Lab 1 : Public Key Infrastructure

Due : July 15, 2024 at 11:59 PM | Total points: 110

Task 1 (20 Pts): Becoming a Certificate Authority

- Provide screenshot of the CA certificate and the key along with the operations you performed.

CA Certificate:

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7b:fd:33:3d:7a:65:68:dc:17:aa:45:f6:d1:87:3f:fb:c0:bf:46:be
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Jul 15 06:22:29 2024 GMT
            Not After : Jul 13 06:22:29 2034 GMT
        Subject: C = US, ST = California, O = Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:a9:e2:ea:ee:d1:f1:89:e4:0d:42:be:f1:9a:37:
                    c9:91:da:bc:2c:e8:03:f9:91:4a:90:bf:38:cc:72:
                    9d:70:98:e3:4e:05:0e:fb:85:04:31:1d:02:57:41:
                    5d:89:52:96:ff:51:bf:10:78:86:2a:0f:17:8b:e1:
                    47:ac:06:6d:03:a3:7c:3d:d9:78:a7:12:4b:90:b8:
                    cb:be:ec:b5:c7:d0:f4:78:c2:11:e6:dc:76:4f:c4:
                    c1:a0:68:c7:a2:2a:8b:20:23:1f:8a:24:33:41:6d:
                    55:a7:50:e1:b0:c8:00:02:bf:db:39:6a:48:84:77:
                    b9:a4:63:4d:cc:2b:c8:89:af:64:40:cc:59:9e:8d:
                    92:65:b1:39:56:63:b2:e5:15:bd:05:3e:5b:56:79:
                    82:71:93:a2:e7:33:9c:da:6b:58:ac:23:66:50:9c:
                    d4:99:fb:93:a3:fa:ef:47:ab:cd:f2:ce:6d:8d:52:
                    f3:f5:54:31:8a:89:7d:ec:a6:41:93:fb:1e:e0:8f:
                    2e:3f:e1:1a:65:c5:db:22:8e:4f:ec:b5:af:6d:5d:
                    65:c8:da:25:7b:b2:14:11:41:2a:96:b3:7c:9b:47:
                    e7:db:9c:bb:e4:bd:e8:37:96:47:b9:40:c5:af:e4:
                    dc:05:70:2d:16:8f:6c:4f:92:1d:ca:35:e0:7a:f8:
                    cc:6d:78:40:9f:bb:bd:1d:be:16:9a:a1:36:69:83:
                    5b:8c:bd:d8:68:cb:7a:ac:b5:46:b6:da:ba:30:25:
                    b9:36:d6:50:9a:37:db:4a:ab:18:8d:b3:72:33:62:
                    82:38:e4:fb:5a:38:16:6c:ba:43:4b:9b:29:73:ab:
                    47:06:1a:32:0b:5e:f2:27:63:97:e9:0c:70:71:ef:
                    6b:99:a6:31:6e:bf:e9:1a:1e:d2:b4:eb:bf:a7:3f:
                    fa:a0:52:ef:31:f7:68:4b:74:14:61:98:5a:31:45:
                    38:0b:1f:7c:ae:41:30:69:c8:e5:0c:38:d5:60:47:
                    2b:b5:d4:4a:97:01:4c:1e:85:c7:4d:bd:d8:0d:1b:
                    bc:98:8c:39:4b:5b:f4:d3:ae:07:2f:f9:fe:1f:e7:
                    26:e5:3a:68:70:0d:92:e4:f4:d8:47:48:f3:ec:b2:
                    7a:73:0a:a5:49:c2:34:b6:d7:0b:be:c2:29:ce:51:
                    5f:1b:d5:89:79:b2:24:f4:c7:9e:e5:66:32:e4:fb:
                    a3:0c:99:fd:57:b1:21:e4:aa:c2:5f:17:1d:13:5a:
                    c3:d5:5c:4e:a1:6c:1e:b3:37:50:c8:93:03:35:c0:
                    c9:47:92:41:e5:61:a1:26:14:ec:ed:ce:51:c6:36:
                    b2:a1:a8:16:48:f8:db:94:0e:8c:13:d8:27:8e:ea:
                    85:32:ed
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B
            X509v3 Authority Key Identifier:
                keyid:7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         25:13:3e:46:c5:8e:59:1a:57:0a:70:21:a1:69:8e:da:42:02:
         c9:99:02:93:df:98:d1:07:3b:8f:67:6f:86:69:9e:04:fd:62:
         4c:68:5d:90:56:c6:c9:19:90:ee:62:25:26:97:60:80:1b:96:
         d7:f6:5c:4b:83:e0:ec:c9:04:fa:8f:18:30:46:1a:12:38:f1:
         c6:43:86:8a:2c:14:68:1d:b0:a2:fc:fa:33:5b:63:63:bb:e3:
         0b:18:85:a4:b2:aa:92:80:e0:ac:a2:48:4d:cd:c5:ce:23:43:
         e7:3e:8a:c5:65:b7:8f:ab:4b:9c:77:45:e4:8f:0e:69:88:d5:
         a2:b1:70:3d:61:15:82:c8:b4:59:ae:b4:53:b9:de:40:01:29:
         3b:e7:a4:e5:73:6b:93:97:bc:4d:03:ca:48:e7:c0:e7:73:87:
         d1:fe:b8:2a:45:48:9e:99:c8:86:4f:fa:6b:55:ba:35:7a:62:
         98:1d:0b:19:04:01:06:57:4b:bd:5a:b8:b9:ff:c2:cb:b3:35:
         1d:a8:ab:11:eb:30:d1:de:44:91:31:39:bb:a8:47:af:06:f0:
         55:8f:a6:98:e9:99:2d:2f:da:14:04:3a:41:e2:dd:8c:4f:0b:
         7d:3e:6c:75:8a:24:aa:01:6e:72:0b:33:8e:68:21:e6:30:5e:
         a0:8f:75:bf:df:8b:f5:74:a3:7d:86:14:b2:11:ff:00:17:6f:
         f7:7d:1e:59:9d:b1:d1:ec:17:6a:9d:c0:b8:da:58:0a:a2:63:
         02:eb:56:d3:18:1d:1c:4f:9f:87:a4:89:f3:ee:fb:08:b0:0b:
         e6:3c:6f:d5:74:db:77:22:c2:7a:dd:d4:33:27:98:34:1d:2a:
         0a:25:3b:bb:30:4f:54:54:8b:9b:93:57:b5:dd:00:a8:66:2f:
         d3:dd:02:da:26:03:88:8c:71:bb:8d:b6:7b:01:99:39:63:1b:
         22:07:17:a5:4a:51:42:6a:23:e3:3c:9d:6e:06:7b:33:5a:9d:
         4a:09:be:6b:31:f4:f9:26:ec:03:0a:e8:51:bc:0d:2c:4b:c5:
         07:a2:40:e6:0d:2c:13:c8:37:d8:34:7a:ba:1f:1a:af:df:5d:
         bf:4d:f5:88:22:7d:3a:26:62:a6:03:46:c7:f7:cd:fb:ae:d8:
         39:b0:0d:7b:59:75:fd:1e:29:f3:6a:e4:3d:f7:6b:6e:ce:54:
         50:d7:32:ad:c8:e7:23:75:e4:3c:35:77:f0:f1:e5:8d:90:d7:
         bc:2f:1c:eb:4d:97:fd:6c:1b:e2:2a:d6:a7:32:50:4b:39:1c:
         2f:43:6a:f2:53:b7:65:01:6f:95:3f:1b:ff:b3:3e:98:e7:cc:
         34:f2:fb:ec:3f:d3:db:4d
```

CA Key:

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:a9:e2:ea:ee:d1:f1:89:e4:0d:42:be:f1:9a:37:
    c9:91:da:bc:2c:e8:03:f9:91:4a:90:bf:38:cc:72:
    9d:70:98:e3:4e:05:0e:fb:85:04:31:1d:02:57:41:
    5d:89:52:96:ff:51:bf:10:78:86:2a:0f:17:8b:e1:
    47:ac:06:6d:03:a3:7c:3d:d9:78:a7:12:4b:90:b8:
    cb:be:ec:b5:c7:d0:f4:78:c2:11:e6:dc:76:4f:c4:
    c1:a0:68:c7:a2:2a:8b:20:23:1f:8a:24:33:41:6d:
    55:a7:50:e1:b0:c8:00:02:bf:db:39:6a:48:84:77:
    b9:a4:63:4d:cc:2b:c8:89:af:64:40:cc:59:9e:8d:
    92:65:b1:39:56:63:b2:e5:15:bd:05:3e:5b:56:79:
    82:71:93:a2:e7:33:9c:da:6b:58:ac:23:66:50:9c:
    d4:99:fb:93:a3:fa:ef:47:ab:cd:f2:ce:6d:8d:52:
    f3:f5:54:31:8a:89:7d:ec:a6:41:93:fb:1e:e0:8f:
    2e:3f:e1:1a:65:c5:db:22:8e:4f:ec:b5:af:6d:5d:
    65:c8:da:25:7b:b2:14:11:41:2a:96:b3:7c:9b:47:
    e7:db:9c:bb:e4:bd:e8:37:96:47:b9:40:c5:af:e4:
    dc:05:70:2d:16:8f:6c:4f:92:1d:ca:35:e0:7a:f8:
    cc:6d:78:40:9f:bb:bd:1d:be:16:9a:a1:36:69:83:
    5b:8c:bd:d8:68:cb:7a:ac:b5:46:b6:da:ba:30:25:
    b9:36:d6:50:9a:37:db:4a:ab:18:8d:b3:72:33:62:
    82:38:e4:fb:5a:38:16:6c:ba:43:4b:9b:29:73:ab:
    47:06:1a:32:0b:5e:f2:27:63:97:e9:0c:70:71:ef:
    6b:99:a6:31:6e:bf:e9:1a:1e:d2:b4:eb:bf:a7:3f:
    fa:a0:52:ef:31:f7:68:4b:74:14:61:98:5a:31:45:
    38:0b:1f:7c:ae:41:30:69:c8:e5:0c:38:d5:60:47:
    2b:b5:d4:4a:97:01:4c:1e:85:c7:4d:bd:d8:0d:1b:
    bc:98:8c:39:4b:5b:f4:d3:ae:07:2f:f9:fe:1f:e7:
    26:e5:3a:68:70:0d:92:e4:f4:d8:47:48:f3:ec:b2:
    7a:73:0a:a5:49:c2:34:b6:d7:0b:be:c2:29:ce:51:
    5f:1b:d5:89:79:b2:24:f4:c7:9e:e5:66:32:e4:fb:
    a3:0c:99:fd:57:b1:21:e4:aa:c2:5f:17:1d:13:5a:
    c3:d5:5c:4e:a1:6c:1e:b3:37:50:c8:93:03:35:c0:
    c9:47:92:41:e5:61:a1:26:14:ec:ed:ce:51:c6:36:
    b2:a1:a8:16:48:f8:db:94:0e:8c:13:d8:27:8e:ea:
    85:32:ed
publicExponent: 65537 (0x10001)
privateExponent:
    00:a8:b2:52:44:30:69:bf:59:9b:e9:69:9e:94:5b:
    4d:67:ee:62:e9:dc:c3:05:b1:c6:ef:91:53:1f:81:
    b8:e1:34:90:92:ca:e7:23:cf:e4:67:b8:bc:b8:54:
    8a:43:70:a5:cc:87:2a:49:7a:c5:0f:42:c9:48:f7:
    bd:aa:0e:ff:75:9b:84:26:0e:ab:86:8b:de:49:a9:
    97:78:d1:a9:78:ef:ff:b3:62:53:50:82:1f:61:fa:
    a9:a3:56:28:d6:d9:94:29:a7:77:0c:40:02:3d:b8:
    0a:54:09:36:f3:ca:c6:67:f4:88:06:ad:89:b1:31:
    0a:41:38:f2:ea:09:98:2b:50:e5:26:8b:45:7a:f2:
    6e:2b:59:1e:ec:b0:37:d6:d0:0d:51:05:a8:c1:68:
    0b:a6:28:ca:9c:f7:5d:8c:6f:08:30:77:3e:84:52:
    17:b3:88:64:05:73:8a:e4:0a:b0:89:a9:7e:93:d5:
    89:b7:55:91:94:56:0f:9b:4d:44:d5:63:8a:37:c7:
    36:4f:ec:81:c0:0a:07:1e:7b:5e:d6:59:5c:08:27:
    b4:89:0c:46:28:5c:9f:1c:bb:2f:45:52:9a:2b:bf:
    ed:76:e0:5e:9c:38:10:3e:12:96:ca:58:8d:75:aa:
    b6:e9:17:89:4e:5b:c1:5c:0a:66:56:83:c5:93:97:
    37:b6:e6:5a:15:85:d3:5e:ae:ef:c7:47:ef:68:59:
    c5:6f:f3:d6:79:37:7b:99:bf:f0:73:36:b6:47:05:
    11:ce:10:3d:79:83:57:53:30:d2:60:5d:77:b6:01:
    35:15:0a:4a:a1:52:b1:5c:b8:9e:a5:8a:69:0c:fa:
    c6:83:f0:77:e8:ce:fb:b6:df:32:8a:b3:4c:a8:e5:
    18:36:14:6c:e6:97:65:9f:8e:8e:21:ed:08:0a:c3:
    09:b5:ce:e7:57:44:6e:90:20:40:e9:e5:fe:cc:7b:
    c0:a5:42:8c:76:66:69:d8:f3:4d:8c:3f:34:0c:eb:
    69:ca:85:db:dd:56:34:62:10:69:fa:33:8c:10:a9:
    c2:2c:a6:5a:67:5c:d8:60:d2:b2:02:b1:bc:f0:57:
    49:a5:7c:64:6e:e1:54:75:17:bb:dc:68:12:db:7e:
    9f:a5:67:fa:2b:a4:31:50:df:ae:0b:72:70:14:fc:
    1d:98:29:3e:65:c8:74:9f:e5:eb:f5:7a:83:fa:52:
    ae:d8:24:ca:9f:02:9c:9a:c0:ef:42:d3:3f:41:de:
    b5:ce:4b:dd:6b:4a:7e:64:0e:6a:c2:15:c2:43:33:
    af:86:11:7b:9c:18:7f:04:fb:41:27:6f:64:93:cd:
    b4:76:91:05:b8:c3:bb:00:15:16:60:f6:46:96:38:
    9f:bf:01
prime1:
    00:d6:7b:6c:77:30:cf:28:53:2f:06:c6:ad:98:f4:
    12:64:18:09:a0:17:61:d3:99:11:25:8f:2b:d2:d7:
    d7:a6:28:d7:af:1f:89:41:86:86:a0:14:80:c2:ec:
    c0:3d:af:2e:52:fa:7b:17:3f:a1:69:ca:ed:0f:2e:
    8b:bb:ce:b1:b6:21:be:6a:23:2d:72:42:76:a4:4a:
    05:8b:87:5d:e8:dd:a0:69:d0:68:f3:0d:30:4a:9e:
    01:3b:d1:07:0f:e2:08:9f:2d:86:8a:53:fe:4b:61:
    11:57:a4:16:86:16:9b:58:09:ce:91:72:eb:24:1e:
    62:89:c2:19:38:15:3e:45:5e:77:47:36:c5:84:56:
    7d:27:b7:4b:36:3f:99:8d:13:4e:92:fe:0b:5b:05:
    3b:22:7f:f8:13:98:58:e4:06:6d:e6:91:88:76:99:
    7e:52:7c:96:7c:d7:76:f9:06:6d:5e:5c:01:46:fc:
    6f:10:71:51:82:d5:d4:71:7e:24:6e:5d:a9:71:af:
    a4:36:fb:b9:b1:52:b9:fe:c5:e9:8d:ee:44:14:9b:
    45:33:b7:3e:71:51:bd:f8:8c:b6:ba:ad:59:76:d2:
    41:cb:e9:d4:ef:2b:84:63:90:6f:3d:e1:65:b3:eb:
    c1:9f:5e:92:2b:d1:57:20:54:1d:8a:38:06:dd:bc:
    dd:e1
prime2:
    00:ca:c5:92:0e:38:37:a2:65:8f:76:e1:6f:0b:b3:
    42:34:06:73:7d:c9:e5:36:3e:be:23:b7:4d:92:94:
    82:8b:5d:66:bf:b5:45:47:57:38:ae:44:c0:85:87:
    c5:e6:1e:e5:47:73:32:52:c2:b7:d6:b9:c4:74:ea:
    e4:18:8e:91:b4:30:3c:8f:15:02:73:16:af:6b:a2:
    9f:cc:f4:0e:32:04:03:67:2d:5c:89:2a:f6:be:e6:
    b7:4d:d2:e4:0f:01:0f:f9:18:91:d8:23:18:31:5f:
    32:7a:15:c0:32:9f:64:11:65:f6:48:f3:35:fc:9b:
    d6:51:4c:34:bc:74:53:ec:8e:c7:ba:be:e0:54:d6:
    2f:7f:f4:0c:78:81:9e:20:c8:be:d7:6b:92:c7:be:
    53:99:1f:b9:8f:8c:cd:4d:57:2b:c3:d5:78:8c:be:
    7d:06:65:17:b2:ab:d9:6b:bd:f2:93:b1:f3:cb:85:
    a1:07:3f:f4:5b:bc:33:1f:30:9b:ef:1a:28:02:59:
    a4:76:da:5b:f6:6e:c6:db:e0:1f:13:ff:12:c0:ea:
    82:21:d3:91:7e:1a:2e:db:06:d0:c1:5e:6c:a6:49:
    77:84:d5:2e:b6:80:3f:34:e3:ab:b6:aa:c1:c2:7a:
    93:41:df:ae:84:c5:2d:90:a4:15:b1:6f:ff:63:12:
    be:8d
```

```
exponent1:
    49:93:99:87:e1:d4:8e:ce:ca:69:16:aa:e2:b7:87:
    bf:92:87:6a:c5:da:a7:4d:f1:15:e3:61:73:38:dc:
    1f:82:0f:4b:62:14:21:c8:56:52:7f:f6:13:e8:47:
    a2:61:80:10:b3:20:9a:bf:17:4e:45:70:c1:2e:84:
    7c:ee:d1:03:db:db:88:69:7c:e3:9f:6d:37:ba:b4:
    e0:42:95:b2:96:a4:ba:e7:e5:b8:cb:23:6f:d5:78:
    32:de:e7:ff:48:d9:10:51:fb:bf:64:44:ed:f2:e4:
    92:1e:16:23:f5:89:60:d0:2c:6e:b4:ef:79:3a:7b:
    2f:2a:c8:9f:f6:99:a0:0e:61:f8:aa:0f:63:f0:8f:
    8a:9a:54:50:cd:cc:8d:1a:bc:6f:ac:7a:94:c4:dc:
    9e:5f:2b:e8:fc:f0:31:79:0b:26:77:72:4a:cd:29:
    0a:7e:f6:d8:e8:c9:45:70:31:00:97:ab:50:80:b4:
    50:fd:ae:aa:a5:53:f5:83:02:58:62:05:08:9c:ea:
    46:7a:60:1f:36:73:db:b4:65:04:6d:62:29:77:82:
    6b:d5:46:b4:75:08:28:45:8d:41:c8:c9:d1:fb:1a:
    db:2a:e2:03:11:f8:9e:77:23:d2:24:8a:51:08:65:
    29:98:b5:a8:16:6e:3f:06:dc:03:58:68:f2:94:21:
    c1
```

```
exponent2:
    00:8d:7c:58:52:65:b5:a4:32:1b:6d:c7:15:35:e3:
    c9:e1:05:53:56:c5:26:93:b8:29:f2:3f:f7:f7:bc:
    7a:6e:86:28:a8:c1:f2:6a:3a:19:09:b8:5d:61:8f:
    00:6e:76:c6:63:19:a5:56:8c:19:bc:d1:78:9c:60:
    3d:f2:48:a0:b0:4b:2c:26:66:71:84:1e:a3:1e:86:
    a5:dc:5b:ba:ff:f9:3e:ea:a2:83:3c:0e:e7:87:02:
    f3:8a:71:09:c2:d2:69:f3:d4:ca:07:37:4d:ad:3d:
    90:ba:11:2d:3f:e5:69:ec:9d:e9:c0:b3:3b:cb:5c:
    6d:a9:e2:73:b5:bf:b1:c3:91:49:1a:2c:0f:da:02:
    6d:b8:69:70:be:31:2b:46:12:ec:de:e1:67:d4:ca:
    20:08:eb:53:0e:30:20:1c:c4:23:7c:8d:1a:85:92:
    71:28:a2:27:6b:fb:6f:45:37:8f:e8:b0:b5:bd:20:
    2b:e1:24:25:fc:50:90:97:45:d2:b8:7e:d6:c5:f5:
    08:c6:09:cd:3b:61:c6:8e:2b:8f:63:e3:8a:91:63:
    d0:93:8b:cd:ac:60:d6:aa:eb:d1:83:eb:c0:02:33:
    a7:1a:df:a9:ad:9c:44:fe:41:92:52:6e:49:ae:ca:
    da:af:8f:45:75:cd:23:e3:16:2b:30:d9:46:29:3a:
    2e:0d
```

```
coefficient:
    7c:6a:0e:29:46:6e:b3:8c:22:69:b8:47:57:b3:02:
    5d:50:ef:44:2d:c7:e0:88:5c:26:ee:b5:93:c8:8d:
    c9:39:fb:13:bf:e5:f6:88:ed:00:62:10:d3:3f:b6:
    76:49:73:2c:8e:f8:dc:eb:a4:1f:a0:e3:81:c2:0e:
    77:51:47:d9:88:ac:19:0b:4e:57:40:65:59:1b:b9:
    1b:89:59:57:75:3c:87:91:be:fb:19:fc:80:bd:99:
    c1:0d:26:68:bf:3f:02:79:39:12:00:8f:70:18:fa:
    32:58:7f:c0:4a:77:f4:c1:20:f5:49:48:65:bd:fd:
    27:6f:64:67:2d:01:80:41:54:62:5d:12:76:6e:24:
    d7:a0:92:07:29:14:72:cf:69:be:12:62:c0:e8:9e:
    df:2e:c3:ca:4e:b5:dc:b0:8c:19:5f:9b:73:80:36:
    47:b6:82:26:95:21:71:27:de:4f:d2:b4:05:b2:a2:
    7d:7b:b7:39:64:e9:cd:9c:c5:d1:f6:af:1c:7c:33:
    6b:53:7e:dc:1b:9b:2e:47:6e:aa:1a:4b:58:8e:06:
    40:4e:18:b6:88:80:29:84:a2:69:74:73:df:56:32:
    3e:8e:88:fa:d6:5b:9d:b5:f9:a1:5f:fc:cc:92:22:
    b3:5b:f0:88:9a:40:6e:a1:5d:a0:64:f0:bf:4a:b3:
    e6
```

- Which part of certificate indicates this is a CA's certificate?

```
X509v3 Basic Constraints: critical
    CA:TRUE
```

The output specifically mentions it in the X509v3 extensions tab.

- Which part of the certificate indicates this is a self-signed certificate?

```
X509v3 Subject Key Identifier:
    7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B
X509v3 Authority Key Identifier:
    keyid:7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B
```

Both subject key and the authority key are the same.

```
Issuer: C = US, ST = California, O = Internet Widgits Pty Ltd
Validity
    Not Before: Jul 15 06:22:29 2024 GMT
    Not After : Jul 13 06:22:29 2034 GMT
Subject: C = US, ST = California, O = Internet Widgits Pty Ltd
```

Moreover, Issuer and Subject fields seem to be the same too.

Task 2 (20 Pts): Generating a Certificate Request for Your Web Server

- Provide screenshot of the certificate generation request along with the output of the OpenSSL commands mentioned in the lab guide.

  openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -subj "/CN=www.illya2024.com/O=illya2024 Inc/=US" -addext "subjectAltName = DNS:www.illya2024.com, DNS:www.illya2024A.com, DNS:www.illya2024B.com" -passout pass:dees

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl req -newkey rsa:2048 -sha256 -keyout serv
er.key -out server.csr -subj "/CN=www.illya2024.com/O=illya2024 Inc./C=US" -addext
"subjectAltName = DNS:www.illya2024.com, DNS:www.illya2024A.com, DNS:www.illya2024B
.com" -passout pass:dees
Generating a RSA private key
.....................................................................................
.....................................................................+++++
.....................................................+++++
writing new private key to 'server.key'
```

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.illya2024.com, O = illya2024 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:9e:4a:9a:17:26:09:96:89:f4:04:03:5b:f2:bd:
                    c4:8b:67:a3:17:7a:f6:8d:f4:57:d9:49:0b:28:61:
                    2a:f1:6d:4b:08:ce:68:3a:70:fe:33:a4:c2:ae:4f:
                    fa:b2:e8:05:c3:23:51:2d:32:6e:ae:2d:d8:3c:7b:
                    ea:ea:b7:a7:a0:5a:17:ee:39:1c:12:b1:0e:1c:84:
                    ee:d7:4f:76:2f:de:7d:3e:0e:78:d8:1b:86:38:c8:
                    77:b5:18:55:1a:c7:36:14:1f:82:6d:54:ba:4c:02:
                    cf:52:56:cc:ed:1d:43:06:38:c9:09:62:be:86:1d:
                    3d:8b:fc:53:de:34:3f:7f:05:ad:87:cd:9d:e6:07:
                    cb:cd:76:74:5d:e8:e5:6f:7c:fb:99:f2:7b:35:00:
                    a1:6c:30:8c:d6:57:7a:f0:9c:ee:e3:b7:03:45:ce:
                    0a:ef:dd:c7:d6:29:06:3a:f6:18:99:51:5b:5e:f1:
                    5c:7d:be:ba:01:d9:06:94:8f:20:88:4c:ce:c0:0b:
                    1b:36:4d:49:fc:c9:d4:7d:cf:4f:2d:00:fa:59:e6:
                    50:a8:f7:09:72:2d:74:33:5d:b6:61:42:d5:7c:8e:
                    e5:70:10:84:f2:ba:e0:39:2c:39:47:c3:2c:dd:18:
                    b8:dc:cf:a1:f2:2e:cc:04:fe:08:33:61:85:82:66:
                    93:09
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.illya2024.com, DNS:www.illya2024A.com, DNS:www.illya2024B.com
    Signature Algorithm: sha256WithRSAEncryption
         9b:ad:30:a7:e2:e7:97:91:c8:98:51:76:b0:f8:29:75:ef:59:
         04:ee:46:12:49:0a:0c:1d:c0:74:1c:f6:20:a1:f4:d3:23:cf:
         ea:6e:84:35:3b:d3:f3:f6:3d:72:f0:d2:ff:c0:fa:f2:df:92:
         97:5e:9b:41:b7:ab:6d:6f:73:75:b2:da:de:a1:b8:a7:dc:18:
         9e:c7:bb:8f:5e:dd:cf:37:f6:62:b4:41:0d:ac:92:b9:c1:9d:
         6c:d2:ef:b9:b5:aa:41:5c:08:5b:9d:9c:7b:f1:0e:49:6a:11:
         9d:d1:57:3f:3e:d5:d6:82:8b:6e:23:66:19:bd:1a:af:79:01:
         56:5c:e1:43:92:f1:ac:52:2f:c9:02:6d:29:13:d9:34:7b:55:
         ea:f4:30:c3:75:a0:c9:eb:85:fd:41:fc:f8:55:e9:4d:2e:43:
         60:20:e8:a9:05:d3:8d:cd:5d:96:bf:2b:b3:1e:83:6e:6b:a6:
         bf:14:f7:a6:b0:57:4c:a3:26:b1:0a:06:70:13:83:9a:dd:4b:
         31:09:1c:18:06:93:23:2f:f7:da:95:be:f0:b9:bf:dd:8d:16:
         f6:56:5d:1a:de:86:90:c8:0f:16:1b:25:76:42:10:a1:c5:ff:
         b3:db:22:b5:60:40:00:f1:28:f2:76:30:5e:26:d1:b5:d0:3a:
         4f:1c:ac:ce
```

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:d5:55:fa:98:ae:17:8b:7b:0e:c6:ad:d4:81:0c:
    de:fa:84:e1:6f:42:36:b1:20:12:f5:ea:a8:88:0c:
    12:7d:0b:4c:c8:dc:4f:53:9a:94:a9:41:b0:5f:04:
    d2:06:91:9c:bb:d8:d7:0e:05:a7:97:dc:f0:79:7a:
    48:a6:49:84:96:ab:86:67:e6:af:09:bc:08:62:e1:
    4f:57:88:69:37:e2:d3:9a:a5:4b:a1:8e:76:c7:71:
    38:b7:ee:b0:e7:42:3b:e9:0e:97:e0:8e:d4:21:2b:
    0b:63:d4:c4:ef:8d:f9:7c:f6:bd:8b:24:d6:97:42:
    e4:6e:1a:0b:1b:4c:30:4e:cc:aa:18:4a:7e:cd:20:
    0b:a3:59:46:5f:73:52:c7:0c:84:2f:bb:e3:55:1a:
    98:e7:43:d9:48:1f:1c:f1:a3:36:57:61:5b:c8:c3:
    40:d6:36:63:7a:24:81:ae:a6:ef:d5:46:1e:35:b5:
    31:25:7e:af:0f:7d:c0:19:33:4f:32:c9:31:9d:5d:
    1c:0b:3e:ee:1c:67:5e:3b:f9:db:10:26:a7:19:60:
    7a:75:21:7e:b0:6b:0c:0f:58:aa:52:4c:f0:98:5b:
    ab:1a:d4:69:54:96:28:95:91:02:b6:2a:c5:65:7e:
    28:ec:84:9e:73:84:c0:b4:9f:20:37:20:0a:92:09:
    eb:e5
publicExponent: 65537 (0x10001)
privateExponent:
    00:af:54:d8:7e:3f:26:6e:a6:16:80:c7:40:cd:47:
    2c:c3:2c:0e:b3:07:f2:37:24:ab:30:9d:49:21:76:
    fa:82:f6:94:86:c8:3a:11:f6:0b:94:07:be:d2:78:
    fd:bc:14:54:82:36:36:98:f9:a0:c1:b8:fd:92:79:
    23:d8:36:b7:d7:b4:e4:e3:e3:bd:9b:fc:83:cf:f0:
    68:eb:01:db:a7:e8:ae:0c:7d:29:69:7f:d2:b3:1b:
    a4:87:d6:8e:61:a2:17:e6:f4:ed:71:cb:31:20:89:
    65:f5:08:5b:4a:9e:9e:9b:4b:96:80:13:28:a2:6c:
    81:9c:d3:9e:a9:32:b6:c9:2a:ff:45:b8:73:b4:da:
    b5:65:0b:b2:1a:11:6a:79:d4:2f:29:d0:38:04:f4:
    b9:8e:95:01:eb:f6:0b:45:0e:ea:ae:47:f8:4e:fb:
    0e:eb:84:26:85:2b:83:bd:63:60:74:c0:d4:f7:d1:
    04:ea:81:0a:8a:d5:55:4e:95:a8:96:75:c3:56:82:
    e3:fa:e7:93:ae:0e:7e:2f:4a:69:25:34:ed:f5:98:
    00:eb:89:39:3a:62:c3:7b:f4:1e:64:83:50:20:11:
    00:31:ee:df:8a:f5:fe:58:3b:cb:1e:fb:24:44:d7:
    9d:d6:5f:d4:9d:76:a7:f1:c5:ee:4f:84:5f:d7:f2:
    64:41
prime1:
    00:f5:f1:3d:69:d8:13:cf:27:a5:a8:d8:2d:1c:38:
    c6:84:08:7a:01:40:13:21:e1:55:1b:72:cc:3a:73:
    8c:ef:40:30:37:16:60:7d:73:4b:43:bf:30:eb:31:
    cb:ad:72:5b:82:0e:51:8d:d9:8c:2b:91:59:3e:82:
    68:2f:86:35:e6:4a:60:48:35:50:8b:d0:a4:59:8a:
    f4:58:3c:e4:b8:fd:dc:99:6a:f1:0d:76:ab:6a:42:
    b3:ef:6d:57:36:c0:82:c5:c2:b5:41:f4:cc:2f:b6:
    34:fb:a4:f6:4a:04:10:83:d4:15:78:ab:97:37:a8:
    53:72:4a:93:80:16:e2:c9:9d
```

```
prime2:
    00:de:0f:62:0e:83:fe:60:2b:47:10:3e:c6:a9:7b:
    f1:73:97:6b:3e:59:5f:44:6f:ce:22:63:e9:19:40:
    03:70:41:20:db:6e:69:bb:3f:29:82:9a:62:73:09:
    51:68:46:9a:25:19:b8:4f:d4:27:df:c4:11:52:a8:
    cf:d2:d1:c2:a2:4a:8b:9e:f2:4e:da:f4:58:8b:02:
    54:c2:33:b8:c6:77:46:49:e8:e1:5c:30:ef:ce:d3:
    28:25:4e:fa:aa:79:ab:0e:cb:62:35:c4:46:d5:73:
    f1:8e:76:b9:b5:7d:4c:be:00:28:72:cc:d3:a9:d7:
    45:e3:d5:79:a7:f0:1c:5c:e9
exponent1:
    00:d9:98:21:4c:c6:f6:e7:bd:dd:2c:60:6e:b0:dc:
    6e:8e:9c:6d:4d:33:e2:79:84:42:67:31:8f:0d:5b:
    f4:62:2c:f9:3b:93:d9:b4:c4:4f:df:d5:85:33:61:
    70:21:b9:de:ca:57:5e:c2:50:aa:5a:55:93:8e:e1:
    93:ca:10:45:19:c5:ce:1f:b4:c3:d9:9f:b3:f8:e1:
    1e:c3:fe:c4:22:03:c0:ac:1f:d8:bb:9f:b5:93:23:
    06:cd:9b:80:a1:19:7b:d9:fa:25:a2:00:32:b3:37:
    d2:f2:9d:85:a6:00:a8:97:ea:09:41:25:17:7a:0f:
    bc:1c:8f:6c:a6:d4:18:bc:65
exponent2:
    6d:06:9e:7d:43:ff:33:d6:6b:c8:a5:19:c3:02:f0:
    94:71:46:9d:51:21:fe:26:ea:cd:65:c2:7f:bc:37:
    33:f9:36:19:a6:87:51:00:fc:ef:7b:bf:54:7d:c1:
    b3:71:de:a2:d2:92:f4:d6:d4:51:00:22:05:34:8e:
    fd:12:31:fe:9e:9d:18:88:1d:81:51:30:db:e7:64:
    18:09:6e:f2:3a:83:8f:2c:40:e1:93:c1:5a:09:c0:
    8f:38:cc:c7:c0:7e:e4:ff:a4:93:83:6f:c7:c3:6a:
    59:29:1f:9a:e5:0f:35:c6:3c:15:c9:4d:2e:f9:5b:
    fe:35:c4:ca:58:90:84:69
coefficient:
    01:f1:45:6b:d9:95:9b:6d:c4:71:33:53:ec:c2:cc:
    3b:39:9f:1b:65:fe:87:e8:79:a7:cc:86:b1:3a:7b:
    10:15:cc:c3:15:1b:52:1c:e9:a6:d6:a1:a0:c9:b0:
    14:68:2a:82:66:a5:8b:ce:3f:f4:17:74:5e:ee:50:
    0b:92:a2:42:25:13:76:41:9a:5d:5b:c8:d6:16:30:
    d9:2f:1c:36:18:7a:3c:25:ee:b2:4a:dd:f8:2b:e0:
    ac:00:fa:88:75:93:4b:99:4a:4e:ab:33:6f:f9:23:
    cc:89:cb:51:be:46:c7:96:02:64:da:38:34:d8:6d:
    3e:26:e2:f1:f1:1d:7f:55
```

Task 3 (20 Pts): Generating a Certificate for Your Server

- Provide screenshot of the successful certificate generation output.

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl ca -config myssl.cnf -policy policy_anything -md sha256 -days
 3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
Using configuration from myssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Jul 15 07:57:39 2024 GMT
            Not After : Jul 13 07:57:39 2034 GMT
        Subject:
            countryName               = US
            organizationName          = illya2024 Inc.
            commonName                = www.illya2024.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                E2:55:62:FE:0D:B5:3F:D5:9B:37:45:0F:4B:80:4B:F0:51:3A:11:B3
            X509v3 Authority Key Identifier:
                keyid:7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B

Certificate is to be certified until Jul 13 07:57:39 2034 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[07/15/24]seed@VM:~/.../Labsetup$
```

- Print out the decoded content of the certificate using the OpenSSL command mentioned in the lab guide.

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Jul 15 07:57:39 2024 GMT
            Not After : Jul 13 07:57:39 2034 GMT
        Subject: C = US, O = illya2024 Inc., CN = www.illya2024.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:9e:4a:9a:17:26:09:96:89:f4:04:03:5b:f2:bd:
                    c4:8b:67:a3:17:7a:f6:8d:f4:57:d9:49:0b:28:61:
                    2a:f1:6d:4b:08:ce:68:3a:70:fe:33:a4:c2:ae:4f:
                    fa:b2:e8:05:c3:23:51:2d:32:6e:ae:2d:d8:3c:7b:
                    ea:ea:b7:a7:a0:5a:17:ee:39:1c:12:b1:0e:1c:84:
                    ee:d7:4f:76:2f:de:7d:3e:0e:78:d8:1b:86:38:c8:
                    77:b5:18:55:1a:c7:36:14:1f:82:6d:54:ba:4c:02:
                    cf:52:56:cc:ed:1d:43:06:38:c9:09:62:be:86:1d:
                    3d:8b:fc:53:de:34:3f:7f:05:ad:87:cd:9d:e6:07:
                    cb:cd:76:74:5d:e8:e5:6f:7c:fb:99:f2:7b:35:00:
                    a1:6c:30:8c:d6:57:7a:f0:9c:ee:e3:b7:03:45:ce:
                    0a:ef:dd:c7:d6:29:06:3a:f6:18:99:51:5b:5e:f1:
                    5c:7d:be:ba:01:d9:06:94:8f:20:88:4c:ce:c0:0b:
                    1b:36:4d:49:fc:c9:d4:7d:cf:4f:2d:00:fa:59:e6:
                    50:a8:f7:09:72:2d:74:33:5d:b6:61:42:d5:7c:8e:
                    e5:70:10:84:f2:ba:e0:39:2c:39:47:c3:2c:dd:18:
                    b8:dc:cf:a1:f2:2e:cc:04:fe:08:33:61:85:82:66:
                    93:09
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                E2:55:62:FE:0D:B5:3F:D5:9B:37:45:0F:4B:80:4B:F0:51:3A:11:B3
            X509v3 Authority Key Identifier:
                keyid:7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B
```

```
Signature Algorithm: sha256WithRSAEncryption
     81:83:2a:d8:58:c7:4f:3a:d3:98:04:46:c4:8f:66:ea:50:ee:
     4d:65:83:ad:15:00:d7:58:c6:40:7e:85:74:c4:1c:ca:ce:3d:
     a6:33:03:69:65:31:7b:14:31:03:63:d6:9b:96:66:85:1b:49:
     be:68:a7:dd:63:90:c5:ad:bb:31:53:ca:4e:bd:fc:46:8b:81:
     2f:d1:e6:2a:47:72:64:ae:85:60:02:ef:9e:36:51:a8:52:0c:
     03:81:ad:41:33:15:25:82:61:40:d5:9d:51:b2:ec:75:ca:78:
     29:c2:db:b1:a6:53:bd:91:04:4c:11:df:bf:96:7a:22:ce:3e:
     69:43:a9:84:9a:58:8b:87:80:3e:df:3a:39:9a:3c:c9:95:ba:
     70:9a:0b:95:5c:cc:ae:f6:5e:47:dc:3a:f5:ab:2d:4e:4d:f1:
     e9:c1:2c:5c:e2:81:6a:ad:63:d5:90:48:bf:67:1e:1a:e3:ac:
     78:16:50:2f:4a:a7:8c:a4:68:3b:c1:14:b3:82:a1:85:49:4e:
     16:9a:57:82:37:f6:aa:80:80:28:ad:76:1a:1f:32:dd:43:dd:
     8c:a2:12:6b:ad:5d:07:4f:57:39:5f:94:b7:59:7c:67:e0:0c:
     14:76:57:99:57:88:d7:a1:4d:e7:37:aa:b8:14:52:51:ff:c2:
     fa:e7:4f:e5:3c:20:5e:f2:1a:15:7f:b8:78:6d:8a:79:89:83:
     c0:3b:d7:3a:cd:af:06:7e:f7:b9:ca:87:21:2a:68:26:a8:65:
     05:03:2a:4a:de:ec:f6:c6:da:aa:4c:77:28:1e:f2:cc:af:49:
     59:cb:83:4a:f3:55:2b:5e:2d:a2:d4:61:ee:52:3d:3c:c9:15:
     30:29:4b:4a:19:f4:74:17:bd:81:4b:d7:6a:e4:40:94:8d:fc:
     57:95:77:09:9d:03:56:66:70:2c:fe:94:77:1d:5b:36:46:9b:
     bf:66:fc:8e:c0:6b:82:9f:a8:ed:14:7b:da:91:66:33:05:71:
     ca:04:26:11:0f:23:2a:b7:3a:58:2a:ea:9f:cc:f3:7f:6f:54:
     28:07:ae:a4:4f:3f:23:87:53:70:28:bc:c1:e9:9d:aa:79:9c:
     14:a8:3a:1e:b1:9f:de:d4:e1:a7:bc:e6:70:e4:cd:b9:55:6d:
     39:dc:3f:c3:ec:d6:5e:aa:7c:2d:85:9d:62:e2:34:d3:c0:63:
     51:87:b8:ed:56:59:9d:7f:ee:6e:38:99:d8:e1:9d:65:fa:07:
     d6:e1:4d:c2:38:30:47:c6:3f:9d:09:43:f8:64:c5:91:90:8f:
     4e:6b:1d:42:19:03:9a:3e:5f:0b:f4:cf:f8:c1:9d:1b:d4:b1:
     26:2e:e8:3b:40:5b:90:79
```

Task 4 (20 Pts): Deploying Certificate in an Apache-Based HTTPS Website

- Provide the screenshot of your custom website creation and explain the changes you made for the server.

```
  GNU nano 4.8  /etc/apache2/sites-available/bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.illya2024.com
    ServerAlias www.illya2024A.com
    ServerAlias www.illya2024B.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    DirectoryIndex index_red.html
</VirtualHost>
```

What I have done is changed the website name and its aliases names in order to match the ones provided in the certification and key files. Moreover, I have changed the certification and key files to match the ones I created.

- Your web server should be named “www. <first name>2024.com”. After starting your custom web server, did you get to browse the website successfully? Provide your observation

```
root@dbd95186c864:/# service apache2 start
 * Starting Apache httpd web server apache2
 *
 * The apache2 configtest failed.
Output of config test was:
AH00526: Syntax error on line 8 of /etc/apache2/sites-enabled/bank32_apache_ssl.
conf:
SSLCertificateFile: file '/certs/server.crt' does not exist or is empty
Action 'configtest' failed.
The Apache error log may have more information.
```

The virtual machine returned an error saying that the need server.crt and server.key files were not found in the /certs/ directory. The reason is that we have not copied our newly created certificate and the key into the virtual machine volume folder.

- What did you do to fix the problem faced in the previous answer? Provide screenshots of all the steps as well as successful output of browsing the website.

1) First, using my local machine, I copied my server.crt and server.key inside the volume folder

```
[07/15/24]seed@VM:~/.../Labsetup$ cp server.crt server.key volumes/
```

2) Next, using my virtual machine, I copied the two files inside a certs folder inside the volume folder

```
root@dbd95186c864:/# cd volumes/
root@dbd95186c864:/volumes# cp server.crt server.key
root@dbd95186c864:/volumes# cp server.crt server.key /certs/
```

3) **Tried to start the apache2 service again.**

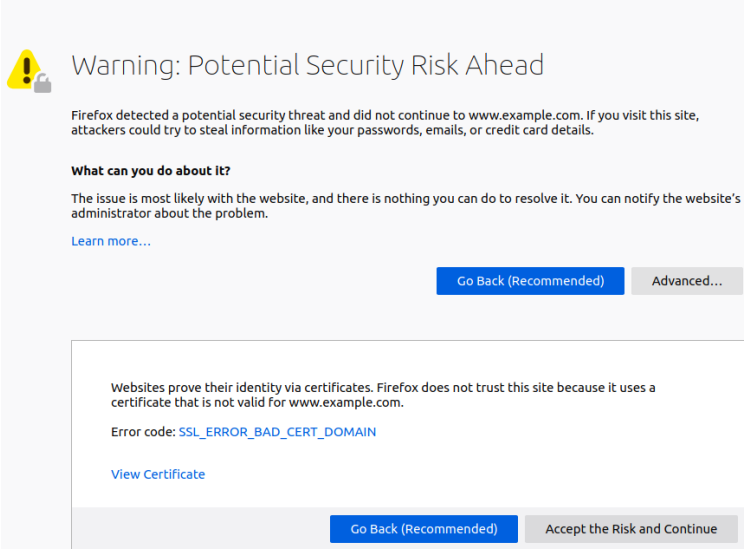
```
root@dbd95186c864:/volumes# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.illya2024.com:443 (RSA):
 *
root@dbd95186c864:/volumes#
```

Task 5 (20 Pts): Launching a Man-In-The-Middle Attack

- How did you launch the Man-In-The-Middle attack? Specifically, what method you used and how did it help?

  In order to launch the Man-In-The-Middle attack I have configured the bank32_apache_ssl.conf file to create a website that has the same link as the existing www.example.com website. Next I have added a fake DNS into my /etc/hosts file and tried to enter the website using https protocol.

- Provide observation of the output of the browser after you browse www.example.com. Also provide screenshot of your output.



The browser prevented the MITM attack and warned me of the potential security risk. Firefox also mentioned that my fake www.example.com website uses a different certificate compared to the one the original example website uses.

Task 6 (Bonus – 10 Pts): launching a Man-In-the-Middle Attack with a Compromised CA

- Design an experiment to show that the attacked can successfully launch MITM attacks on any HTTPS website. Provide screenshots of your successful attack and explain attack and observations.

For this experiment I will use the www.example.com/.

1) **First of all, I created a fake certificate signing request and a key and called them fake.csr and fake.key respectively.**

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl req -newkey rsa:2048 -sha256  -keyout fake.key -out fake.csr -subj "/CN=www.example.
com/O=Fake Inc./C=US"  -passout pass:dees
Generating a RSA private key
.....................................................................................+++++
.....................................+++++
writing new private key to 'fake.key'
```

2) **Next, using CA certificate and its private key I signed the certificate and made the fake certificate – fake.crt.**

```
[07/15/24]seed@VM:~/.../Labsetup$ openssl ca -config myssl.cnf -policy policy_anything -md sha256 -days 3650  -in fake.csr -out
 fake.crt -batch  -cert ca.crt -keyfile ca.key
Using configuration from myssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4099 (0x1003)
        Validity
            Not Before: Jul 16 02:42:16 2024 GMT
            Not After : Jul 14 02:42:16 2034 GMT
        Subject:
            countryName               = US
            organizationName          = Fake Inc.
            commonName                = www.example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F6:C9:60:6B:DF:9D:45:6E:84:95:0E:F4:33:76:2F:06:11:FA:31:1E
            X509v3 Authority Key Identifier:
                keyid:7A:0A:38:20:72:1D:15:FE:67:DE:C3:D3:19:80:08:1C:76:E4:0F:6B

Certificate is to be certified until Jul 14 02:42:16 2034 GMT (3650 days)
```

3) **Next I copied both fake.crt and the fake.key into the /certs/ directory and modified the bank32_apache_ssl.conf file in order to fake the www.example.com website using a fake link - https://www.example.com, using the fake certificate and the key.**

```
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.example.com
    DirectoryIndex index_red.html
    SSLEngine On
    SSLCertificateFile /certs/fake.crt
    SSLCertificateKeyFile /certs/fake.key
</VirtualHost>
```

4) Finally, here is the original website(on the left) and the fake one(on the right)