哈尔滨工业大学(深圳)

《网络与系统安全》 实验报告

实验四

PKI 实验

学 院: 计算机科学与技术

姓 名: 宗晴

学 号: 200110513

专 业: 计算机类

日 期: 2023 年 5 月

1. 根据如下命令查看证书信息，并回答下面两个问题。

命令为：openssl x509 -in ca.crt -text -noout。

命令 openssl x509 -in ca.crt -text –noout 的结果如下图所示;

```
[05/18/23]seed@VM:~/PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3e:b5:df:8d:68:71:4e:38:e7:eb:5d:b3:c2:53:73:dc:01:df:2f:10
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May 18 08:28:24 2023 GMT
            Not After : May 15 08:28:24 2033 GMT
        Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:c7:e0:6e:7f:22:0e:36:9d:d7:90:b0:33:d6:33:
                    c7:d1:9e:2c:37:3c:78:13:ca:2d:79:57:de:d4:de:
                    d3:c6:59:58:e5:95:b9:54:94:7d:61:4f:52:a4:d8:
                    f5:5c:4b:ad:8c:02:9f:dd:64:76:99:97:a0:cc:77:
                    cc:4b:30:fc:c2:f4:c3:73:6b:a2:06:5c:e9:db:71:
                    01:56:19:e4:c6:e3:09:bd:cd:ef:d8:13:d0:e5:7e:
                    11:53:49:ff:0a:40:96:7c:d2:20:c3:3e:6e:e6:e2:
                    cd:52:51:28:0e:6d:06:b9:eb:69:d1:4b:0f:b5:61:
                    c3:79:80:ca:fe:9c:57:a8:f0:4f:88:a4:20:fc:eb:
                    55:97:e5:9d:5a:6c:75:c6:c0:e8:f3:13:31:0d:48:
                    83:8d:a6:6f:2a:ed:44:3f:9a:37:86:13:a3:11:e3:
                    02:b0:ae:1f:84:d8:3d:e9:4e:65:a2:6e:d7:db:29:
                    1e:d1:13:58:1c:d1:71:d5:84:75:93:3f:f4:b5:7b:
                    89:6e:94:08:43:5f:36:1d:6e:d4:7c:ea:56:17:d9:
                    39:3d:67:79:0e:83:06:2a:f0:06:59:36:a9:e2:a4:
                    8e:bf:29:fc:a9:a3:53:0c:13:7a:22:4d:86:bb:f4:
```

```
                89:6e:94:08:43:5f:36:1d:6e:d4:7c:ea:56:17:d9:
                39:3d:67:79:0e:83:06:2a:f0:06:59:36:a9:e2:a4:
                8e:bf:29:fc:a9:a3:53:0c:13:7a:22:4d:86:bb:f4:
                d1:f5:ff:5f:cc:8d:82:0b:8c:ae:ba:fa:4b:c8:1f:
                a5:e9:94:ea:8b:22:aa:d8:fa:87:f1:fc:bb:d9:3c:
                1a:d0:67:c8:c7:b6:09:8b:e7:87:de:5e:00:37:bc:
                65:d6:af:d8:f1:e6:12:ad:1c:47:af:b9:31:6b:d4:
                29:7e:44:10:f3:b2:4c:f6:d7:88:5f:8a:0b:9e:a6:
                79:b2:e3:a5:a4:cb:31:e8:2a:0a:8e:20:c2:54:32:
                ed:95:f5:e6:af:4c:95:d1:0a:d0:52:49:08:af:43:
                18:5e:24:3c:b5:b5:0e:9e:1a:00:17:a6:ab:ee:aa:
                3d:68:6e:cc:2f:be:74:3b:19:74:d0:77:b2:66:4c:
                8f:7f:df:55:7c:26:aa:44:98:5c:cf:17:1b:45:e2:
                77:f0:d0:3e:d1:b5:c4:69:ab:95:98:d0:32:85:be:
                91:73:ec:ce:79:00:b9:7d:60:a4:08:70:d6:ee:ec:
                2b:a8:f6:e6:64:e8:62:67:d4:53:82:6e:bd:04:a3:
                2e:24:8b:c8:76:70:02:ee:ab:18:fd:df:7a:b7:9d:
                37:af:7d:86:23:3d:b9:c0:5d:79:65:39:eb:62:28:
                fd:ed:c7:d3:f3:5d:55:20:1f:b9:a2:79:95:6b:7a:
                2c:c2:96:1f:81:bc:a0:3d:dc:7b:6c:e7:76:f0:da:
                2c:97:e4:e1:e6:0b:ad:57:50:a9:cb:d6:83:25:7c:
                95:5d:43
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            19:9B:AC:87:6F:8E:99:BB:14:E9:DE:E7:FB:65:E4:8B:65:EB:FE:85
        X509v3 Authority Key Identifier:
            keyid:19:9B:AC:87:6F:8E:99:BB:14:E9:DE:E7:FB:65:E4:8B:65:EB:FE:85

        X509v3 Basic Constraints: critical
            CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
```

```
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         bb:ed:60:b4:94:ff:7b:1d:d6:ae:a0:9d:1d:f0:29:5f:45:2e:
         3c:29:20:e3:31:22:1a:9e:95:c4:24:43:65:b0:02:c4:70:1f:
         6a:93:34:60:4a:35:02:65:20:ba:2a:b5:91:fc:4d:3f:7a:c3:
         86:a7:df:3d:95:36:56:24:1b:48:80:62:f7:8c:22:2b:39:fe:
         dd:90:78:43:d1:fd:3e:52:a1:f6:44:fc:4c:f7:d7:56:72:e8:
         b2:4b:c3:88:33:54:ff:f6:3c:a9:e7:d2:6a:0a:ae:81:26:c9:
         17:97:10:c2:d8:78:da:04:2b:c8:b8:55:5b:27:b3:63:60:63:
         1e:da:dd:52:63:b7:0d:2d:64:77:b3:0d:39:26:70:f0:ec:1d:
         72:ec:3e:3f:04:b9:ce:bb:60:3b:1e:73:e3:ff:64:f8:32:7d:
         a0:b4:2d:d5:11:0f:d4:f3:21:99:67:07:bf:43:64:40:9b:1e:
         8b:74:7c:ca:39:60:6c:72:67:ca:be:c8:7a:9a:e2:49:ca:a3:
         46:0f:0f:c2:e5:61:48:33:7b:46:93:68:0e:1e:ac:e4:e1:18:
         c8:5a:64:a4:99:77:7a:1f:e9:5f:95:63:20:c3:08:8a:cb:15:
         6a:48:8d:6c:f4:7f:fc:5f:51:bf:d0:ad:9d:9b:bd:06:53:d1:
         89:36:51:8d:42:f0:00:a8:69:91:6d:96:48:ca:19:d9:43:fd:
         9a:a5:a9:27:d6:17:51:a8:31:fc:5a:59:ec:a2:ff:71:84:db:
         65:98:8b:62:1d:7f:97:f3:19:a8:2d:03:eb:64:9f:1f:89:65:
         12:9d:9e:b9:ce:bf:e7:9d:f4:18:19:f7:ab:0f:76:11:d4:ed:
         aa:df:59:e0:81:7d:f7:9d:1e:0a:71:f7:ed:ce:86:9f:a3:80:
         00:fa:8c:fd:65:ea:2a:2e:25:48:4a:c0:39:1d:fd:f1:6b:a2:
         29:69:ee:57:d7:f3:19:66:1b:2e:ae:d9:3f:bf:e8:d6:c5:e5:
         0a:9e:b6:0e:00:47:f3:b6:6c:29:ea:ee:2b:1b:82:9c:96:a7:
         ca:f9:76:08:88:03:9c:85:c4:22:13:14:03:2d:77:18:e1:99:
         7d:7c:17:ec:f7:37:19:9b:81:53:7b:82:73:6b:cd:26:94:3e:
         d0:cf:09:19:d4:d5:fb:60:49:b7:83:15:bf:1e:f0:d0:81:75:
         b2:86:cf:e1:d9:9b:02:f7:8a:46:58:43:ce:a0:22:72:0a:42:
         1c:36:2a:4f:f9:64:64:02:fe:8e:fb:6c:df:d1:2b:1a:46:be:
         3f:da:ab:26:4a:b2:1c:a6:1c:22:a2:ce:00:0e:cb:28:80:cc:
         ae:56:6f:57:5d:1c:c6:0c
[05/18/23]seed@VM:~/PKI$
```

命令 openssl rsa -in ca.key -text -noout 的结果如下图所示;

```
[05/18/23]seed@VM:~/PKI$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:c7:e0:6e:7f:22:0e:36:9d:d7:90:b0:33:d6:33:
    c7:d1:9e:2c:37:3c:78:13:ca:2d:79:57:de:d4:de:
    d3:c6:59:58:e5:95:b9:54:94:7d:61:4f:52:a4:d8:
    f5:5c:4b:ad:8c:02:9f:dd:64:76:99:97:a0:cc:77:
    cc:4b:30:fc:c2:f4:c3:73:6b:a2:06:5c:e9:db:71:
    01:56:19:e4:c6:e3:09:bd:cd:ef:d8:13:d0:e5:7e:
    11:53:49:ff:0a:40:96:7c:d2:20:c3:3e:6e:e6:e2:
    cd:52:51:28:0e:6d:06:b9:eb:69:d1:4b:0f:b5:61:
    c3:79:80:ca:fe:9c:57:a8:f0:4f:88:a4:20:fc:eb:
    55:97:e5:9d:5a:6c:75:c6:c0:e8:f3:13:31:0d:48:
    83:8d:a6:6f:2a:ed:44:3f:9a:37:86:13:a3:11:e3:
    02:b0:ae:1f:84:d8:3d:e9:4e:65:a2:6e:d7:db:29:
    1e:d1:13:58:1c:d1:71:d5:84:75:93:3f:f4:b5:7b:
    89:6e:94:08:43:5f:36:1d:6e:d4:7c:ea:56:17:d9:
    39:3d:67:79:0e:83:06:2a:f0:06:59:36:a9:e2:a4:
    8e:bf:29:fc:a9:a3:53:0c:13:7a:22:4d:86:bb:f4:
    d1:f5:ff:5f:cc:8d:82:0b:8c:ae:ba:fa:4b:c8:1f:
    a5:e9:94:ea:8b:22:aa:d8:fa:87:f1:fc:bb:d9:3c:
    1a:d0:67:c8:c7:b6:09:8b:e7:87:de:5e:00:37:bc:
    65:d6:af:d8:f1:e6:12:ad:1c:47:af:b9:31:6b:d4:
    29:7e:44:10:f3:b2:4c:f6:d7:88:5f:8a:0b:9e:a6:
    79:b2:e3:a5:a4:cb:31:e8:2a:0a:8e:20:c2:54:32:
    ed:95:f5:e6:af:4c:95:d1:0a:d0:52:49:08:af:43:
    18:5e:24:3c:b5:b5:0e:9e:1a:00:17:a6:ab:ee:aa:
    3d:68:6e:cc:2f:be:74:3b:19:74:d0:77:b2:66:4c:
    8f:7f:df:55:7c:26:aa:44:98:5c:cf:17:1b:45:e2:
    77:f0:d0:3e:d1:b5:c4:69:ab:95:98:d0:32:85:be:
    91:73:ec:ce:79:00:b9:7d:60:a4:08:70:d6:ee:ec:
```

```
    91:73:ec:ce:79:00:b9:7d:60:a4:08:70:d6:ee:ec:
    2b:a8:f6:e6:64:e8:62:67:d4:53:82:6e:bd:04:a3:
    2e:24:8b:c8:76:70:02:ee:ab:18:fd:df:7a:b7:9d:
    37:af:7d:86:23:3d:b9:c0:5d:79:65:39:eb:62:28:
    fd:ed:c7:d3:f3:5d:55:20:1f:b9:a2:79:95:6b:7a:
    2c:c2:96:1f:81:bc:a0:3d:dc:7b:6c:e7:76:f0:da:
    2c:97:e4:e1:e6:0b:ad:57:50:a9:cb:d6:83:25:7c:
    95:5d:43
publicExponent: 65537 (0x10001)
privateExponent:
    51:65:9b:7a:18:a3:53:28:aa:7d:d8:d3:f3:5a:78:
    f8:6b:82:b4:27:e2:fa:a4:2e:2a:a9:57:2c:b7:65:
    e4:f3:c3:d9:13:45:3b:25:91:7d:cc:70:ea:83:14:
    40:b6:ed:01:04:9c:97:eb:6e:c5:13:d3:bf:10:d6:
    58:94:a5:8a:bb:64:d1:1f:37:07:82:55:16:31:8a:
    0a:c7:56:bc:8b:ff:0e:95:cc:23:e1:c6:03:7f:78:
    8c:c3:a8:a2:43:35:45:b5:c8:f3:d9:fc:0d:f8:b5:
    06:dd:d8:03:2f:f1:3a:4b:9d:77:47:2b:29:81:9b:
    ba:62:71:c8:88:60:c6:82:be:d0:f5:8e:1d:91:b4:
    f4:bb:e4:7d:cb:87:97:1e:3e:7f:a7:04:25:d5:af:
    05:43:8f:28:1b:21:dd:08:ef:ad:a1:57:9a:54:29:
    67:4c:31:b7:c6:dc:47:a3:ce:8d:fc:b7:d9:1f:80:
    d6:42:1b:72:f8:f4:73:b0:92:b5:19:a9:8d:32:b7:
    00:1a:36:d7:40:f1:e7:c0:97:b6:1b:34:5e:57:ef:
    10:8b:8f:e8:12:01:b4:00:b5:85:25:56:bf:de:a5:
    e7:41:b1:0c:60:5f:d4:9e:25:f1:cc:42:9f:4e:8f:
    26:b0:0e:12:5e:5a:64:5b:b1:58:a1:cf:b4:ba:f6:
    b4:55:b0:73:d5:e0:65:17:26:07:93:1f:41:22:e8:
    93:c3:c6:f7:80:5f:c0:50:24:11:7e:e8:51:10:49:
    30:91:9f:75:33:3a:9a:b2:04:84:ca:79:58:a0:0a:
    f7:fd:38:b1:ee:96:d0:f0:94:07:fe:05:96:00:b7:
    0b:22:15:b6:ac:0b:70:15:6d:46:cf:b3:73:ec:d1:
```

```
    0b:22:15:b6:ac:0b:70:15:6d:46:cf:b3:73:ec:d1:
    48:13:3a:6a:af:22:25:c5:ee:b3:0d:9e:6d:cd:07:
    eb:33:d1:a9:e5:d7:a6:b6:b4:7f:02:a6:4b:2d:a0:
    09:9e:bc:94:86:91:c5:43:96:57:0a:bd:02:0a:c4:
    6c:9a:d9:9c:e0:04:00:74:12:2d:0a:56:d7:e5:4d:
    9c:70:b0:e8:b8:c0:eb:de:5e:38:e8:e6:3c:e5:59:
    9a:df:15:f4:fe:d4:1b:aa:4c:5b:14:33:c5:6f:7b:
    e9:0e:0f:d1:57:7c:38:ac:50:95:d0:fa:3b:96:50:
    b7:38:06:1c:2b:6a:e1:23:64:0f:1d:de:3a:1b:9d:
    46:19:5a:7f:38:64:1a:ec:06:10:8e:ac:8c:eb:35:
    34:b9:2d:81:2b:ed:d5:94:38:05:12:e5:d5:be:e7:
    40:18:2b:47:fc:dc:8a:7a:d6:9c:09:61:af:ed:d6:
    6c:2c:eb:ac:62:48:08:1a:77:c9:a1:9d:ed:94:98:
    02:a9
prime1:
    00:ec:2d:ef:e5:b6:ea:74:54:6c:4e:83:1e:dc:6a:
    c7:0c:5c:ee:fa:e2:2c:c0:ea:92:bf:0b:ea:fd:61:
    04:62:87:44:ce:8b:8a:1b:0e:17:eb:3e:2d:98:7d:
    de:b4:b8:21:e4:9e:f1:d9:53:18:f7:31:83:fb:f0:
    52:0b:5e:ce:c6:b1:e4:69:8e:85:17:1a:b6:35:c1:
    18:c0:79:b7:09:b7:27:d8:e3:5b:0c:56:a3:1e:0d:
    32:29:42:12:1e:7a:7e:c4:2d:fd:af:6a:0f:aa:ea:
    34:bc:c8:7e:85:51:dd:25:1f:23:ad:02:8d:0a:99:
    13:14:6a:7c:49:c2:38:76:4f:84:58:ae:6e:cf:96:
    bf:f0:a1:82:e8:bd:db:41:93:a8:4e:c5:f6:2c:49:
    29:50:ad:1c:b6:85:74:e0:d1:e3:47:3c:21:a5:45:
    5a:b8:c9:03:0f:f4:c2:73:3b:d5:20:2e:5a:5b:26:
    a7:95:66:34:cb:99:9d:41:e3:f7:12:5d:83:28:5c:
    7a:ce:38:b1:91:70:bb:10:98:22:f3:a3:d8:30:e5:
    06:b2:fb:5d:3f:fd:1c:9f:b4:97:13:b5:c7:4a:4c:
    5e:38:14:fd:d0:b7:50:ee:aa:48:97:3b:7b:e4:19:
    74:0c:82:e4:07:ea:5d:3a:5f:2c:24:4b:47:3c:39:
```

```
    d3:8f
prime2:
    00:d8:a6:91:90:f5:04:14:ed:b6:ea:27:62:1d:d4:
    fa:75:17:8a:46:6d:3e:19:13:96:46:82:31:ab:fe:
    db:4f:88:d7:5b:6b:f4:2e:30:a7:b5:42:56:66:af:
    47:0b:1f:ed:99:25:a0:52:4f:8d:5c:a1:f3:da:ab:
    2e:8d:8c:12:ba:3a:78:bf:14:a4:26:4d:ad:46:a5:
    71:e0:2d:58:db:4c:1d:a1:92:54:d7:90:11:94:35:
    27:52:3a:97:64:57:17:cd:58:1d:10:0a:3f:b9:39:
    8f:6c:ee:60:5c:89:0c:f4:d8:ca:86:ad:ec:3b:94:
    57:f2:59:34:46:e8:8f:94:a4:1f:e4:3f:55:66:07:
    0d:88:a6:7e:32:b1:bc:f8:81:45:29:c0:87:e6:dc:
    0b:42:06:68:03:67:69:a2:1c:a9:5a:88:e5:aa:b8:
    4c:21:f6:ac:bc:91:5d:6f:33:25:a9:55:ce:e3:7e:
    31:74:fc:2a:d1:60:c9:11:72:c6:58:0a:73:ed:93:
    bd:22:52:db:a5:67:98:cd:e9:43:3a:05:16:f6:b9:
    74:23:20:54:b8:d6:d0:89:96:34:df:d8:8e:6a:6f:
    7e:a0:4a:08:25:39:f4:85:ad:16:3b:84:29:37:d0:
    92:57:63:af:92:79:fc:e9:73:39:c4:9e:ae:bc:c4:
    f1:0d
exponent1:
    00:a1:97:ac:93:d7:5b:02:cc:e0:6d:b7:78:de:06:
    90:b9:fc:bb:e6:1b:e9:d2:f4:ac:02:da:fc:a4:f0:
    44:37:c5:a5:66:4c:42:e9:cf:f2:bd:99:85:48:d8:
    96:0f:c0:0c:30:88:2f:a1:2a:21:e2:bf:96:36:42:
    6f:60:28:36:01:ec:a5:03:33:e8:0b:ae:d3:0c:64:
    59:b3:17:94:0c:a9:ac:31:d1:1c:f2:8c:34:7e:d3:
    38:86:d2:15:e3:94:9c:37:4d:e0:4c:ac:9c:9b:ac:
    32:f9:17:94:b9:53:11:a3:dc:72:64:65:62:6a:e5:
    e1:10:0e:eb:8a:eb:c0:05:f2:d1:f2:7b:26:86:11:
    f6:b1:85:50:34:3d:f2:4e:23:e0:fc:44:a5:f2:16:
    fc:95:9e:5c:0e:e5:b0:da:41:c0:e7:74:54:f0:e7:
```

```
    4a:f3:33:55:4d:0d:82:1d:a5:ca:64:82:52:80:1b:
    2a:7e:25:b7:e9:b5:e8:ca:b4:56:cf:d1:fb:73:1a:
    13:4c:15:ae:28:7c:a1:00:f1:96:b8:6c:59:f6:da:
    3c:83:29:48:dc:07:2a:16:7b:51:02:c3:54:df:98:
    f0:be:1e:5e:aa:f7:42:00:89:b1:b1:07:99:f4:af:
    15:9f:99:ce:bb:3b:b7:1d:c1:10:4a:a4:d6:d0:76:
    20:31
exponent2:
    5a:24:54:04:c0:2d:46:97:f1:b7:53:53:9b:9d:f5:
    e7:aa:37:ba:3d:d1:cc:95:3d:bd:70:86:42:4d:f3:
    ea:0f:c1:ab:24:2b:a0:dc:55:ab:31:42:c9:ce:bb:
    fc:80:f8:56:f4:34:d4:8a:8d:02:b1:cf:c8:77:d9:
    12:c3:e9:36:db:05:4a:5b:c8:40:b7:a9:14:ef:d9:
    85:b0:d8:7b:c6:1b:be:12:28:82:d8:4a:b8:23:b5:
    8c:9d:1c:48:7f:84:43:c8:19:af:86:d4:24:b9:32:
    57:dc:86:f3:79:82:8e:8d:75:16:bc:5e:c2:1b:62:
    cc:4f:19:55:37:86:26:0e:73:c6:80:23:84:24:03:
    19:8c:4c:8d:c3:2e:21:27:88:23:6b:1c:20:8e:05:
    91:1f:21:3f:e9:53:26:44:4e:a2:80:bb:2e:61:28:
    2c:29:7a:8d:aa:dd:f9:5a:8a:9c:fe:3a:ea:a4:a2:
    e7:4d:d4:72:f1:96:37:50:4d:fe:6b:ba:f8:6a:b4:
    13:07:ee:a3:cf:8a:e0:81:e1:9a:ce:6b:53:94:ae:
    21:bf:5e:00:da:40:42:3e:e1:19:11:fd:8f:83:7c:
    68:2c:e5:5e:b7:d2:69:9c:2e:d7:ec:91:49:cb:da:
    57:c9:fe:4f:2f:ba:6f:57:a5:fd:8d:18:9f:2a:42:
    31
coefficient:
    7e:b4:88:e0:2c:a2:67:08:63:44:08:40:31:4d:4e:
    4b:20:cd:0a:3f:5c:2f:c2:02:82:83:6e:55:f7:a9:
    a8:c2:9d:1f:1b:45:64:3f:f1:45:8c:0e:7a:ff:be:
    6c:6f:b0:1e:04:26:d2:48:75:b8:c3:d3:ad:a9:98:
    10:08:93:df:c1:cd:b4:6a:d0:ef:99:19:b2:bb:53:
    36:ed:9b:5c:3a:e9:83:b5:7a:20:ad:38:b1:8d:27:
    00:2b:f7:b7:08:33:21:ec:7d:90:73:a7:59:79:d1:
    d9:ac:70:cf:12:fd:86:26:51:b9:1d:29:45:61:b3:
    eb:bc:b2:6e:d7:ab:36:c9:fe:32:2e:99:23:56:89:
    5c:7d:a9:1e:23:ad:fc:8e:af:66:75:19:d3:34:b4:
    d6:e9:8e:88:f2:9f:d9:1a:6d:45:6d:c6:51:ce:5b:
    44:c6:16:f9:b3:8f:86:c9:f8:f5:7d:e8:96:2a:0f:
    b3:ab:b6:ee:f4:20:3f:93:7b:76:d7:4c:8c:9e:00:
    a8:56:15:44:57:82:ed:94:77:3a:db:53:2e:00:b7:
    21:86:02:f3:ae:f5:59:31:cc:54:6c:f1:fe:c1:f4:
    e5:2a:71:cc:35:76:a1:7f:25:cb:4b:55:d2:78:e1:
    61:f5:c8:19:b8:2b:de:90:a0:35:34:cf:1d:fb:b6:
    1e
[05/18/23]seed@VM:~/PKI$
```

(1) 证书的哪部分内容表明这是证书的持有方?

```
Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
```

如上图所示，证书的该部分内容表明这是证书的持有方。

（2）从证书的哪部分内容可以看出这是自签名的证书？

```
Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
```

如上图所示，该行表示证书的签发机构，可以看出与证书的持有方相同，因此表明这是自签名的证书

2. 用如下命令查看 www.bank32.com 的服务器证书，至少说出与 ca.crt 的证书的两点不同。

openssl x509 -in server.crt -text -noout：

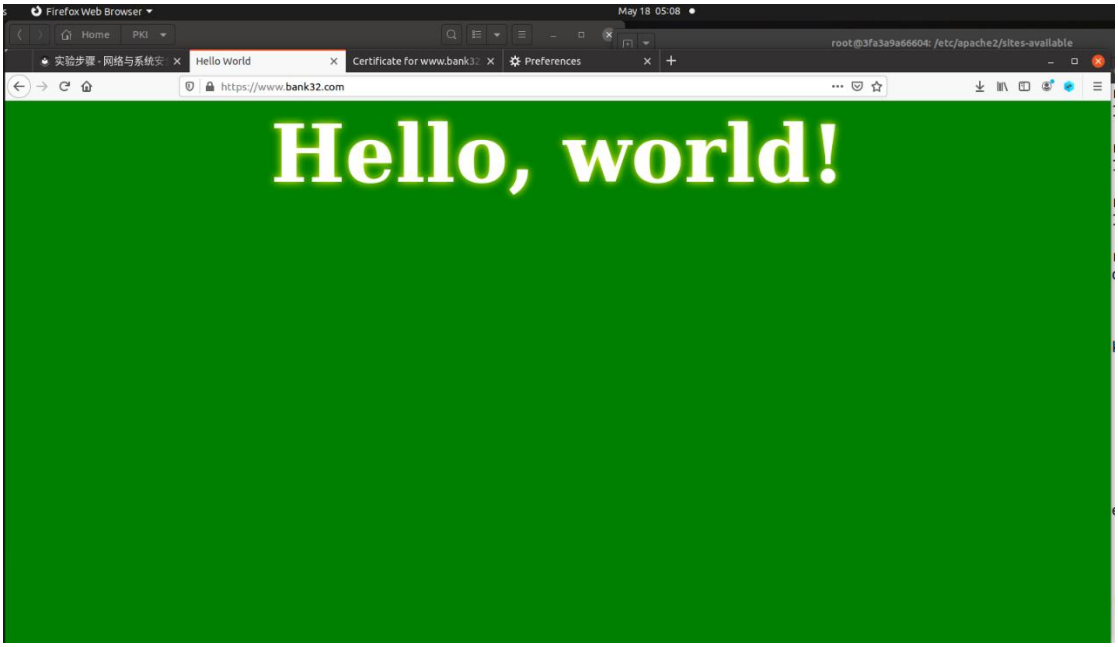
```
[05/18/23]seed@VM:~/PKI$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May 18 08:46:47 2023 GMT
            Not After : May 15 08:46:47 2033 GMT
        Subject: C = US, O = Bank32 Inc., CN = www.bank32.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bb:37:1a:19:e9:36:49:78:d4:f6:08:3f:8b:a6:
                    99:15:92:64:d8:b4:c4:89:f9:35:4e:f5:23:36:bc:
                    3d:19:0c:48:02:9b:90:09:43:f9:eb:12:34:fd:67:
                    6a:b8:52:ac:3a:18:5d:1f:da:c6:77:a4:c6:db:74:
                    30:da:1c:88:46:61:7a:60:d9:3c:8d:17:88:24:53:
                    c7:a5:e2:bb:fd:97:22:90:32:65:e1:5e:c4:7b:5c:
                    0c:cb:48:a5:70:70:0e:e3:8a:58:eb:b1:3d:f8:4a:
                    e6:45:0f:11:64:6c:34:a7:b5:ea:d6:27:84:15:e7:
                    a1:e3:d3:aa:f8:24:c7:d8:0d:d0:ba:6a:14:57:3a:
                    18:82:fa:43:98:6e:21:b3:17:bc:18:ba:fa:8f:a0:
                    64:93:e1:17:21:56:99:e8:02:40:ed:7b:ec:90:a7:
                    0f:5c:ec:9e:75:dd:b7:c4:c8:0b:9a:ec:02:ee:9e:
                    3c:1c:a0:12:58:15:a0:6c:0c:99:49:87:3d:07:5b:
                    a4:fb:e9:98:ab:52:1b:0d:1a:db:b1:70:8c:00:bc:
                    d6:30:3f:2c:85:6b:58:c8:7b:55:a4:52:5f:e3:7a:
                    b1:c2:5f:9d:ff:91:7b:a5:b2:e9:93:f3:2c:75:9f:
                    82:45:6b:23:ea:eb:92:48:99:78:05:b6:49:98:c9:
```

```
                d6:30:3f:2c:85:6b:58:c8:7b:55:a4:52:5f:e3:7a:
                b1:c2:5f:9d:ff:91:7b:a5:b2:e9:93:f3:2c:75:9f:
                82:45:6b:23:ea:eb:92:48:99:78:05:b6:49:98:c9:
                6e:7b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            7B:21:5D:71:C2:7B:90:A7:55:58:33:66:12:98:89:E6:ED:C2:07:5A
        X509v3 Authority Key Identifier:
            keyid:19:9B:AC:87:6F:8E:99:BB:14:E9:DE:E7:FB:65:E4:8B:65:EB:FE:85

        X509v3 Subject Alternative Name:
            DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com
Signature Algorithm: sha256WithRSAEncryption
     1c:46:4d:a0:a7:9b:9f:03:a9:7e:f4:3a:7d:27:7b:d7:6f:44:
     87:76:a4:55:9b:bd:d5:f8:85:5d:2f:46:76:31:27:bb:b4:88:
     c5:47:69:37:06:4e:9d:e9:e4:43:ef:1a:01:14:c6:a2:27:70:
     4e:9a:8a:22:52:a8:ea:57:7d:1b:c3:e7:f0:9e:e6:c9:e8:1b:
     da:dd:26:40:e3:26:50:ad:9d:c5:a8:74:d7:3b:0c:aa:3e:01:
     83:3a:20:78:f9:84:a6:a7:57:7d:8c:ab:48:60:b2:c1:5f:39:
     60:ee:6d:99:81:38:f8:81:51:31:4c:e7:cb:92:f5:03:92:b8:
     ed:db:09:ac:80:5b:54:c9:d1:12:5f:4e:85:0c:7b:46:13:d2:
     aa:ee:11:8d:fa:b5:5b:fa:45:fe:46:f1:72:95:21:d0:fb:59:
     0c:1c:ea:03:3e:26:42:f4:ba:3a:88:e0:26:a7:65:e6:3e:00:
     16:a4:fc:a5:7c:fd:0d:06:f1:17:ee:f4:cc:0e:6f:c6:c6:0a:
     37:13:45:30:9f:90:a2:4c:47:81:53:05:4b:70:d7:2a:85:e7:
     dc:19:ab:d9:ee:f1:c7:00:11:2e:95:c3:fb:c9:b9:c8:62:80:
     04:a0:90:7b:91:3a:f9:92:09:7b:46:c4:11:66:e3:64:50:67:
```

与 ca.cr 的证书的不同之处在于：证书的拥有者与 ca.cr 不同，此处为 www.bank32.com 所拥有，且不再与证书的签发机构相同，不再是自签名。证书的有效时间也不同。此外，RSA Public-Key 的长度不同，此处为 2048bit，而 ca.cr 中是 4096bit。Serial Number 的格式不同。

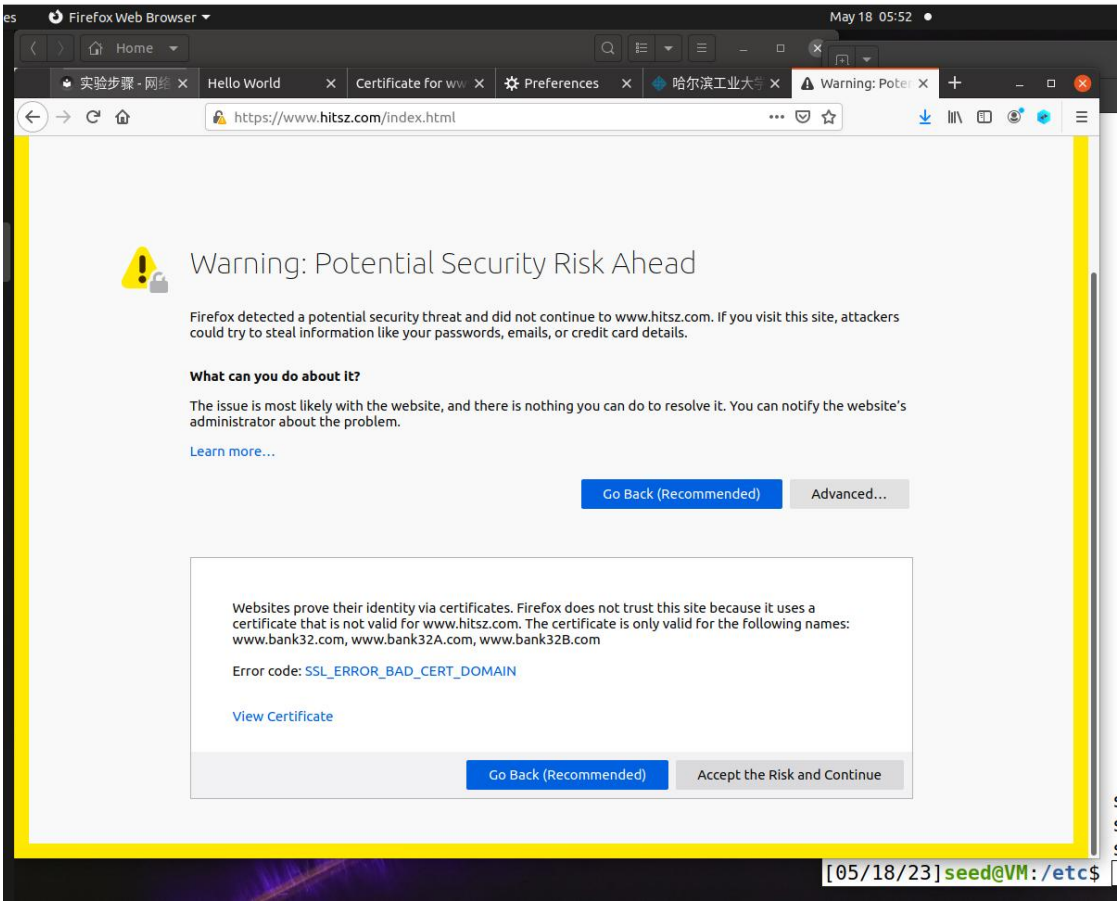
3. 请将能够正确访问 www.bank32.com 的截图贴在下面。



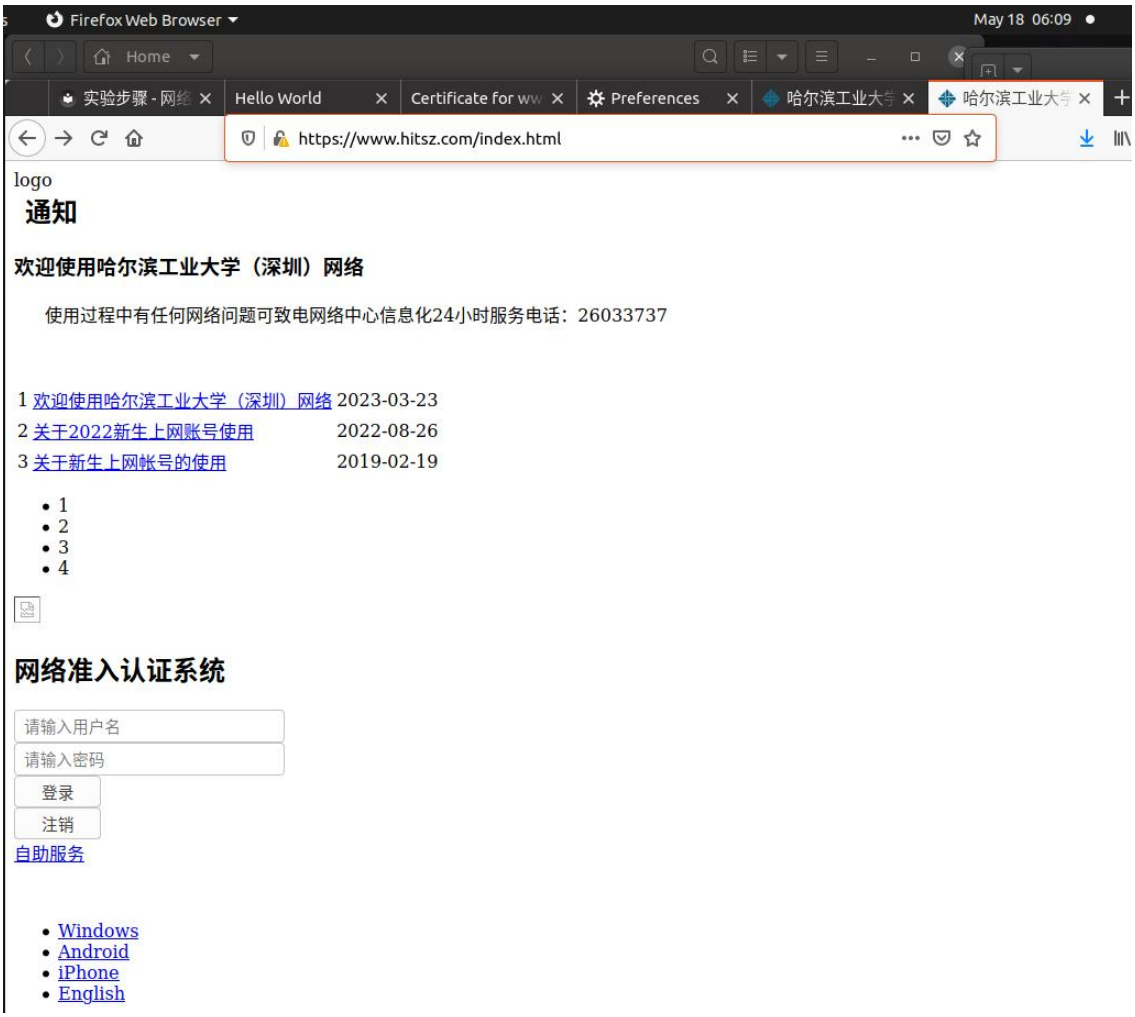
4. 将能够拦截访问一个（例如 www.hitsz.edu.cn）网站的截图和 CA 被劫持后能够正常访问的截图贴在下面。并分析说明。（建议大家随机选取一个网站，不使用 www.hitsz.edu.cn）

   我选取的网站是校园网的登陆界面，使用的网址是 www.hitsz.com

   能够拦截访问 www.hitsz.com 网站的截图如下：



CA 被劫持后能够正常访问的截图如下：



5. 分析 CA 证书各密码算法的作用。

对称加密：发送双发使用相同的密钥对消息进行加解密，常见的对称加密为 DES、3DES,AES 等。特点是效率高，但需要进行密钥分发，且无法进行身份认证。

非对称加密：发送双方各自拥有一对公钥私钥，其中公钥是公开的，私钥是保密的。当发送方向接收方发送消息时，发送方利用接收方的公钥对消息进行加密，接收方收到消息后，利用自己的私钥解密就能得到消息的明文。可以进行身份认证。非对称加密方法有 RSA、Elgamal、ECC 等。

单向散列的哈希算法：根据任意长度的数据生成固定长度的摘要，若数据稍有不同，则摘要完全不同。数据不可逆，即不能通过摘要生成数据，可以保证数据完整性。常见的方法有 sha1，md5 等。