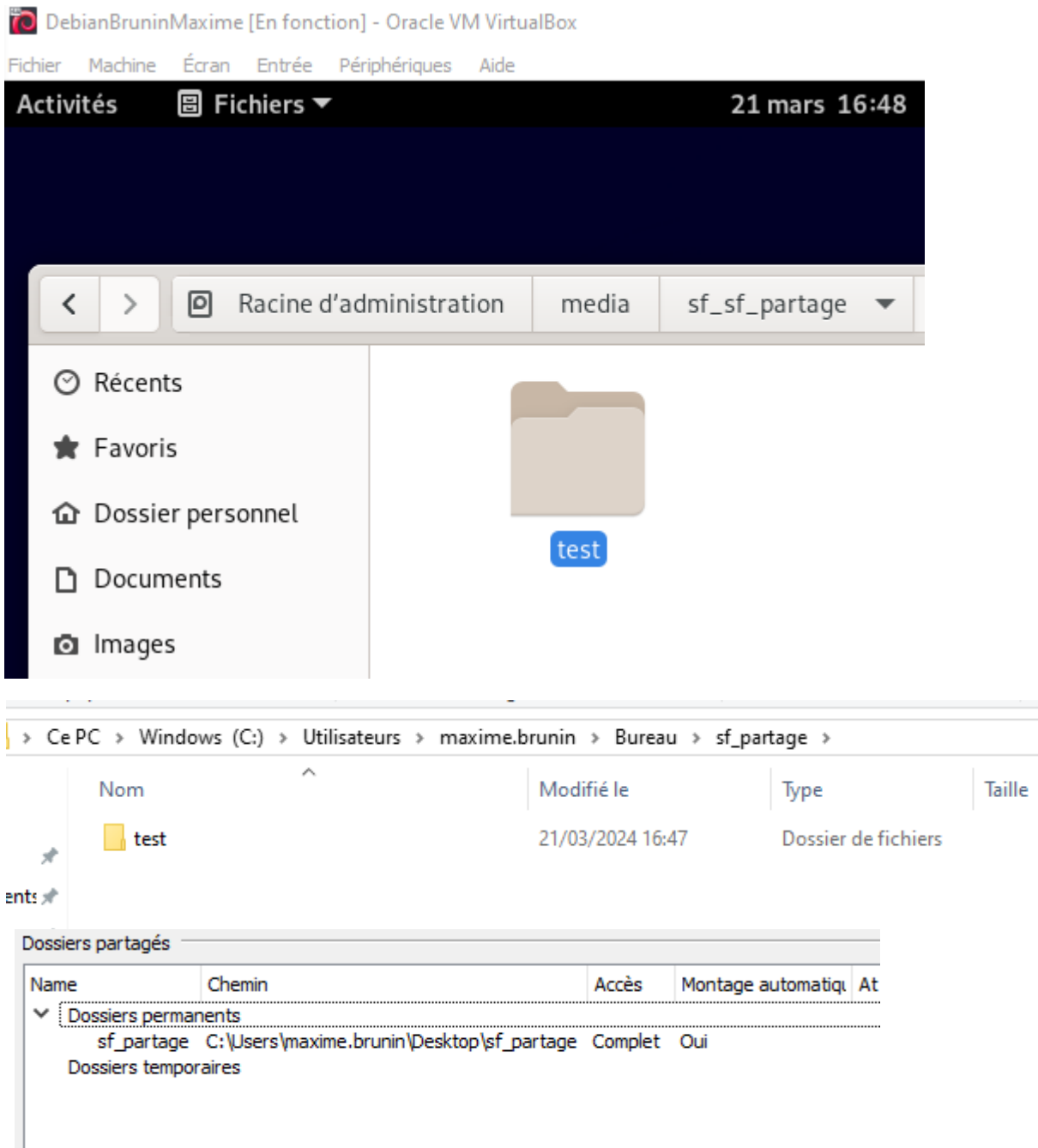
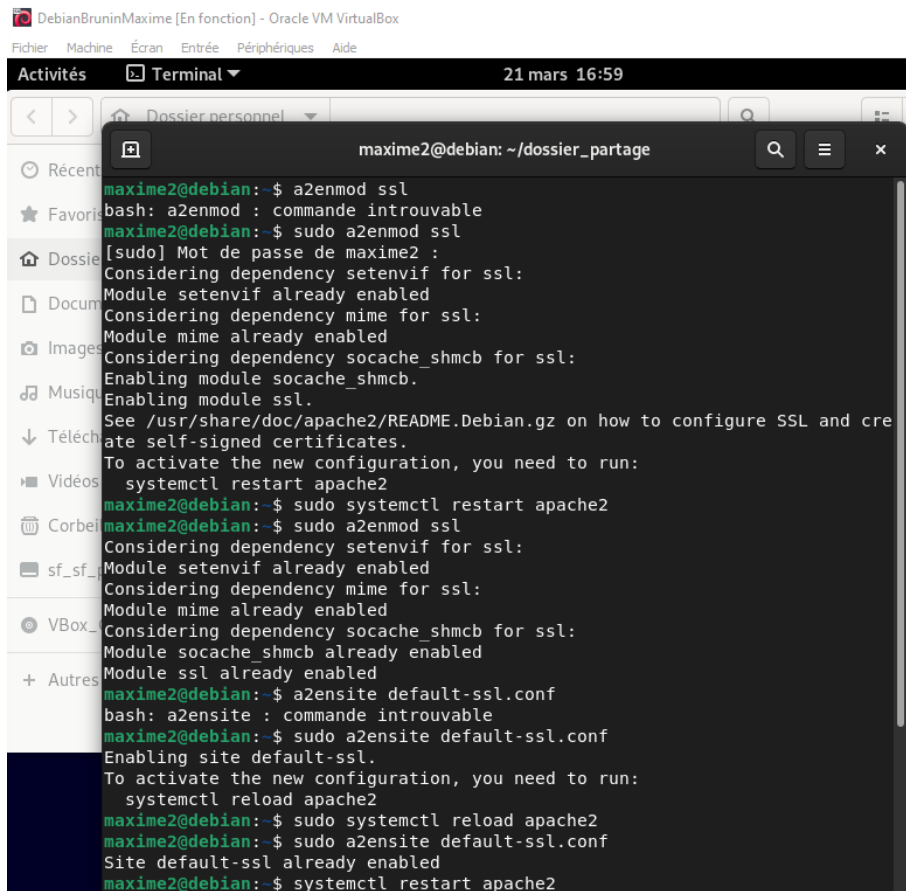


## I- Contexte



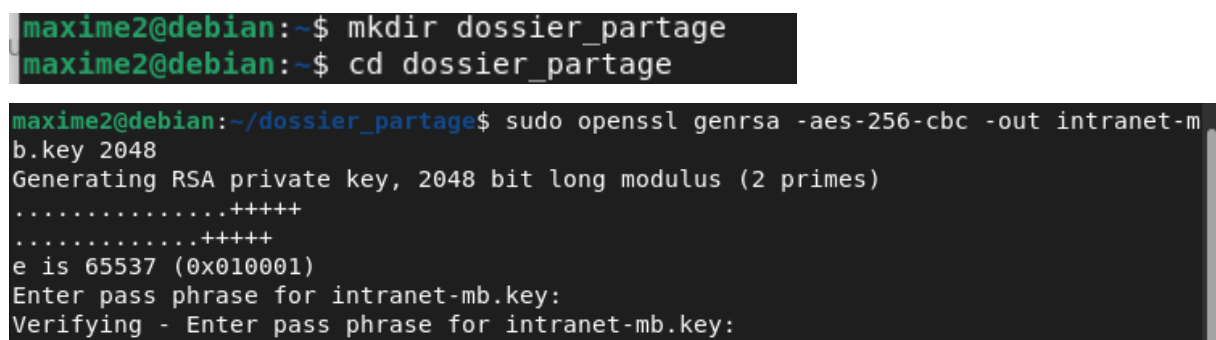


## II- Activation du mode SSL d'Apache 2



```
DebianBruninMaxime [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités Terminal 21 mars 16:59
maxime2@debian: ~/dossier_partage
maxime2@debian:~$ a2enmod ssl
bash: a2enmod : commande introuvable
maxime2@debian:~$ sudo a2enmod ssl
[sudo] Mot de passe de maxime2 :
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
maxime2@debian:~$ sudo systemctl restart apache2
maxime2@debian:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Module ssl already enabled
maxime2@debian:~$ a2ensite default-ssl.conf
bash: a2ensite : commande introuvable
maxime2@debian:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
maxime2@debian:~$ sudo systemctl reload apache2
maxime2@debian:~$ sudo a2ensite default-ssl.conf
Site default-ssl already enabled
maxime2@debian:~$ systemctl restart apache2
```

## III- Création d'un certificat X509 pour le serveur intranet



```
maxime2@debian:~$ mkdir dossier_partage
maxime2@debian:~$ cd dossier_partage
maxime2@debian:~/dossier_partage$ sudo openssl genrsa -aes-256-cbc -out intranet-mb.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for intranet-mb.key:
Verifying - Enter pass phrase for intranet-mb.key:
```

## Brunin Maxime TP serveur HTTP

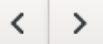
DebianBruninMaxime [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Activités

Fichiers

21 mars 17:03



Dossier personnel

dossier\_partage

🕒 Récents

★ Favoris

🏠 Dossier personnel

📁 Documents

📷 Images



intranet-mb.key



maxime2@debian: ~/dossier\_partage

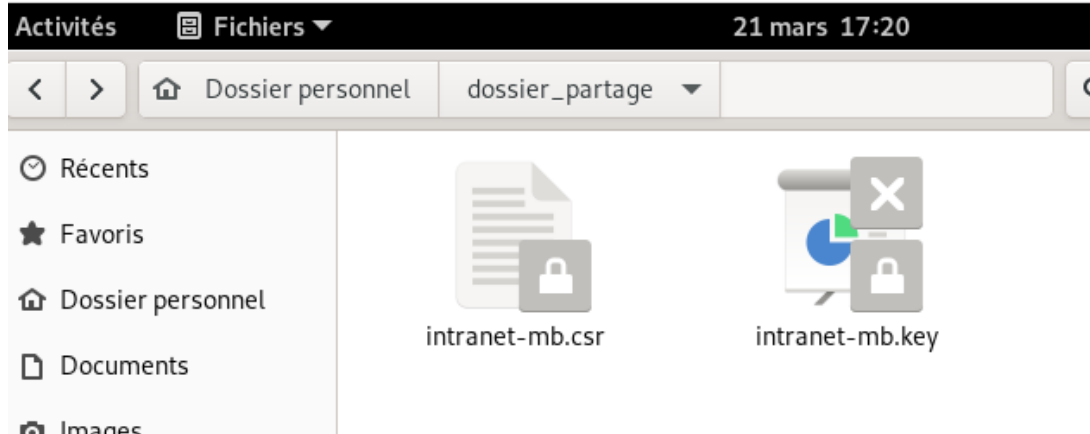


```
maxime2@debian:~/dossier_partage$ sudo openssl rsa -in intranet-mb.key -text
Enter pass phrase for intranet-mb.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
 00:bb:f5:18:a0:fb:27:b3:97:05:41:9e:e6:69:b7:
 ca:d0:59:41:59:f9:a8:66:97:36:d0:85:32:9b:79:
 21:cb:a0:8d:ba:9b:ee:be:c7:92:41:bc:03:00:c5:
 61:53:a8:8b:8b:6e:74:e2:db:d3:db:83:8b:78:e8:
 f9:88:a8:9d:ef:22:53:83:00:9f:73:01:59:ee:91:
 0f:cb:fc:49:7f:ca:56:86:1e:80:bb:4e:d6:b8:2e:
 c9:72:ff:ac:cf:30:40:2e:7f:05:3f:ef:72:e7:df:
 f8:08:fd:ad:59:2b:3a:80:a3:9c:e4:22:59:b6:25:
 22:43:24:08:3c:c8:d9:64:bd:da:ba:f2:12:49:b5:
 29:f2:df:3f:3b:a6:9c:15:50:18:71:04:85:16:91:
 f2:c8:c0:dc:16:17:84:9d:56:8e:3b:1a:d6:41:eb:
 16:6a:43:32:02:1b:e1:da:7c:3a:26:f9:f6:68:eb:
 50:a8:8e:b4:e1:d1:e4:67:ef:98:26:78:f8:ed:ba:
 f3:f2:6d:88:83:7b:cb:2e:ed:59:49:85:ec:d6:79:
 66:24:b0:9e:9a:1a:e0:95:96:ba:20:09:0a:9b:b4:
 90:c8:68:8a:ce:12:8c:58:e0:e6:4f:81:ea:09:cf:
 88:6f:72:6b:10:a5:54:95:23:20:d8:77:81:20:11:
 33:c9
publicExponent: 65537 (0x10001)
privateExponent:
 00:ac:c6:fd:40:de:1e:fc:c3:92:9d:63:c8:42:de:
 24:9d:a9:ae:9d:5b:16:26:58:52:97:14:1a:15:39:
 20:8b:e2:a6:e6:27:79:2b:fe:a0:bf:b4:68:be:48:
 b2:d3:08:58:5e:6f:c7:1a:d3:20:c8:e4:ff:4c:c2:
 3c:c0:16:e0:37:76:c2:75:e6:18:ac:cb:4d:34:34:
 3c:e5:32:a1:0d:cb:9e:05:e3:fc:4a:32:8a:c6:fc:
 9b:4a:0f:25:77:bf:ce:ff:ee:db:90:8e:38:7e:56:
 2f:d7:73:f9:e9:c2:07:21:41:45:73:a0:ef:fe:b3:
 db:ef:04:2c:5e:53:f3:22:da:9f:cb:62:ed:a0:64:
 84:35:57:fa:fc:27:03:2e:e0:4d:39:8f:b3:1a:97:
 dd:e7:3f:c3:1a:6c:82:5c:3a:cb:8d:3b:e1:79:84:
 fe:98:65:82:b9:a8:18:2f:92:60:f9:48:a8:0a:a1:
 0f:20:57:49:8f:13:02:fe:6b:03:2a:4a:a5:45:e6:
 2b:91:a7:db:ed:38:ca:a9:1e:47:9d:3d:88:77:9b:
 31:5e:26:7b:60:ca:c3:bb:36:e2:cf:93:86:40:93:
 cd:b6:a7:5d:20:32:c1:43:93:5c:c7:ae:64:e3:b9:
 31:bb:58:e2:46:d7:9d:c9:b0:03:26:95:e1:88:4f:
 5c:91
prime1:
 00:e1:64:ab:06:e3:31:6e:4c:1e:4d:e6:3a:53:85:
 81:cf:5a:a3:12:c2:3d:77:3d:97:e9:03:b1:d8:23:
 95:05:2c:b8:cb:ef:e8:be:81:95:a6:32:75:66:f5:
 71:b3:39:63:bd:a5:eb:3a:2b:3b:53:46:ce:57:2a:
 3e:79:50:cb:27:d3:b7:82:45:fe:16:2a:e3:17:a0:
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAU/UYoPsns5cFQZ7mabfK0FlBWfmoZpc20IUym3khy6CNupvu
vseSQbwDAMVhU6iLi2504tvT240Le0j5iKid7yJTgwCfcwFZ7pEPy/xJf8pWhh6A
u07WuC7Jcv+szzBALn8FP+9y59/4CP2tWSs6gK0c5CJZtiUiQyQIPmjZL3auvIS
SbUp8t8/06acFVAYcQSFFpHyMDcFheEnVa00xrWQesWakMyAhvh2nw6Jvn2a0tQ
qI604dHkZ++YJnj47brz8m2Ig3vLLu1ZSYXs1nlmJLCemhrglZa6IAkKm7SQyGiK
zhKMW0DmT4HqCc+Ib3JrEKVULSMg2HeBIBEzyQIDAQABAoIBAQCsxv1A3h78w5Kd
Y8hC3iSdqa6dWxYmWFKXFB0VOSCL4qbmJ3kr/qC/tGi+SLLTcFheb8ca0yDI5P9M
wjzAFuA3dsJ15hisY000NDzlmQENy54F4/xKMorG/JtKDyV3v87/7tuQjjh+Vi/X
c/npwgchQUVzo0/+s9vvBCxeU/Mi2p/LYu2gZIQ1V/r8JwMu4E05j7Mal93nP8Ma
bIJc0suN0+F5hP6YZYK5qBgvkmd5SKgKoQ8gV0mPEwL+awMqSqVF5iuRp9vt0Mqp
HkedPYh3mzFeJntgys07NuLPk4ZAK822p10gMsFDklzHrmTjuTG7W0JG153JsAMm
leGIT1yRAoGBA0FkqwbjMW5MHk3m0l0Fgc9aoxLCPXc9l+kDsdljQUsumvv6L6B
laYydWb1cbM5Y72l6zor01NGzlcqPnlQyyfTt4JF/hYq4xegvVRR5TTA6fyPIMaJ
KFyTWbteDioWUNPvyN0FlNFkIM5gWiPcg4TeQ02Q85R+0R7QdVyiGgfAoGBANV7
DHmfUdwTJW5INRhh9zK6TRBP1H0t2nY7jMPGrpWD6AmVYH4Hska0fshwW+0M/cg5
WXzKtIxTyq+nqbyeCc8yET1jzqkBbhbLxA00/G45nQpTBGPBTgLeuCI89tuBu43j
dq6EE5dnf4SwRJl7PslTLVUQmo05ZGoyCBDSKQcXAoGBAMt+GM8qFbnQLVgFcUlW
8ubjnPFVvyrFyD4PIOTUEznNy7YMDuTYL+SqD8b5+EJooP1bLEmj0HeSKL8Xm7np
0NFPW5HZYXJgHBF8BRN4s0h094wXK082a+NRAaWhYEaEwqTmC0JJRLfbn6bT504V
qoZ2rD5Gs2c2KPEXuzNbqX3fAoGBALwq15BpnNfksGuCjfpN73vxJpgoJV2pGxR3
7N1rtNrpB4/a8NB1UJchr7KxBvXtK4xesHgEnBvMh61lLZ5Bltfgg72eybvCH010
8hlI4Uuu0LMW9ZmP+1kgQyE6p0RYF587TzMJq9MaURX94JmAPplqaQgvuGI++Tl5
nA5nj+5FAoGAUWDbT8kvHQYpYIXvbAbBs02ZwBBR/4uQe1XDgzUhs8/d9zCL+wt
Ybl/aIE1yqRoIBT2CwLKM5GGQqn1h7y9giuqZF50zrPxzP8uNiUtX3JK5ARwRRl
ja9XqYzfL3wRg4sKe/ht3eC14SAsWIqbrsU+GNpjYkwIvo8ZHXJgMTw=
-----END RSA PRIVATE KEY-----
```

```
maxime2@debian:~/dossier_partage$ sudo openssl req -new -key intranet-mb.key -out
intranet-mb.csr
Enter pass phrase for intranet-mb.key:
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]:FR
State or Province Name (full name) [Some-State]:Nord
Locality Name (eg, city) []:Lille
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Dobucage
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.dobucage.intra
Email Address []:administateur@dobucage.intra

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



```
maxime2@debian:~/dossier_partage$ sudo openssl req -in intranet-mb.csr -text
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = FR, ST = Nord, L = Lille, O = Dobucage, CN = www.dobucage.intra, emailAddress = administrateur@dobucage.intra
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:
      00:bb:f5:18:a0:fb:27:b3:97:05:41:9e:e6:69:b7:
      ca:d0:59:41:59:f9:a8:66:97:36:d0:85:32:9b:79:
      21:cb:a0:8d:ba:9b:ee:be:c7:92:41:bc:03:00:c5:
      61:53:a8:8b:8b:6e:74:e2:db:d3:db:83:8b:78:e8:
      f9:88:a8:9d:ef:22:53:83:00:9f:73:01:59:ee:91:
      0f:cb:fc:49:7f:ca:56:86:1e:80:bb:4e:d6:b8:2e:
      c9:72:ff:ac:cf:30:40:2e:7f:05:3f:ef:72:e7:df:
      f8:08:fd:ad:59:2b:3a:80:a3:9c:e4:22:59:b6:25:
      22:43:24:08:3c:c8:d9:64:bd:da:ba:f2:12:49:b5:
      29:f2:df:3f:3b:a6:9c:15:50:18:71:04:85:16:91:
      f2:c8:c0:dc:16:17:84:9d:56:8e:3b:1a:d6:41:eb:
      16:6a:43:32:02:1b:e1:da:7c:3a:26:f9:f6:68:eb:
      50:a8:8e:b4:e1:d1:e4:67:ef:98:26:78:f8:ed:ba:
      f3:f2:6d:88:83:7b:cb:2e:ed:59:49:85:ec:d6:79:
      66:24:b0:9e:9a:1a:e0:95:96:ba:20:09:0a:9b:b4:
      90:c8:68:8a:ce:12:8c:58:e0:e6:4f:81:ea:09:cf:
      88:6f:72:6b:10:a5:54:95:23:20:d8:77:81:20:11:
      33:c9
    Exponent: 65537 (0x10001)
  Attributes:
    challengePassword :btsinfo
  Requested Extensions:
    Signature Algorithm: sha256WithRSAEncryption
      2e:c4:0c:40:a1:1d:d2:e5:75:6c:65:86:a8:5b:64:04:92:01:
      45:50:bf:eb:d1:8f:ad:f4:7d:2e:ae:3a:35:5e:90:05:0b:3b:
      56:7e:b0:c2:97:86:4a:92:ed:0d:cf:0a:7f:ac:ea:5a:29:17:
      2a:13:19:a3:09:49:b4:a3:fd:19:48:2c:59:e7:04:b9:02:b1:
      5c:38:40:f6:e2:52:77:53:0c:0f:3d:c6:30:79:88:e1:5d:25:
      1b:ac:64:28:f9:cd:b9:95:14:4d:d2:e2:5d:0a:f7:b6:d1:ec:
      5e:84:51:65:4d:56:c4:61:28:27:6d:55:e9:61:43:a8:7d:5b:
      17:e6:0e:87:e4:f5:20:13:b4:42:36:56:bc:fa:eb:d7:e1:d2:
      e9:df:84:c5:15:9a:e9:d4:34:4f:93:6a:c6:4e:6c:fa:f3:e2:
      05:86:f8:dd:76:60:c6:7c:85:24:b7:3b:b3:c1:da:98:24:79:
      71:ef:30:c9:8a:cf:b0:56:75:95:e3:56:d0:4c:7e:b4:12:aa:
      3e:2b:48:08:c1:d9:f8:cb:82:8b:07:66:77:10:71:53:1a:a6:
      3d:06:45:07:2c:3d:31:e0:d0:1b:ce:d2:71:ff:e0:28:5c:13:
      c3:a1:94:eb:38:cb:9d:e4:ae:14:47:e3:e3:c6:53:97:6c:7d:
```



```
78:a3:c1:1f
-----BEGIN CERTIFICATE REQUEST-----
MIIC5zCCAC8CAQAwYkxCZAJBgNVBAYTAKZSMQ0wCwYDVQQIDAR0b3JkMQ4wDAYD
VQQHDAVMaWxsZTERMA8GA1UECgwIRG9idWNhZ2UxGzAZBgNVBAMMEnd3dy5kb2J1
Y2FnZS5pbmRyYTERMCKGCSqGSIb3DQEJARYcYWRtaW5pc3RhdGV1ckBkb2J1Y2Fn
ZS5pbmRyYTERCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALv1GKD7J70X
BUGe5mm3ytBZQVn5qGaXNtCFMpt5Icugjbqb7r7HkkG8AwDFYV0oi4tud0Lb09uD
i3jo+Yione8iU4MAN3MBWe6RD8v8SX/KVoYegLt01rguyXL/rM8wQC5/BT/vcuff
+Aj9rVkr0oCjn0QiWbYlIkMkCDzI2WS92rryEkm1KfLfPzumnBVQGHEEHraR8sjA
3BYXhJ1Wjjsa1kHrFmpDMgIb4dp80ib59mjruKI0t0HR5GfvmCZ4+0268/JtiIN7
yy7tWUmF7NZ5ZiSwnpoa4JWWuiAJCpu0kMhois4SjFjg5k+B6gnPiG9yaxClVJUj
INh3gSARM8kCAwEAAaAYMBYGCSqGSIb3DQEJBzEJDAAdidHNpbmZvMA0GCSqGSIb3
DQEBGwUAA4IBAQAuxAxAoR3S5XVsZYaoW2QEkGFFUL/r0Y+t9H0urjo1XpAFCztW
frDCL4ZKku0Nzwp/r0paKRcqExmjCUm0o/0ZSCxZ5wS5ArFc0ED24lJ3UwwPPcYw
eYjhXSUbrGQo+c25lRRN0uJdCve20exehFFlTVbEYSgnbVXpYU0ofVsX5g6H5PUg
E7RCNla8+uvX4dLp34TFFZrp1DRPk2rGTmz68+IFhvjdmdGgfIUktzuzwdqYJHlx
7zDJis+wVnWV41bQTH60Ego+K0gIwdn4y4KLB2Z3EHFTGqY9BkUHLd0x4NAbztJx
/+AoXBPDoZTrOMud5K4UR+Pjxl0XbH14o8Ef
-----END CERTIFICATE REQUEST-----
```

#### IV- Paramétrage d'Apache

```
maxime2@debian:~/dossier_partage$ sudo cp intranet-mb.key intranet-mb.key.org
```



```
maxime2@debian:~/dossier_partage$ sudo openssl rsa -in intranet-mb.key.org -out
intranet-mb.key
Enter pass phrase for intranet-mb.key.org:
writing RSA key
```

La clé RSA est écrite sur le document copié depuis le document original. La commande permet donc de copier une clé RSA d'un document à un autre.

```
maxime2@debian:~/dossier_partage$ sudo chmod 400 intranet-mb.key
```

Avec cette commande Le propriétaire du fichier a le droit de lire le fichier, le groupe auquel appartient le fichier, ni les autres utilisateurs n'ont de droits d'accès au fichier.


```
maxime2@debian:~/dossier_partage$ ls -l
total 12
-rw-r--r-- 1 root root 1082 21 mars 17:19 intranet-mb.csr
-r----- 1 root root 1679 22 mars 15:50 intranet-mb.key
-rw----- 1 root root 1766 22 mars 15:48 intranet-mb.key.org
```

```
maxime2@debian:~/certificats$ sudo mv intranet-mb.crt /etc/ssl/certs
[sudo] Mot de passe de maxime2 :
maxime2@debian:~/certificats$ sudo mv intranet-mb.key /etc/ssl/private
```

```
# SSLCertificateFile directive is needed:
SSLCertificateFile /etc/ssl/certs/intranet-mb.crt
SSLCertificateKeyFile /etc/ssl/private/intranet-mb.key
```

```
SSLCertificateFile /etc/ssl/certs/intranet-mb.crt
SSLCertificateKeyFile /etc/ssl/private/intranet-mb.key
```

🔒 https://localhost



## Apache2 Debian Default Page

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective \*-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed



<a href="http://www.dobucage.intra">www.dobucage.intra</a>	
<b>Nom du sujet</b>	
Pays	FR
État / Province	Nord
Localité	Lille
Organisation	Dobucage
Nom courant	www.dobucage.intra
Adresse e-mail	administateur@dobucage.intra
<b>Nom de l'émetteur</b>	
Pays	FR
État / Province	Nord
Localité	Lille
Organisation	AC-Dobucage
Nom courant	www.dobucage.intra
Adresse e-mail	administrateur-ac@dobucage.intra
<b>Validité</b>	
Pas avant	Thu, 28 Mar 2024 07:01:08 GMT
Pas après	Fri, 28 Mar 2025 07:01:08 GMT
<b>Informations sur la clé publique</b>	
Algorithme	RSA
Taille de la clé	2048
Exposant	65537
Module	BB:F5:18:A0:FB:27:B3:97:05:41:9E:E6:69:B7:CA:D0:59:41:59:F9:A8:66:97:3...
<b>Divers</b>	
Numéro de série	4B:39:D9:EB:77:87:1D:54:50:31:0C:87:54:C5:08:BB:D6:7E:43:0D
Algorithme de signature	SHA-256 with RSA Encryption
Version	1
Télécharger	<a href="#">PEM(cert)</a> <a href="#">PEM(chain)</a>
<b>Empreintes numériques</b>	
SHA-256	5F:A6:57:48:6F:20:32:AE:EF:E6:3C:FF:83:3A:78:30:39:14:77:00:2E:6B:DA:1...
SHA-1	6F:22:E4:CC:20:D5:97:C6:C7:64:B7:C6:C3:02:A1:4B:6C:AA:8E:36

## VII – Quizz

Une clé privée RSA est une clé asymétrique.

Une clé publique RSA est une clé asymétrique

Une clé de session est une clé symétrique.