**Lab Environment**

We built and made up the container with :

dcbuild

dcup

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Then we got access to the docker shell with docksh command.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**DNS setup**

We added the IP of our container with the intended domain name in /etc/hosts file of our host VM.This simulates a DNS Cache poisoning.

A screenshot of a computer

AI-generated content may be incorrect.

**Lab Tasks**

**Task 1: Becoming a Certificate Authority (CA)**

We created the copy of openssl.cnf file so the original one did not got lost.

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

We created the serial and index.txt file in our working folder which are required by openssl to create and maintain authority database.

A screenshot of a computer

AI-generated content may be incorrect.

We created a self signed certificate for our certificate authority.

A screenshot of a computer

AI-generated content may be incorrect.

**• What part of the certificate indicates this is a CA’s certificate?**

The CA : True clause indicate that the certificate is of certificate is of certificate authority.

A screenshot of a computer

AI-generated content may be incorrect.

**• What part of the certificate indicates this is a self-signed certificate?**

The same subject key and Authority key indicates that it is a self signed certificate.

A screenshot of a computer

AI-generated content may be incorrect.

**• In the RSA algorithm, we have a public exponent e, a private exponent d, a modulus n, and two secret numbers p and q, such that n = pq. Please identify the values for these elements in your certificate and key files.**

Modulus (n=pq):

00:aa:7f:94:30:74:fa:53:fe:58:be:7d:2b:7a:c3:

af:3a:6a:b8:7f:c9:68:b1:7b:dc:0b:65:b0:ca:3e:

5d:b1:0e:d4:2e:7f:03:c8:0c:3c:51:3c:e2:47:2d:

ba:e2:8a:23:6f:d3:ff:fe:c8:e4:5f:c0:c7:1a:a4:

06:3b:19:13:f8:71:73:ea:f7:ce:cf:07:aa:f3:ce:

c9:7c:c0:75:d6:58:36:02:63:38:27:32:45:4d:86:

38:4d:73:82:79:1d:19:d2:ef:54:1f:7d:bb:13:e1:

51:fe:0e:01:13:c0:b9:0e:00:83:13:51:ee:b5:95:

2f:ff:67:c1:e7:17:90:ad:38:4f:fc:92:eb:53:b4:

85:ba:78:b2:60:65:d2:cb:c2:55:78:b3:f2:30:e4:

60:e2:3b:b5:49:ad:25:3e:2c:38:b9:fe:7e:44:6f:

ad:22:7a:ec:51:df:40:2c:3d:64:7b:47:a5:e1:2a:

b9:b8:d5:48:fb:22:30:7a:31:57:0a:eb:ba:f7:85:

60:f5:61:62:b8:9b:3e:d2:fe:cf:21:81:ee:e0:54:

91:88:14:ff:0a:ef:c5:1e:0f:09:cd:24:71:12:f6:

81:15:37:d9:40:62:1b:98:28:ec:4a:0b:31:c4:f9:

89:9a:5a:78:c8:cc:ec:14:97:2a:9b:10:3e:b9:df:

8e:e7:2d:54:bc:02:b1:62:a3:23:35:a9:8c:67:f7:

d6:b9:85:b4:2b:f6:9e:2c:e8:85:1d:82:bb:b1:b9:

d0:b4:a9:ce:91:59:04:2e:4d:da:2c:ec:48:22:5e:

63:c3:27:29:1d:bb:a2:c5:a1:44:aa:51:87:fe:1f:

5c:a4:f9:7b:d7:28:f5:94:15:e5:46:5f:0e:29:73:

40:60:42:e6:c1:ad:24:c3:86:5e:99:57:17:ea:f4:

7f:e4:8f:1d:ed:4a:c7:e6:14:48:4f:8b:49:db:cf:

13:f0:0e:56:89:28:cd:1c:14:73:8d:58:be:89:c6:

ee:74:22:f8:82:ce:ba:20:18:81:6f:10:31:50:23:

32:50:ba:5f:a7:31:a5:50:55:d1:63:9e:4b:6d:f6:

a5:ff:2c:cf:49:c2:8e:89:75:da:57:2e:b4:6a:20:

55:58:8f:79:ae:27:98:ea:9e:98:9b:9d:fe:79:45:

57:d2:86:bc:26:d5:51:96:21:47:e9:03:24:ea:63:

0f:49:62:9f:ed:5a:be:de:35:0b:78:5a:67:ae:3b:

51:67:2a:e3:59:3f:c5:1a:80:1c:52:4d:2f:51:3b:

f8:09:6e:38:f2:83:79:d8:58:76:fb:c2:18:9b:7a:

03:46:fb:73:ba:30:02:49:f0:8c:09:09:8e:75:71:

4e:60:ed

A screen shot of a computer

AI-generated content may be incorrect.

publicExponent(e): 65537 (0x10001)

privateExponent(d):

5e:3c:7b:ac:b8:cb:2f:a7:92:67:5f:09:ac:26:02:

71:18:51:77:97:db:fc:d5:47:cf:28:da:a9:3e:05:

4c:fa:b4:3e:2a:c7:ed:47:0e:03:9c:d2:38:a3:46:

fb:35:7c:d6:af:67:7b:ec:8f:85:79:28:d3:49:bb:

83:e8:9d:88:21:34:ff:b7:0e:20:91:cd:64:4a:74:

45:36:9f:2a:e4:c0:9d:5b:37:cb:3a:56:e1:bd:80:

db:16:30:14:3f:08:69:f5:0c:1b:07:c4:61:fd:94:

f3:05:cc:84:9d:6d:eb:16:4f:5c:5b:59:c4:15:7c:

5c:ff:7d:45:fc:59:63:d4:8f:29:3c:0f:43:c9:b0:

6c:5b:8f:c4:06:23:97:a9:86:d2:5b:2b:4e:e8:bb:

bf:ef:5e:89:25:61:43:56:ef:d7:a5:99:26:bc:4f:

06:92:c8:91:8c:02:8d:31:35:9b:8a:03:5e:4b:de:

31:11:f9:ef:8c:7b:1c:de:ae:8c:83:b4:68:60:d9:

31:67:2d:48:79:ce:24:92:df:eb:56:44:b0:cb:2d:

50:f8:c1:ea:ca:91:b9:c6:78:15:61:c1:f9:c8:33:

9a:85:ae:d7:8e:22:50:5c:b6:15:4a:d0:ac:5d:7c:

37:cb:2f:9d:54:de:5b:97:1d:de:6d:01:2e:7d:29:

1f:27:d9:c6:be:42:c9:50:09:06:b5:7e:c6:eb:ce:

38:45:53:83:8e:91:9e:b0:44:fe:42:91:0a:5a:48:

2f:b5:46:c2:2d:94:b0:9e:91:4e:6d:b2:5f:59:a3:

3a:dc:a7:fb:b8:83:0e:97:9c:98:b9:62:54:d5:0c:

c5:5a:65:da:f5:62:7d:44:cb:09:86:5e:35:fb:1a:

b5:69:68:28:b5:b8:e3:ec:00:91:67:7d:b6:e9:cc:

94:be:88:c9:f8:94:3c:8e:f8:0c:ab:81:b6:86:b3:

ed:fe:32:a0:05:08:46:71:a0:0f:8f:03:6b:c7:40:

45:f2:9e:19:27:77:d2:48:63:50:c6:ea:91:10:4c:

3d:01:7e:5b:83:2f:f3:da:54:bd:27:d1:5e:25:76:

ac:ce:3a:a2:26:fc:09:4e:e2:7c:03:af:f4:2e:94:

d1:50:34:3e:f8:69:ff:6b:d2:81:49:d2:47:b6:13:

a5:3d:8b:ca:c3:08:24:0d:f7:ec:51:ec:b4:79:d0:

47:d6:9a:16:21:56:a7:4a:6a:8a:24:f0:15:d1:83:

d2:c8:97:d4:73:d1:c3:da:9d:fc:08:79:81:7e:a9:

58:49:51:26:db:29:8a:7c:85:b7:2a:86:87:10:8e:

bd:f8:ce:bf:fd:3e:27:6d:52:f9:1c:f5:bf:80:5e:

3e:25

A screen shot of a computer

AI-generated content may be incorrect.

prime1(p):

00:e2:3b:e5:e4:1a:bc:ca:e1:b9:db:a3:a5:de:7a:

3e:d1:fd:4e:f9:16:32:c5:db:5f:fb:79:0f:13:68:

3e:d1:e6:fa:b2:c1:62:0a:7b:bd:a8:bf:58:12:ea:

8b:2d:f5:21:cd:f2:85:43:e9:30:ff:38:04:27:04:

f4:fb:9e:6e:f6:ba:a3:d1:32:17:f7:9c:04:00:20:

15:06:ab:cb:f3:32:fc:cf:4e:3e:92:fb:33:74:ac:

cc:f6:35:7d:b1:1c:2d:85:ed:2c:84:2b:9f:78:e7:

9c:07:54:18:6a:c9:4f:1f:6e:73:1c:3f:dd:76:35:

db:f6:97:3b:af:ec:36:fd:49:8c:29:1d:eb:26:49:

b5:60:47:98:83:9f:db:28:85:0d:cb:9e:53:24:5c:

0f:41:fa:6c:0c:6a:45:72:a9:d6:a6:90:df:d5:4a:

58:ba:83:03:14:e1:ca:90:b0:f5:54:83:a2:60:19:

80:54:12:ab:84:65:e2:9c:df:1a:9e:be:38:10:13:

a0:ce:2d:df:c5:1f:14:eb:47:bf:81:71:f1:bd:13:

07:ac:4f:79:08:d9:46:b4:c9:94:7f:4a:cb:8b:ab:

ac:46:fd:5c:1d:00:b1:06:d3:4a:83:17:78:da:86:

b5:2a:ec:d0:22:c3:e7:a7:16:ab:5e:f8:e5:e1:0b:

49:93

A screen shot of a computer screen

AI-generated content may be incorrect.

prime2(q):

00:c0:ee:5f:25:d2:59:3e:41:97:67:d8:af:23:ee:

d7:dd:e6:96:fb:13:da:17:c8:17:3e:83:9c:ec:57:

b2:59:c1:ab:45:00:50:68:05:45:ef:1c:00:9f:0f:

d3:b9:61:0a:f1:6b:ee:47:aa:95:50:bc:6a:83:c1:

6b:42:ba:3c:c9:75:fe:e1:b1:06:02:ec:08:bb:a0:

02:d6:31:f8:2a:58:9b:c2:b6:e6:83:dc:b9:ef:15:

04:fc:fa:45:33:64:10:73:77:b2:cf:0b:0e:01:de:

ec:00:9d:c5:92:e8:ba:b7:8f:10:06:03:4c:d6:84:

fa:f4:49:47:5d:1a:61:81:01:3f:64:24:d8:07:ea:

da:23:d7:b1:f2:08:b7:29:a2:14:6a:fc:d6:b3:5b:

3a:a2:42:d2:f1:8e:2e:85:71:1e:91:fd:ac:a2:f7:

b8:6c:64:2e:b2:90:82:ae:22:cf:36:2e:97:e1:70:

4e:5b:e6:52:7b:77:7c:43:98:54:fd:99:7c:96:6a:

08:11:43:20:bb:e3:63:50:27:94:5b:01:18:60:dc:

36:75:64:91:19:25:1e:0f:e7:df:26:da:39:af:75:

5a:d2:cb:d6:6d:98:25:75:b2:0e:2e:09:b5:f8:1e:

90:31:37:97:8a:69:86:77:e3:54:9b:43:62:ba:40:

3b:7f

A screen shot of a computer code

AI-generated content may be incorrect.

exponent1(private exponent reduced modulo (p-1) for faster decryption using CRT):

00:8d:5c:ee:36:8d:7a:80:af:71:8a:4c:04:9e:32:

f6:c4:12:2b:61:bb:bc:38:23:ef:22:dc:af:4d:ea:

2a:ae:d0:4c:c0:9b:d3:de:47:19:e8:b2:bf:9e:fa:

4d:c3:86:d3:fb:b3:5a:10:68:4b:04:7f:05:21:38:

98:b8:0d:74:ba:d9:3e:f9:bd:fa:79:ef:54:14:9b:

f7:67:76:bb:f7:18:5a:1e:53:7f:08:2a:cd:29:4f:

bc:b6:f0:0f:bd:36:a5:3f:75:47:06:c3:97:5f:5e:

22:01:f6:4b:57:96:b8:c9:24:23:eb:78:00:b3:17:

ce:7d:94:5c:68:7e:0a:92:54:7d:af:47:91:a3:18:

15:ac:b6:b0:17:37:31:23:6d:98:84:2e:47:37:86:

0a:c6:a8:6b:11:8a:ea:20:4e:fd:e0:90:d0:3c:9f:

bb:37:b8:1b:99:d5:c8:d4:86:ae:95:83:b7:57:a3:

37:ab:d1:0a:b9:ad:4c:5f:c7:8d:03:ba:4a:9f:c9:

14:07:21:65:1c:f0:62:0a:ee:87:3c:a4:6d:70:3e:

ce:e1:9d:bb:3c:8b:40:02:41:9f:77:b6:cd:df:55:

83:4d:cc:8c:dd:56:8c:47:7e:89:a5:c6:69:ee:ea:

93:93:e1:eb:e0:7d:57:67:f1:e3:5d:71:db:7a:b6:

a9:df

A screen shot of a computer screen

AI-generated content may be incorrect.

exponent2(private exponent reduced modulo (q-1) for faster decryption using CRT):

00:b0:72:d2:2e:63:1d:1f:a5:19:75:ee:64:ef:b6:

27:53:58:eb:48:a2:35:5a:7e:b3:53:87:47:63:98:

29:13:91:de:b3:f2:bf:97:03:0b:9c:cd:bd:7b:bc:

1b:e5:75:6d:6e:b3:49:6f:de:01:45:9f:ac:c2:e7:

88:d3:b4:44:97:f4:04:b2:21:16:e0:61:42:f3:66:

3a:71:ef:ad:89:fd:14:27:96:e3:68:41:dd:03:5d:

f3:fb:f2:60:8b:c9:be:89:fc:35:5a:ca:3f:7b:52:

88:01:60:4a:2c:3c:11:58:83:cd:21:d2:ae:d9:9b:

31:71:6d:fb:88:98:f2:07:ec:3e:2f:b6:ca:a5:23:

13:72:a8:78:a4:65:78:2e:e9:7f:47:02:0a:d2:6a:

63:4b:b7:55:f9:7a:11:ee:15:30:e2:50:61:2d:82:

e5:f6:ac:01:51:6a:7d:3a:09:b7:fd:53:cb:b0:70:

e8:19:80:a2:7b:2d:22:47:27:f0:c3:27:37:1c:d1:

c8:a3:11:03:c5:13:07:e7:6c:eb:6f:f7:a6:76:1f:

b0:e6:d8:9d:23:a4:20:c4:67:4a:5d:dc:43:d9:c6:

b8:d4:05:7d:0d:2a:93:47:fb:1a:a0:dc:5c:c2:9a:

21:42:02:17:e4:8c:f2:60:7f:57:07:d1:2f:60:2c:

12:bd

A screen shot of a computer code

AI-generated content may be incorrect.

Coefficient(The modular inverse of q modulo p, used in CRT):

73:db:27:74:d9:df:9b:aa:5c:2d:12:7e:c7:c6:8a:

19:b3:79:c8:cb:22:21:e4:00:e6:87:d3:8a:3a:89:

96:e3:fb:f9:3e:94:82:97:80:46:e9:bf:b5:0e:e0:

86:ec:61:c0:ab:2d:4d:ab:09:a6:6a:cd:e0:8d:32:

bd:de:6b:8b:1d:ca:5c:66:16:ff:b1:c2:50:9c:33:

c3:c2:61:03:9f:4d:8d:da:92:a3:a6:25:d1:31:4e:

b9:5b:10:d1:f9:a9:6f:40:0a:55:1a:72:1d:20:99:

21:38:2a:c5:52:92:a2:7b:70:27:f7:c4:b3:25:2c:

1a:25:14:a9:67:c4:94:88:55:ce:60:b9:c8:77:10:

bc:5d:e7:5d:72:09:c3:34:11:52:35:02:14:93:9a:

2a:b8:aa:ce:59:1b:17:b8:32:c1:e6:b4:7b:56:98:

9a:9d:8f:4a:8c:dd:fb:ae:30:64:5b:5d:9d:1f:54:

b7:73:e1:ce:2e:d2:64:c0:3a:41:0d:89:81:a0:86:

9b:12:96:14:7e:c7:25:b2:b2:56:1b:4c:b8:56:dc:

4f:69:4b:9b:13:a1:61:08:00:b9:4f:ef:f5:60:c1:

cf:b1:3f:3e:d5:83:23:09:ed:6b:29:6e:a6:2e:79:

59:bc:1b:78:ed:47:13:1c:51:e8:97:95:27:b3:ba:

d7

A screenshot of a computer screen

AI-generated content may be incorrect.

**Task 2: Generating a Certificate Request for Your Web Server**

We created csr of our domian i.e. www.saif2025.com

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Task 3: Generating a Certificate for your server**

Then we created a signed certificate for our domain that is verified by CA we created in task 1.

A screenshot of a computer

AI-generated content may be incorrect.

The CA=False tells it is not a Certificate Authority’s Certificate. The different subject key and Authority key indicates it is not a self signed certificate.

A screenshot of a computer

AI-generated content may be incorrect.

**Task 4: Deploying Certificate in an Apache-Based HTTPS Website**

We created a new folder and placed html files in there.

A screen shot of a computer

AI-generated content may be incorrect.

Then we updated the /etc/apache2/sites-available/bank32\_apache\_ssl.conf

A screen shot of a computer

AI-generated content may be incorrect.

Then we enabled the ssl certificate and started apcahe2 server.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

We can easily access the http site.

A screen shot of a computer

AI-generated content may be incorrect.

But when we accessed the https domain our server raised the security warning. Because the certificate is not signed by a well known CA authority whose certificate is not publicly available. So due to inavailablity of CA certificate the browser was unable to verify the certificate of our domain and raised a security warning.

A screenshot of a computer

AI-generated content may be incorrect.

To resolve this issue, we manually add the certificate of our CA in authorities of our browser. We copied the CA certificate to our host VM with the help of shared Folder.

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

We added the certificate in about:preferences#privacy.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Then we visited the website with https it succeeded without any security warning.

A green screen with white text

AI-generated content may be incorrect.

**Task 5: Launching a Man-In-The-Middle Attack**

**Step 1: Setting up the malicious website.**

In this step we setup a malicious spoofed website to trick users to visit our malicious webpage when it tries to access a legitmate webiste.

For this we created a dummy website im MITM folder.

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Then we updated the configuration file of apache2 to host a website for www.tesla.com hostname and used the prevoiusly created certificates of [www.saif2025.com](http://www.saif2025.com) .

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2: Becoming the man in the middle**

For redirection, we have to launch a successful dns posioning attack .In this task we simulated this attack by just adding entry in /etc/hosts file

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3: Browse the target website.**

When we browsed the site the victim landed to our webpages but the browser raised a security warning because domain name in the the offered certificate is different from the domain name in request. So browser doesnot allow this kind of connections and raises security warning.

A screenshot of a computer

AI-generated content may be incorrect.

**Task 6: Launching a Man-In-The-Middle Attack with a Compromised CA**

To reslove the above issue, we need to compromise the CA.In next phase we consider that CA is compromised ie private key of CA is stolen. So we created a spoofed certificate for [www.tesla.com](http://www.tesla.com) with that compromised key.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

We changed the certifcate path to use the newly created certificate.

A screenshot of a computer

AI-generated content may be incorrect.Then we again tested the website access through browser and this time we successfully landed to spoofed webpages wirhout any security warning because now the domain name difference was not present.

A green screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Important Note:**

Please revert any changes made in host VM so that these changes are not permanent.