MINI PROJECT

352 CIS Lab (Information Security)

Marks: 7 Marks

Name: Sarah Fahad Akala **ID : 445804653**

Name: Lama Ahmed Alfusili **ID : 445803877**

Name: Bsmah Ibrahim Al Amer **ID : 444806632**

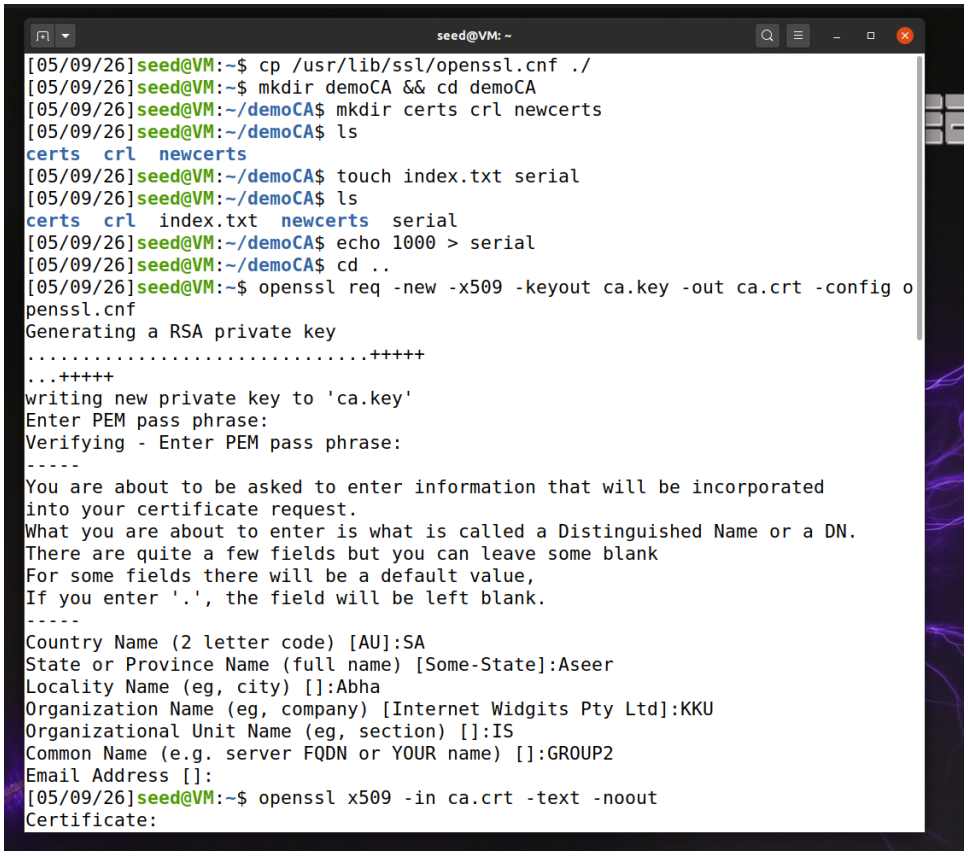
Instructions:

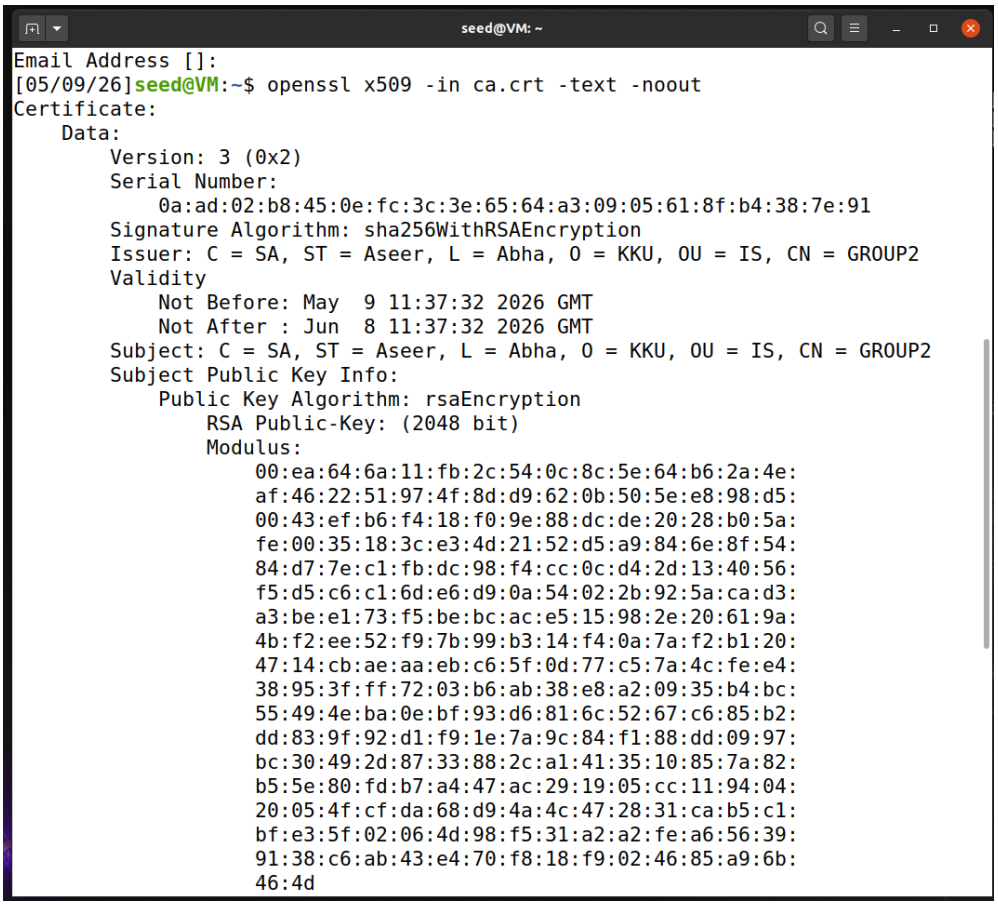
1- **Group activity: Max 3 students.**
2- **Use SEED Ubuntu and Kali Linux to solve the questions.**
3- **Due Date: 9th May 2025**
4- **Take screenshots for your work.**
5- **For each task and submit Online**

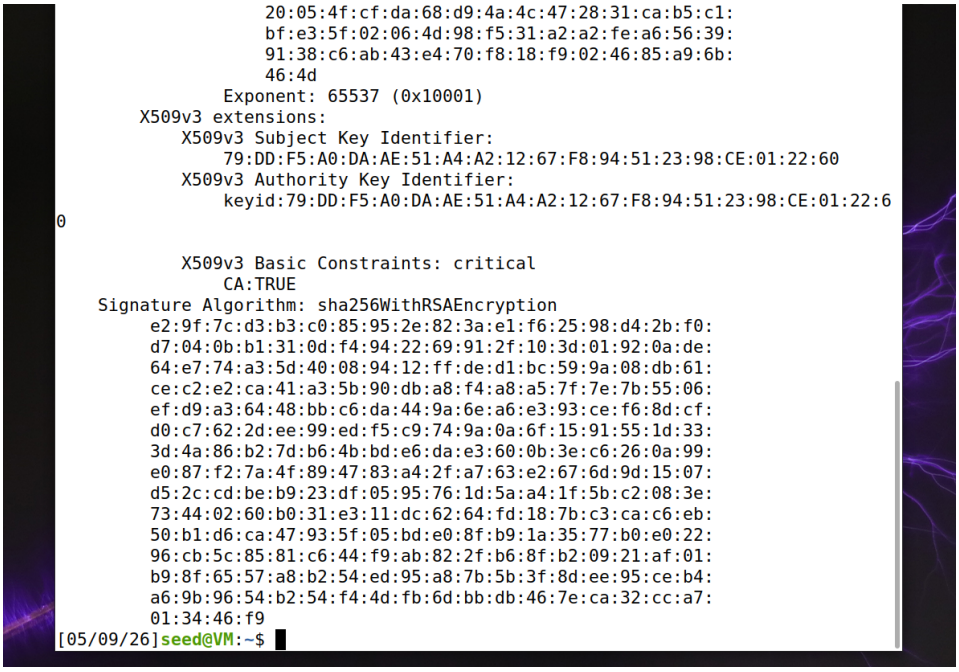
Question 1 (3.5 Marks)

Create a certificate for the following server: SEEDPKILab2020.com by apply the following steps:

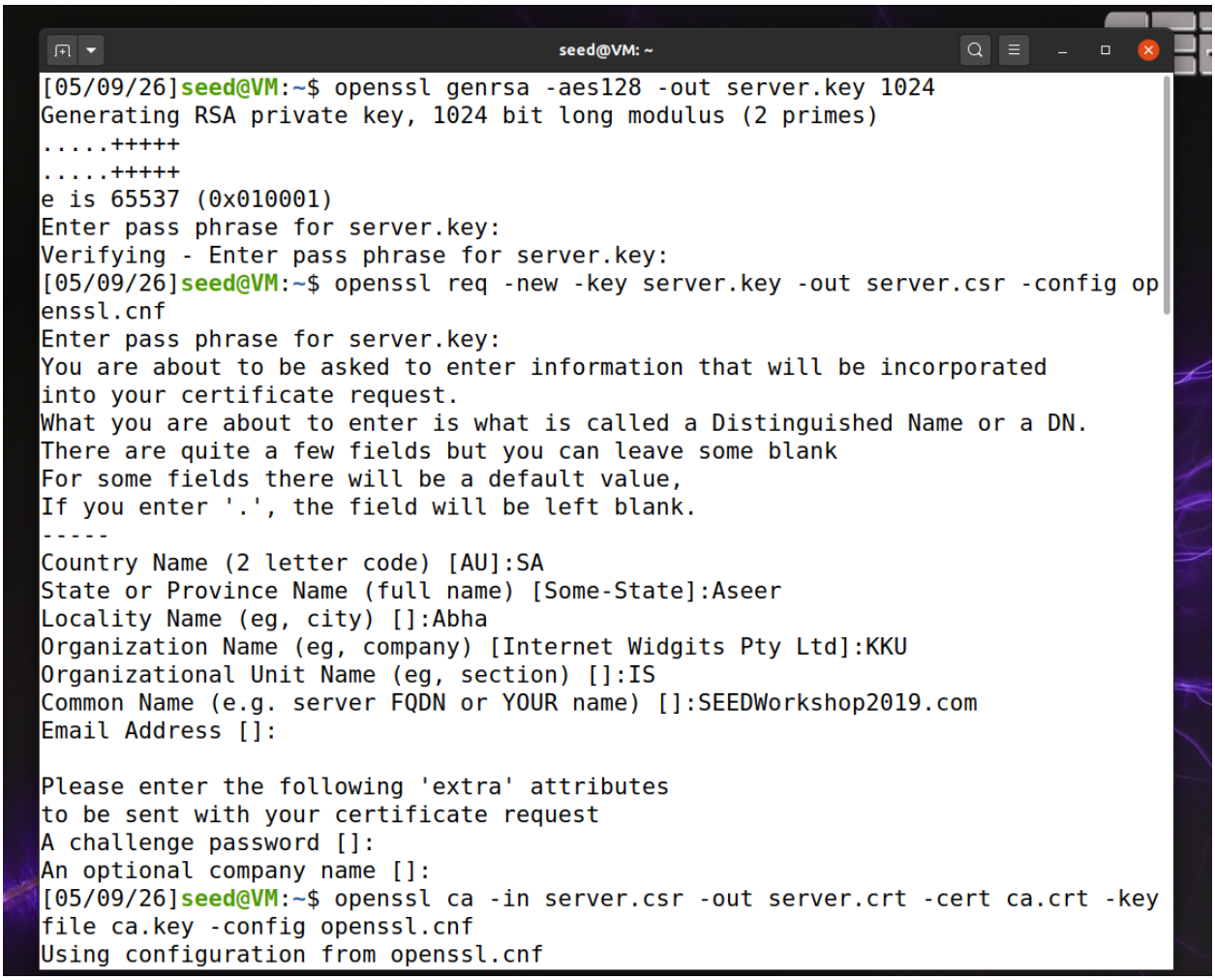
1. Become a Certificate Authority CA

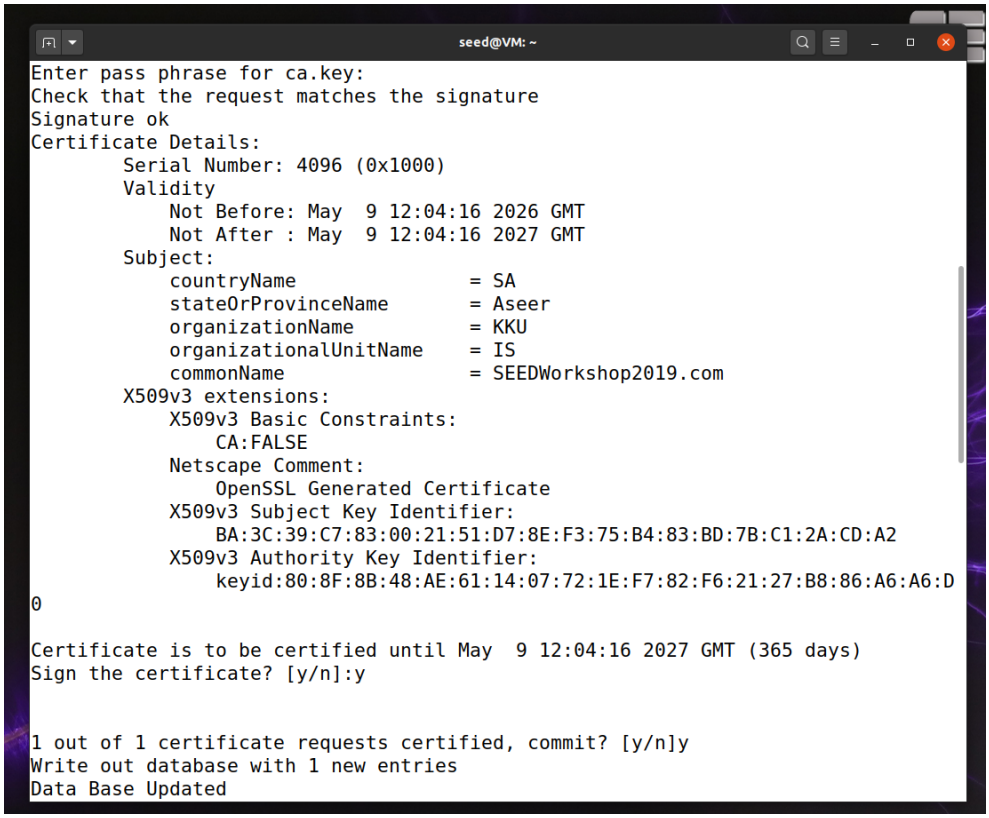


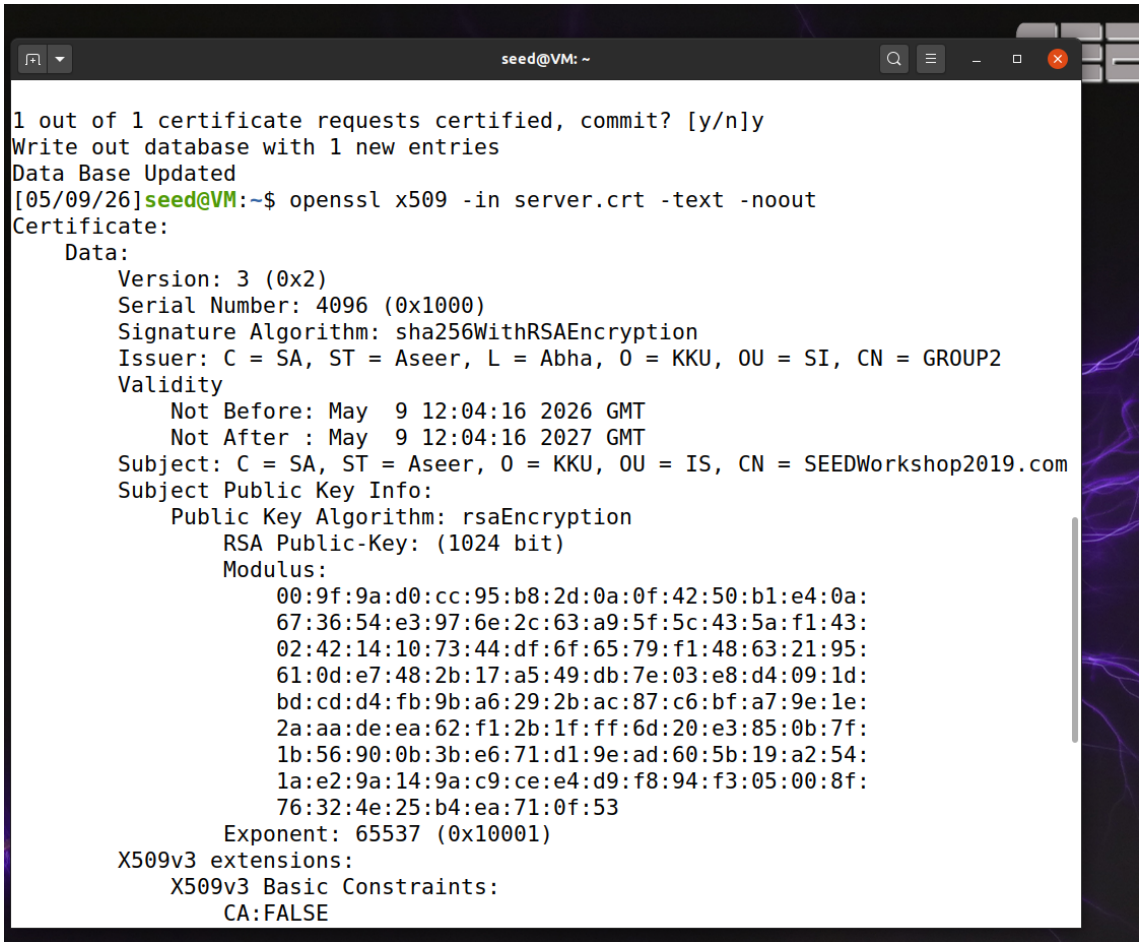


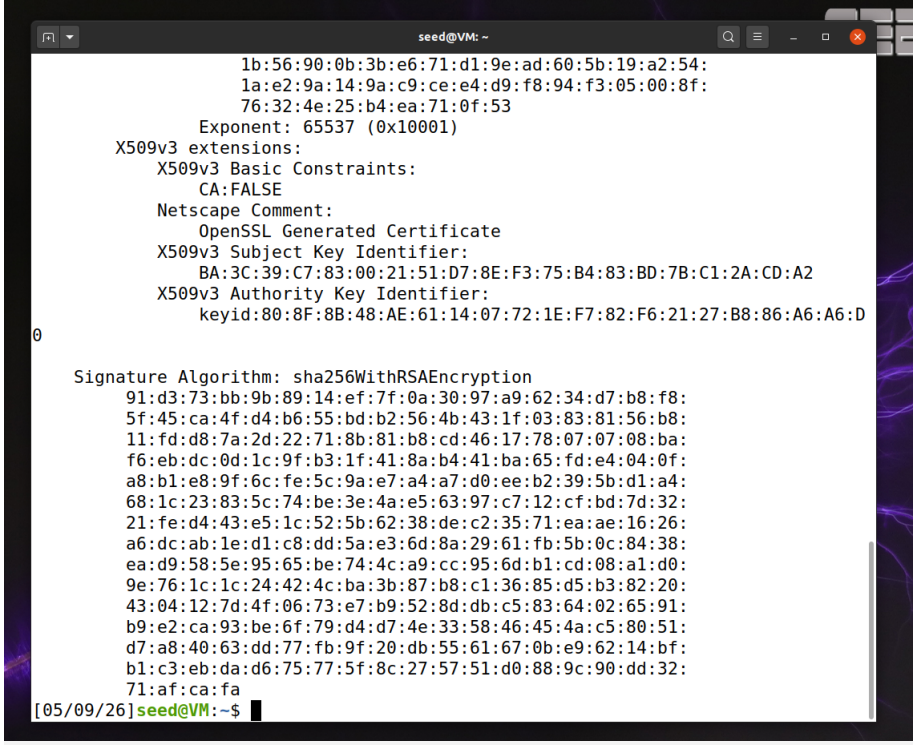


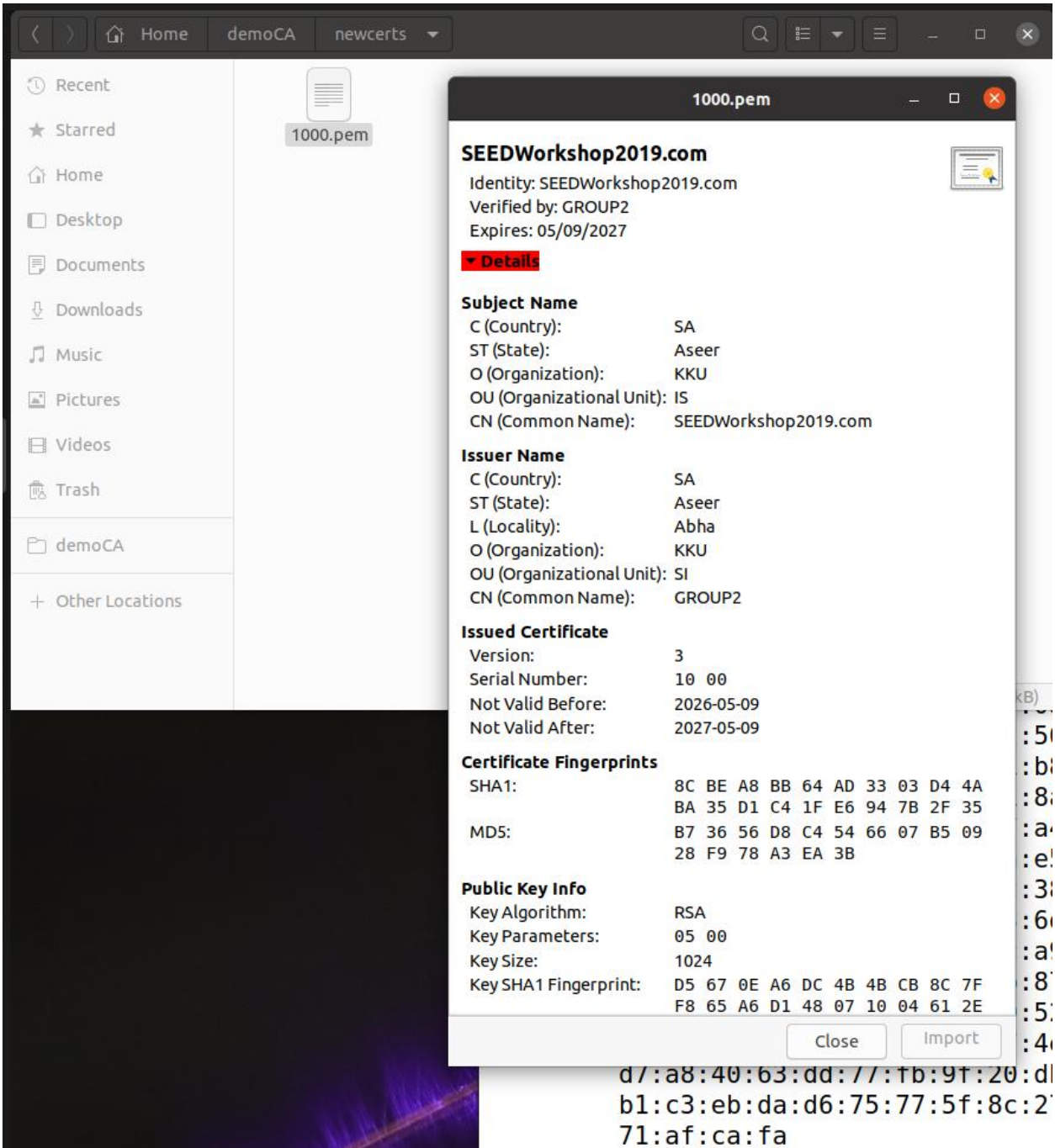
2. Create a certificate for seedworkshop2019.com




seed@VM: ~
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 4096 (0x1000)
Validity
Not Before: May 9 12:04:16 2026 GMT
Not After : May 9 12:04:16 2027 GMT
Subject:
countryName = SA
stateOrProvinceName = Aseer
organizationName = KKU
organizationalUnitName = IS
commonName = SEEDWorkshop2019.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
BA:3C:39:C7:83:00:21:51:D7:8E:F3:75:B4:83:BD:7B:C1:2A:CD:A2
X509v3 Authority Key Identifier:
keyid:80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D
0
Certificate is to be certified until May 9 12:04:16 2027 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

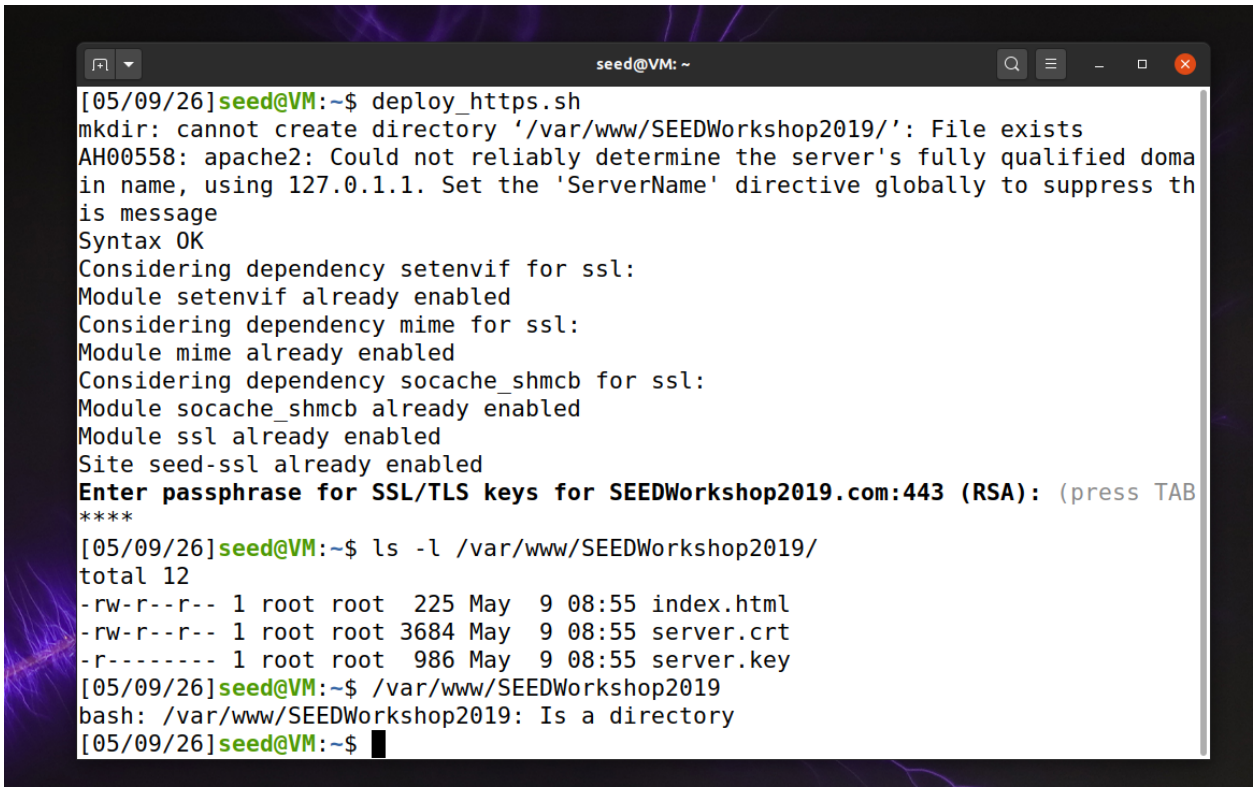

seed@VM: ~
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[05/09/26]seed@VM:~$ openssl x509 -in server.crt -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4096 (0x1000)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = SA, ST = Aseer, L = Abha, O = KKU, OU = SI, CN = GROUP2
Validity
Not Before: May 9 12:04:16 2026 GMT
Not After : May 9 12:04:16 2027 GMT
Subject: C = SA, ST = Aseer, O = KKU, OU = IS, CN = SEEDWorkshop2019.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (1024 bit)
Modulus:
00:9f:9a:d0:cc:95:b8:2d:0a:0f:42:50:b1:e4:0a:
67:36:54:e3:97:6e:2c:63:a9:5f:5c:43:5a:f1:43:
02:42:14:10:73:44:df:6f:65:79:f1:48:63:21:95:
61:0d:e7:48:2b:17:a5:49:db:7e:03:e8:d4:09:1d:
bd:cd:d4:fb:9b:a6:29:2b:ac:87:c6:bf:a7:9e:1e:
2a:aa:de:ea:62:f1:2b:1f:ff:6d:20:e3:85:0b:7f:
1b:56:90:0b:3b:e6:71:d1:9e:ad:60:5b:19:a2:54:
1a:e2:9a:14:9a:c9:ce:e4:d9:f8:94:f3:05:00:8f:
76:32:4e:25:b4:ea:71:0f:53
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE

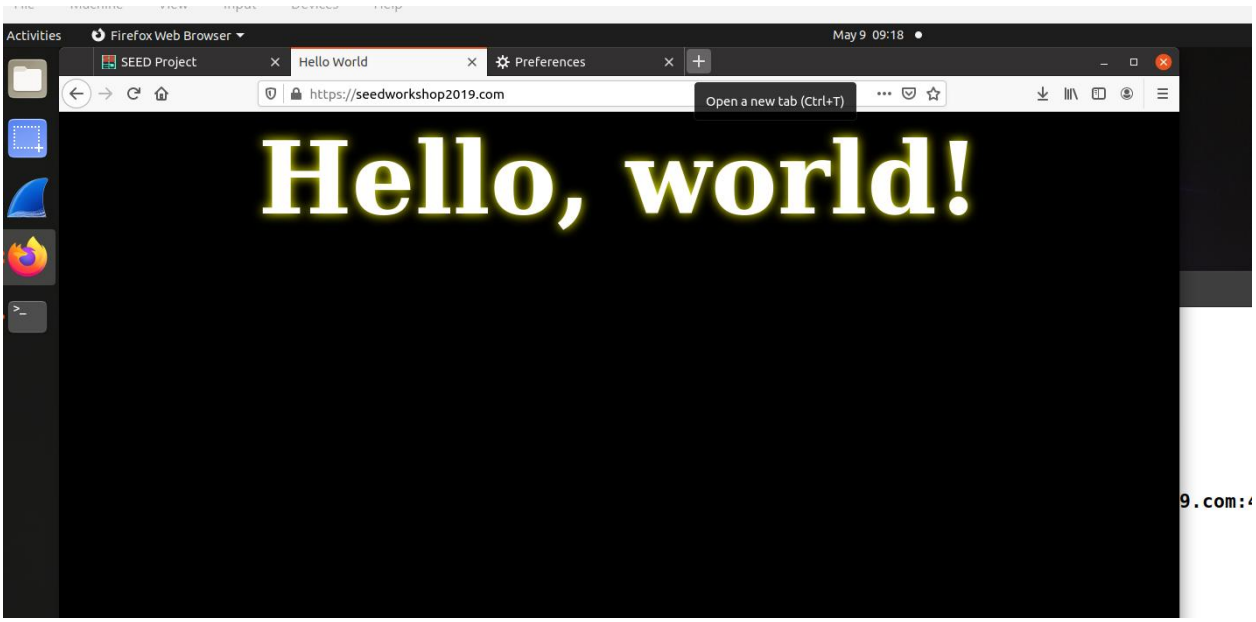

seed@VM: ~
1b:56:90:0b:3b:e6:71:d1:9e:ad:60:5b:19:a2:54:
1a:e2:9a:14:9a:c9:ce:e4:d9:f8:94:f3:05:00:8f:
76:32:4e:25:b4:ea:71:0f:53
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
BA:3C:39:C7:83:00:21:51:D7:8E:F3:75:B4:83:BD:7B:C1:2A:CD:A2
X509v3 Authority Key Identifier:
keyid:80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D
0
Signature Algorithm: sha256WithRSAEncryption
91:d3:73:bb:9b:89:14:ef:7f:0a:30:97:a9:62:34:d7:b8:f8:
5f:45:ca:4f:d4:b6:55:bd:b2:56:4b:43:1f:03:83:81:56:b8:
11:fd:d8:7a:2d:22:71:8b:81:b8:cd:46:17:78:07:07:08:ba:
f6:eb:dc:0d:1c:9f:b3:1f:41:8a:b4:41:ba:65:fd:e4:04:0f:
a8:b1:e8:9f:6c:fe:5c:9a:e7:a4:a7:d0:ee:b2:39:5b:d1:a4:
68:1c:23:83:5c:74:be:3e:4a:e5:63:97:c7:12:cf:bd:7d:32:
21:fe:d4:43:e5:1c:52:5b:62:38:de:c2:35:71:ea:ae:16:26:
a6:dc:ab:1e:d1:c8:dd:5a:e3:6d:8a:29:61:fb:5b:0c:84:38:
ea:d9:58:5e:95:65:be:74:4c:a9:cc:95:6d:b1:cd:08:a1:d0:
9e:76:1c:1c:24:42:4c:ba:3b:87:b8:c1:36:85:d5:b3:82:20:
43:04:12:7d:4f:06:73:e7:b9:52:8d:db:c5:83:64:02:65:91:
b9:e2:ca:93:be:6f:79:d4:d7:4e:33:58:46:45:4a:c5:80:51:
d7:a8:40:63:dd:77:fb:9f:20:db:55:61:67:0b:e9:62:14:bf:
b1:c3:eb:da:d6:75:77:5f:8c:27:57:51:d0:88:9c:90:dd:32:
71:af:ca:fa
[05/09/26]seed@VM:~$

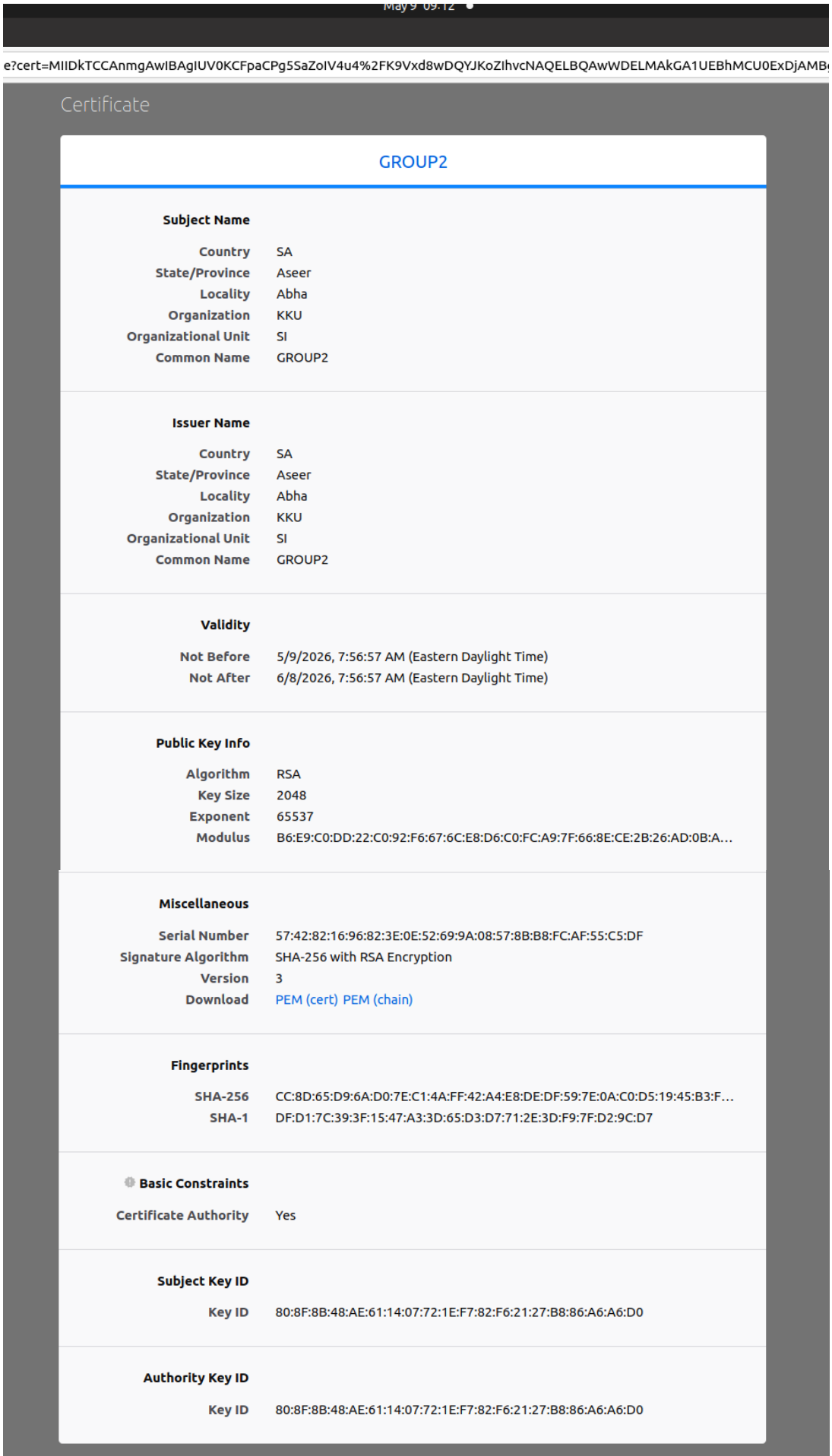

Home
demoCA
newcerts
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
demoCA
Other Locations
1000.pem
1000.pem
SEEDWorkshop2019.com
Identity: SEEDWorkshop2019.com
Verified by: GROUP2
Expires: 05/09/2027
Details
Subject Name
C (Country): SA
ST (State): Aseer
O (Organization): KKU
OU (Organizational Unit): IS
CN (Common Name): SEEDWorkshop2019.com
Issuer Name
C (Country): SA
ST (State): Aseer
L (Locality): Abha
O (Organization): KKU
OU (Organizational Unit): SI
CN (Common Name): GROUP2
Issued Certificate
Version: 3
Serial Number: 10 00
Not Valid Before: 2026-05-09
Not Valid After: 2027-05-09
Certificate Fingerprints
SHA1: 8C BE A8 BB 64 AD 33 03 D4 4A BA 35 D1 C4 1F E6 94 7B 2F 35
MD5: B7 36 56 D8 C4 54 66 07 B5 09 28 F9 78 A3 EA 3B
Public Key Info
Key Algorithm: RSA
Key Parameters: 05 00
Key Size: 1024
Key SHA1 Fingerprint: D5 67 0E A6 DC 4B 4B CB 8C 7F F8 65 A6 D1 48 07 10 04 61 2E
Close
Import
d7:a8:40:63:dd:77:fb:9f:20:d
b1:c3:eb:da:d6:75:77:5f:8c:2
71:af:ca:fa

3. Deploying Certificate in an Apache-Based HTTPS Website

Note: Submit ca.crt and server.crt that must include you Group number






May 9 09:12
e?cert=MIIDkTCCAnmgAwIBAgIUV0KCFpaCPg5SaZoIV4u4%2FK9Vxd8wDQYJKoZIhvcNAQELBQAwWDELMAkGA1UEBhMCU0ExDjAMB
Certificate
GROUP2
Subject Name
Country SA
State/Province Aseer
Locality Abha
Organization KKU
Organizational Unit SI
Common Name GROUP2
Issuer Name
Country SA
State/Province Aseer
Locality Abha
Organization KKU
Organizational Unit SI
Common Name GROUP2
Validity
Not Before 5/9/2026, 7:56:57 AM (Eastern Daylight Time)
Not After 6/8/2026, 7:56:57 AM (Eastern Daylight Time)
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus B6:E9:C0:DD:22:C0:92:F6:67:6C:E8:D6:C0:FC:A9:7F:66:8E:CE:2B:26:AD:0B:A…
Miscellaneous
Serial Number 57:42:82:16:96:82:3E:0E:52:69:9A:08:57:8B:B8:FC:AF:55:C5:DF
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 CC:8D:65:D9:6A:D0:7E:C1:4A:FF:42:A4:E8:DE:DF:59:7E:0A:C0:D5:19:45:B3:F…
SHA-1 DF:D1:7C:39:3F:15:47:A3:3D:65:D3:D7:71:2E:3D:F9:7F:D2:9C:D7
Basic Constraints
Certificate Authority Yes
Subject Key ID
Key ID 80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D0
Authority Key ID
Key ID 80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D0

Certificate

SEEDWorkshop2019.com | GROUP2

Subject Name

Country	SA
State/Province	Aseer
Organization	KKU
Organizational Unit	IS
Common Name	SEEDWorkshop2019.com

Issuer Name

Country	SA
State/Province	Aseer
Locality	Abha
Organization	KKU
Organizational Unit	SI
Common Name	GROUP2

Validity

Not Before	5/9/2026, 8:04:16 AM (Eastern Daylight Time)
Not After	5/9/2027, 8:04:16 AM (Eastern Daylight Time)

Public Key Info

Algorithm	RSA
Key Size	1024
Exponent	65537
Modulus	9F:9A:D0:CC:95:B8:2D:0A:0F:42:50:B1:E4:0A:67:36:54:E3:97:6E:2C:63:A9:5F:...

Miscellaneous

Serial Number	10:00
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	28:4C:30:5A:F9:35:E0:CA:D0:8C:CC:7F:9D:ED:04:D9:58:C9:64:57:3F:F4:57:A2...
SHA-1	8C:BE:A8:BB:64:AD:33:03:D4:4A:BA:35:D1:C4:1F:E6:94:7B:2F:35

Basic Constraints

Certificate Authority	No

Subject Key ID

Key ID	BA:3C:39:C7:83:00:21:51:D7:8E:F3:75:B4:83:BD:7B:C1:2A:CD:A2

Authority Key ID

Key ID	80:8F:8B:48:AE:61:14:07:72:1E:F7:82:F6:21:27:B8:86:A6:A6:D0

Question 2: **(3.5 Marks)**

Network Scanning and MITM Attacks

1. Network scanning using nmap tool.

2. Network package analysis tool such as Wireshark.

3. Perform MITM attack using ARP Cache Poisoning Attack tool such as Ettercap, and analyze the result using Wireshark.

Note: Show the username and password as group # as credentials that you have used on the Victim Side