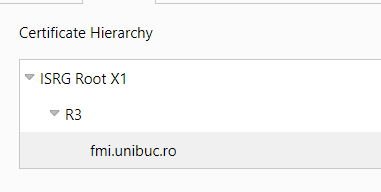
Lab 11

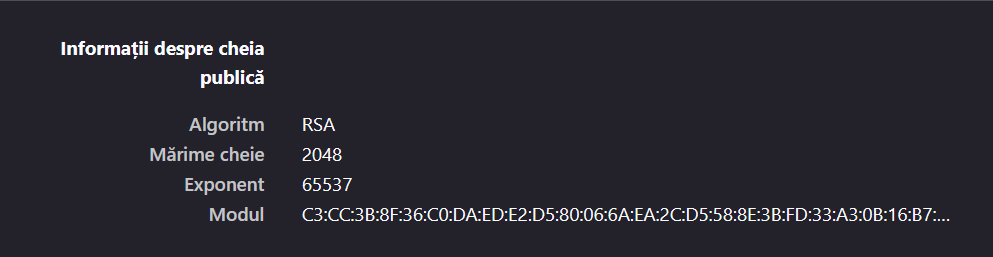
1A)

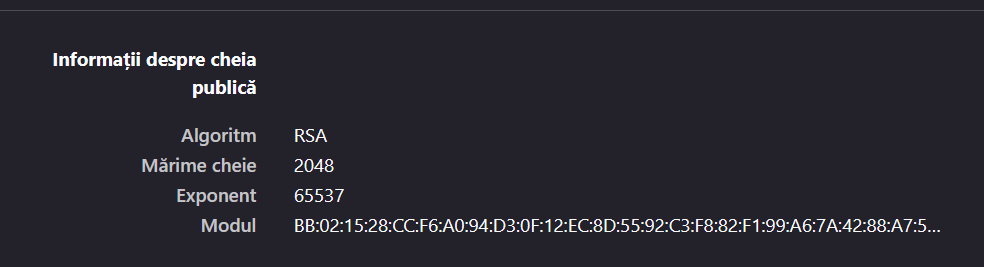


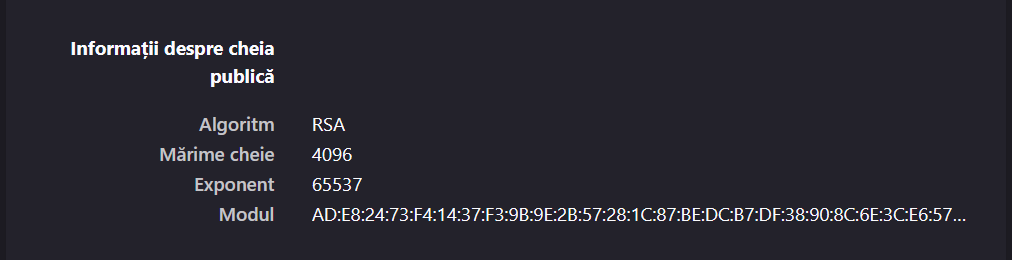
B) 10/24/23, 5:37:11 PM GMT+3

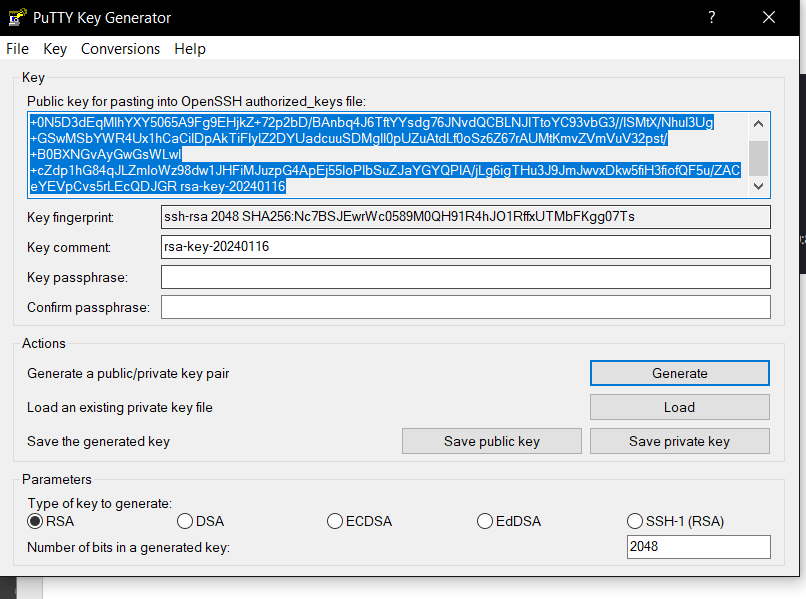
1/22/24, 4:37:10 PM GMT+2

C) 

D) 



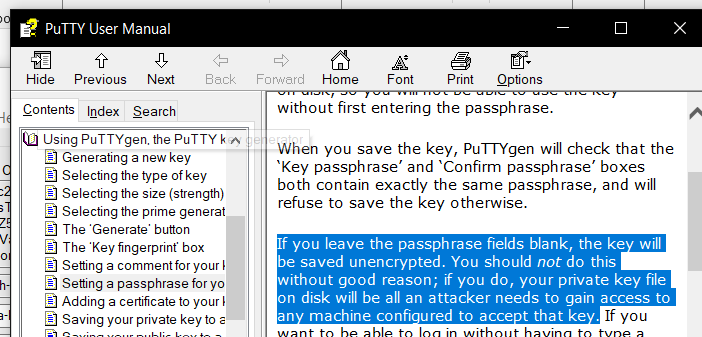


2. 

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCnzV8uzzDxncMOKbmuwVUA01bDxTGInhs+0N5D3dEqMIhYXY5065A9Fg9EHjkZ+72p2bD/BAnbq4J6TftYYsdg76JNvdQCBLNJITtoYC93vbG3//lSMtX/NhuI3Ug+GSwMSbYWR4Ux1hCaCiIDpAkTiFIyIZ2DYUadcuuSDMglI0pUZuAtdLf0oSz6Z67rAUMtKmvZVmVuV32pst/+B0BXNGvAyGwGsWLwl+cZdp1hG84qJLZmIoWz98dw1JHFiMJuzpG4ApEj55loPIbSuZJaYGYQPlA/jLg6igTHu3J9JmJwvxDkw5fiH3fiofQF5u/ZACeYEVpCvs5rLEcQDJGR rsa-key-20240116

c) cripteaza cheile

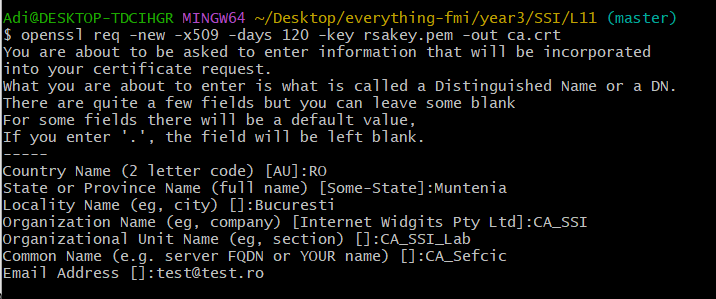
If you leave the passphrase fields blank, the key will be saved unencrypted. You should not do this without good reason; if you do, your private key file on disk will be all an attacker needs to gain access to any machine configured to accept that key.



2.

openssl genrsa -out rsakey.key 2048

openssl req -new -x509 -days 120 -key rsakey.pem -out ca.crt



Certificate:

Data:

Version: 3 (0x2)

Serial Number:

32:16:bc:51:96:55:60:6c:94:40:46:28:4a:1b:20:d6:0f:44:02:e1

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RO, ST = Muntenia, L = Bucuresti, O = CA\_SSI, OU = CA\_SSI\_Lab, CN = CA\_Sefcic, emailAddress = test@test.ro

Validity

Not Before: Jan 16 21:59:15 2024 GMT

Not After : May 15 21:59:15 2024 GMT

Subject: C = RO, ST = Muntenia, L = Bucuresti, O = CA\_SSI, OU = CA\_SSI\_Lab, CN = CA\_Sefcic, emailAddress = test@test.ro

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:ce:2e:b2:24:14:58:dd:3d:24:93:70:05:39:01:

bf:d5:51:d2:6e:a0:df:39:30:3c:f6:7d:fc:0d:51:

eb:b8:29:94:19:1b:67:94:d6:3b:39:3b:a3:a5:34:

90:2e:34:f5:2d:9c:a1:99:60:ac:fa:76:e9:21:eb:

09:d6:2f:d8:d7:c6:ee:94:5a:a8:5f:7f:ec:92:a0:

ae:6b:55:09:7a:bd:be:70:bd:2a:1a:59:8c:c6:42:

b0:c0:89:f9:b2:be:17:17:76:35:43:74:9c:3f:f4:

ad:9c:6a:1c:b3:76:f5:9b:93:f4:c1:df:8c:fb:35:

23:90:aa:3f:1e:30:0b:10:5d:e6:b1:6d:27:14:9f:

fc:18:bf:66:47:a7:ae:dc:df:a1:0b:09:88:f4:7d:

84:24:6c:6a:46:5c:12:24:c1:3c:1e:dc:8f:01:99:

2f:f9:a7:eb:71:f6:e5:46:d0:46:ef:16:f4:b5:41:

91:97:b3:be:e2:bd:51:05:28:89:c1:7a:f5:b7:a0:

8d:10:06:fe:98:f9:b5:75:fe:5f:a5:de:66:c8:51:

d5:0a:87:f0:5c:e7:8a:ee:a8:07:29:ab:32:46:71:

e8:63:aa:56:cb:dd:b1:d0:98:3e:ef:e3:4b:33:d5:

06:f9:91:81:93:9d:e3:4e:28:a0:9b:41:0e:d6:e5:

61:0f

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

72:81:08:5E:AD:9C:49:E5:52:7E:85:4F:13:EB:A1:6C:EC:D2:D6:7E

X509v3 Authority Key Identifier:

keyid:72:81:08:5E:AD:9C:49:E5:52:7E:85:4F:13:EB:A1:6C:EC:D2:D6:7E

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha256WithRSAEncryption

cb:dc:cb:1b:d8:41:76:04:40:17:28:d7:d8:2f:7a:f2:14:7b:

08:93:11:17:7e:65:85:22:10:ba:9b:14:a6:e7:52:c1:b8:c8:

ce:26:93:2e:a5:21:46:bd:c4:5e:33:fd:87:bc:ee:d5:12:54:

f6:94:41:7e:fc:11:ed:59:28:0a:02:06:66:43:93:5a:73:a7:

8e:5f:eb:a2:92:8e:eb:2c:80:e4:fc:d4:6b:05:af:6c:d9:54:

86:d8:b2:93:74:20:ca:4d:69:23:8c:b4:7a:16:ee:0f:73:f6:

c3:69:d5:59:22:12:dd:0b:b4:c7:46:02:e4:2f:35:3c:7f:fe:

16:c7:fe:cd:a3:fe:04:6a:ca:d4:56:c4:88:8d:74:c0:f3:05:

85:e1:82:94:a4:7a:89:f3:62:58:06:ed:c0:5e:18:66:44:b8:

78:bb:76:e8:f9:3d:89:da:b1:49:90:2f:36:15:ca:1e:9e:1d:

4a:38:8c:4b:16:49:76:16:fa:39:a5:76:da:cc:db:43:a8:f7:

15:94:80:af:2f:09:01:d6:2a:ef:24:6b:19:08:4f:30:d4:e7:

67:a8:c4:34:a1:25:07:8e:e2:0f:d2:31:7c:32:5f:dd:86:56:

2a:64:c5:bc:b8:ef:c9:98:e8:08:f7:cd:9d:93:52:c9:84:6a:

96:72:49:8e

openssl req -new -key sub.key -out sub.csr

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]:RO

State or Province Name (full name) [Some-State]:Muntenia

Locality Name (eg, city) []:Bucuresti

Organization Name (eg, company) [Internet Widgits Pty Ltd]:SUB\_SSI

Organizational Unit Name (eg, section) []:SUB\_Sefcic

Common Name (e.g. server FQDN or YOUR name) []:test\_sub@test.ro

Email Address []:amgresitscuze

openssl x509 -req -days 60 -in sub.csr -CA ca.crt -CAkey rsakey.pem -set\_serial 1 -out sub.crt

Signature ok

subject=C = RO, ST = Muntenia, L = Bucuresti, O = SUB\_SSI, OU = SUB\_Sefcic, CN = test\_sub@test.ro, emailAddress = amgresitscuze

Getting CA Private Key

openssl x509 -text -noout -in sub.crt

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 1 (0x1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RO, ST = Muntenia, L = Bucuresti, O = CA\_SSI, OU = CA\_SSI\_Lab, CN = CA\_Sefcic, emailAddress = test@test.ro

Validity

Not Before: Jan 16 22:16:36 2024 GMT

Not After : Mar 16 22:16:36 2024 GMT

Subject: C = RO, ST = Muntenia, L = Bucuresti, O = SUB\_SSI, OU = SUB\_Sefcic, CN = test\_sub@test.ro, emailAddress = amgresitscuze

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:9a:e1:bb:65:8c:31:e6:0f:1b:cf:58:19:27:57:

dd:8e:ba:d9:cd:b7:e5:8a:70:91:fd:74:5c:a0:39:

d2:fe:db:bf:e6:39:ef:15:f0:5a:41:25:8e:ee:04:

73:14:22:f2:53:e0:7d:2c:cc:44:0f:d8:24:b9:68:

ae:df:61:42:10:71:26:3a:53:05:d7:65:c9:b6:22:

08:79:8c:77:46:6f:a5:eb:6c:76:f0:31:7e:2c:43:

fe:86:6a:94:d2:29:17:0b:a7:cb:bb:fc:bd:2c:d3:

c0:c7:ce:d4:17:eb:0a:a2:d6:dd:88:5e:42:10:07:

25:9d:95:46:2a:e6:f1:0d:5e:ff:be:0f:ea:49:b3:

cb:9d:b1:26:34:25:c7:05:46:90:35:70:78:6e:e2:

b7:48:f5:54:70:5f:17:65:57:aa:d3:67:17:74:88:

41:af:8f:d2:32:72:cf:f2:4a:d1:94:1d:f5:bb:fc:

8c:f6:d7:ed:fc:37:89:0c:f6:f2:b8:40:19:95:17:

97:c5:03:84:e1:9b:17:05:b8:d2:1b:74:fa:05:8f:

06:08:dc:54:97:62:d8:a4:b1:43:eb:7d:14:5f:03:

36:56:a5:b5:c2:d7:d4:4f:af:75:e4:ae:d9:16:a3:

28:b4:dd:ae:1e:ba:0e:55:80:67:19:5f:47:90:6d:

f1:09

Exponent: 65537 (0x10001)

Signature Algorithm: sha256WithRSAEncryption

66:ba:ea:ee:8d:ef:9d:be:5a:03:4d:95:dc:ba:9a:ef:7c:8c:

58:27:d0:e1:6d:ca:8a:f3:fd:71:10:2b:04:05:69:ec:cc:ba:

ca:d4:29:46:35:5d:41:20:ce:78:a2:b6:cc:89:a9:c3:5b:62:

f6:b0:2f:a5:8c:db:15:48:cc:75:4e:26:14:86:ba:a8:90:06:

39:7c:f3:c8:cf:ff:46:67:b4:cb:53:81:49:76:fc:0f:0d:38:

dc:8a:0c:d8:75:75:90:a3:55:61:87:b0:1b:06:fb:8d:19:3e:

a7:43:b6:2b:c9:be:00:0e:13:59:54:04:62:e8:52:a9:85:fd:

47:89:45:dd:23:37:0d:47:29:33:50:0e:96:72:1c:06:e9:27:

39:4f:68:f4:30:7a:87:67:1d:0a:1f:6f:55:04:3e:ba:60:59:

e3:08:d3:d9:cf:72:60:4e:53:10:f5:71:ac:45:15:4a:50:05:

97:03:2a:db:0e:55:21:2a:a5:af:29:86:78:64:7c:df:53:17:

26:33:b3:70:50:c2:dc:41:e9:b9:6e:45:4d:4a:2c:6e:34:39:

57:00:fc:8c:98:ff:31:d6:4f:a5:5e:58:bc:d9:2b:76:12:38:

16:f1:59:6f:51:3e:e4:21:8c:6c:03:63:06:9c:b5:46:6e:1f:

ab:d2:a9:47