3.1 Equivalent Assumptions (20 pts)

Consider a specific cyclic group $\mathbb{G}$ of prime order q generated by $g \in \mathbb{G}$. Show that the following problems are deterministic poly-time equivalent:

1 • Given g^{α}, g^{β}, compute $g^{\alpha\beta}$.

2 • Given g^{α}, compute g^{α^2}.

3 • Given g^{α} and $\alpha \neq 0$, compute $g^{\frac{1}{\alpha}}$.

4 • Given g^{α}, g^{β} with $\beta \neq 0$, compute $g^{\frac{\alpha}{\beta}}$.

Note that all problem instances are defined with respect to the same group $\mathbb{G}$ and generator $g \in \mathbb{G}$.

證明解決一個就可以解決其他

1 和 2 能互換

因為 $\alpha^2 = \alpha * \alpha$ ，把 2 轉成 $g^{\alpha} * g^{\alpha}$ ，用 1 的方法就能算出 $g^{\alpha\alpha}$

3 和 4 能互換

因為可以用 4 的方法算 g^1, g^{α}得到 3 要的 $g^{1/\alpha}$

1 和 4 能互換

因為可以用 3 把 g^{β}轉成 $g^{1/\beta}$

所以能解決一個就可以解決其他的

3.2 Implicit certificate (15 pts)

1. The equivalence of Alice's private and public keys. That is, prove $Q_A = aG$.

Alice 的私鑰 a 是由 QA= γ '+QCA 得出，其中 γ '=Decode(Cert)

根據證書請求協議，Cert 是由 γ 和 IDA 編碼而成的，而 γ =αG+kG

證明 QA=aG：

aG=(e'α+s)G

s=ek+c

aG=(e'α+ek+c)G

因為 e'=H(Cert)且 e=H(Cert)，因此 e'=e

aG=(eα+ek+c)G

aG=eαG+ekG+cG

由於 γ = α G+kG

aG=e γ +QCA

由於 QA= γ +QCA 且 e=H(Cert)：

QA=e γ +QCA

因此，證明了 QA=aG

2. Please show that given CA's public key Q_{CA}, without the CA secret key c, it is computationally infeasible to generate a valid certificate. The certificate is valid if $Q_A = aG$.

假設有人試圖偽造一個有效證書，他需要滿足：

1. 計算出 γ ，使得 QA= γ +QCA 成立。
2. 根據證書請求協議， γ = α G+kG，且 Cert=Encode(γ ,IDA)

要達到這一點需要：

1. 生成 Cert 並計算 e=H(Cert)：

   Cert=Encode(γ ,IDA)

2.計算 s：

   s=ek+c

但 c 是 CA 的秘鑰，只有 CA 知道。因此如果沒有 c，計算 s 是不可行的

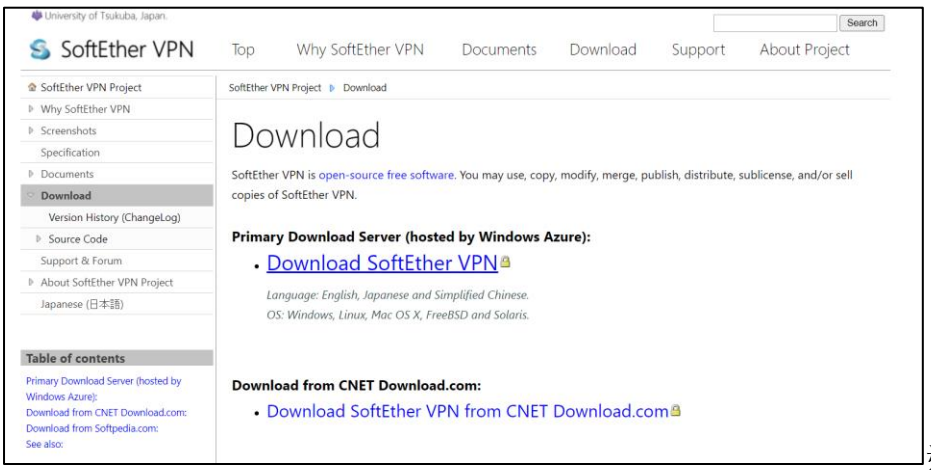
證明：

根據 s=ek+c，如果不知道 c，則無法計算 s

沒有 s，Alice 無法計算她的私鑰 a=e' α +s，因此也無法計算出對應的公鑰 QA=aG

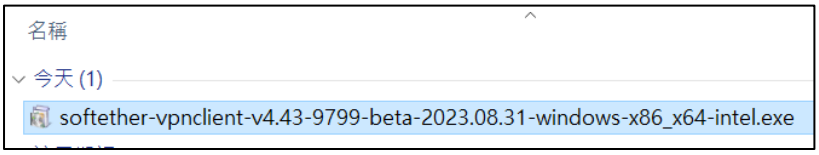
因此，給定 CA 的公鑰 QCA 而沒有 CA 的秘鑰 c，生成一個有效證書（滿足 QA=aG）在計算上是不可行的

3.3 SoftEther (25 pts)

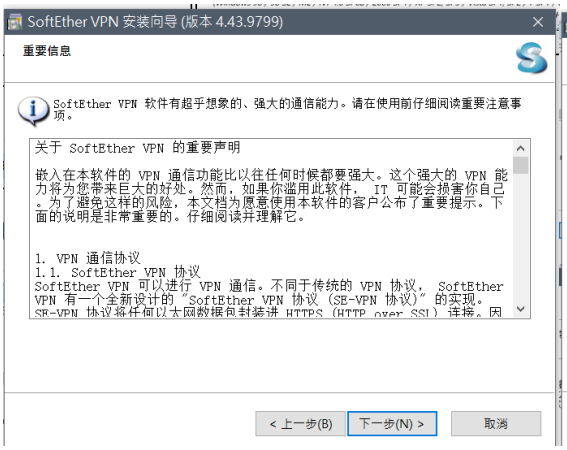


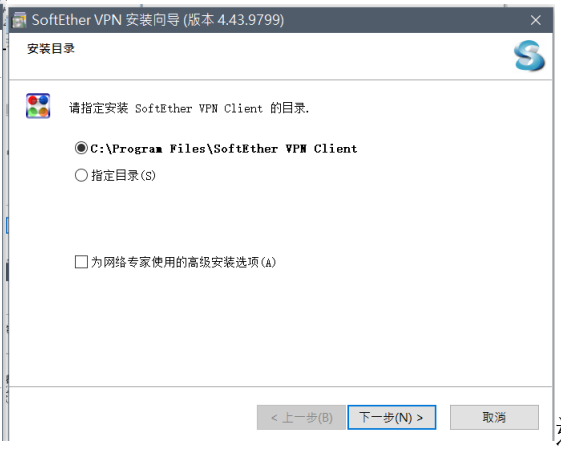
進入官網點選下載

下載最新版本



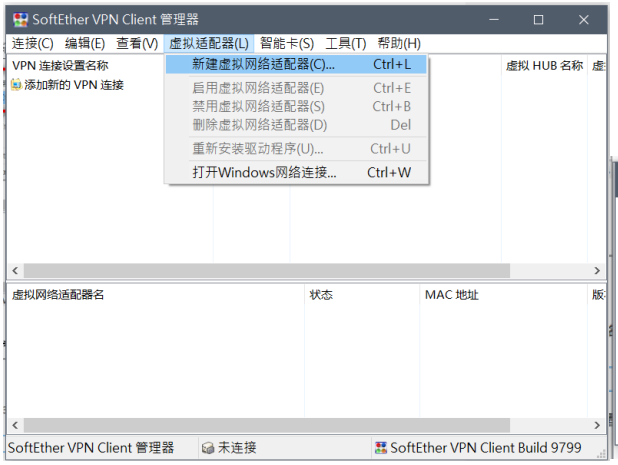
點擊安裝

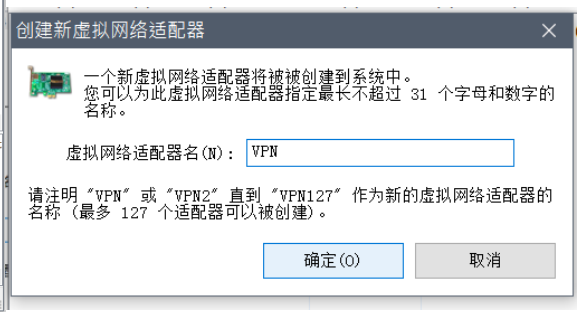


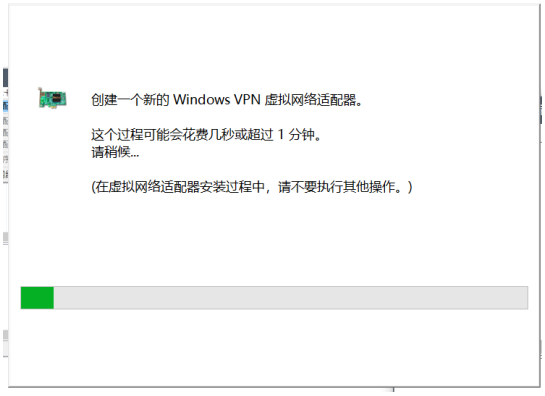


進行安裝設定

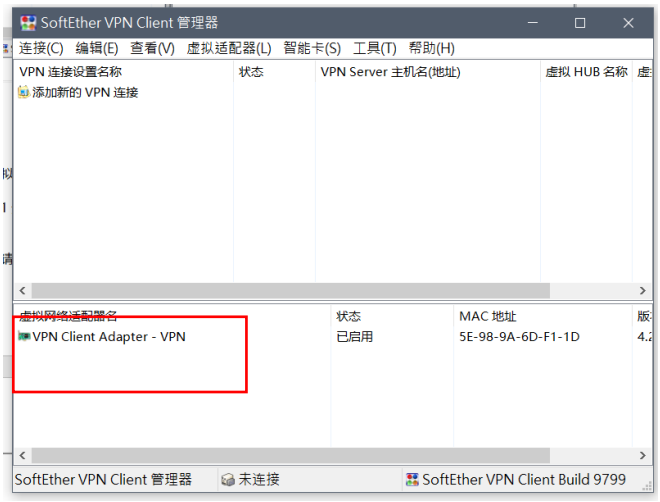
安裝完成，進入軟體



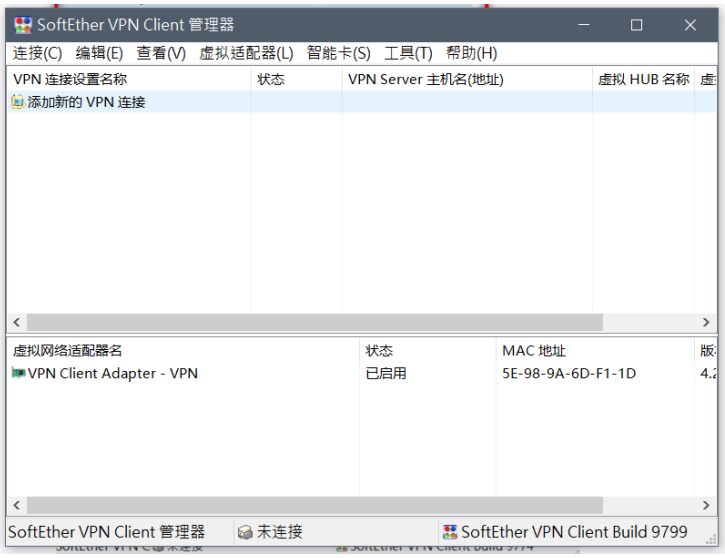




創建新的虛擬網路適配器

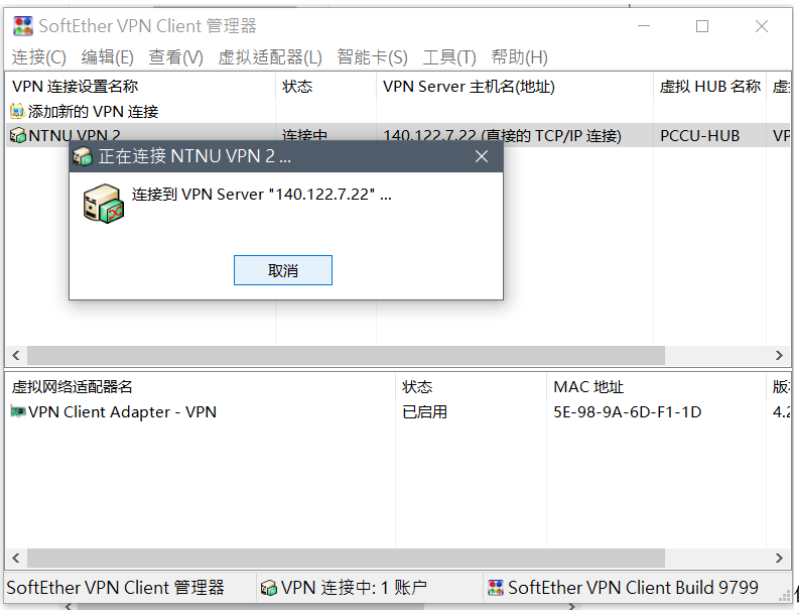


建立完畢



添加新的 VPN 連線

輸入資訊

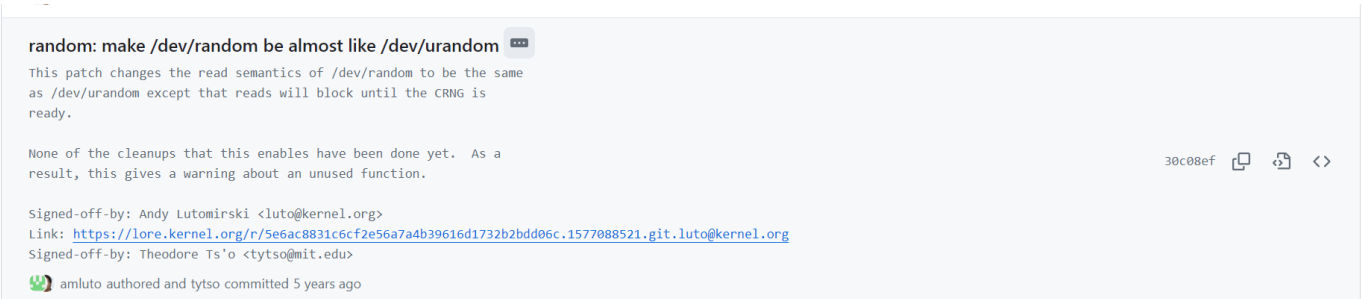


雙擊進行連接

3.4 Random Number Generator in Linux Kernel (10 pts)

Commit 在這裡

https://github.com/torvalds/linux/commit/30c08efec8884fb106b8e57094baa51bb4c44e32



3.5 Lab: MD5 Collision Attack Lab (15 pts)

Task 1: Generating Two Different Files with the Same MD5 Hash

```
seed@seedlab:/home/a0320506/Labsetup$ sudo ./md5collgen -p prefix.txt -o out1.bin out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out1.bin' and 'out2.bin'
Using prefixfile: 'prefix.txt'
Using initial value: d979dd92659a0b4d267cc4e04108cfd7

Generating first block: .
Generating second block: S11.....
Running time: 1.26914 s
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo  diff out1.bin out2.bin
Binary files out1.bin and out2.bin differ
seed@seedlab:/home/a0320506/Labsetup$ md5sum out1.bin
f36451f1f8c8cf1616eca7f899cea67f  out1.bin
seed@seedlab:/home/a0320506/Labsetup$ md5sum out2.bin
f36451f1f8c8cf1616eca7f899cea67f  out2.bin
```

Question 1. If the length of your prefix file is not multiple of 64, what is going to happen?

如果 prefix file 不是 64 的倍數，md5collgen 用 0 填充

– **Question 2.** Create a prefix file with exactly 64 bytes, and run the collision tool again, and see what happens.

```
seed@seedlab:/home/a0320506/Labsetup$ sudo ./md5collgen -p prefix.txt -o out1.bin out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out1.bin' and 'out2.bin'
Using prefixfile: 'prefix.txt'
Using initial value: ea0a10d6a708f42ec946467a5db5f498

Generating first block: ..
Generating second block: S01...
Running time: 0.86505 s
seed@seedlab:/home/a0320506/Labsetup$ sudo  diff out1.bin out2.bin
Binary files out1.bin and out2.bin differ
seed@seedlab:/home/a0320506/Labsetup$ md5sum out1.bin
00ce275f922617dfcd5ae22c4d427d40  out1.bin
seed@seedlab:/home/a0320506/Labsetup$ md5sum out2.bin
00ce275f922617dfcd5ae22c4d427d40  out2.bin
```

– **Question 3.** Are the data (128 bytes) generated by `md5collgen` completely different for the two output files? Please identify all the bytes that are different.

```
seed@seedlab:/home/a0320506/Labsetup$ hexdump -C out1.bin
00000000  48 65 6c 6c 6f 20 77 6f  72 6c 64 00 00 00 00 00  |Hello world.....|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000040  b2 1d 2a ef a6 14 12 af  57 cb 22 38 b6 6f ba 9d  |..*.....W."8.o..|
00000050  25 47 5e 97 1a e6 2c 36  09 02 82 02 d0 0f bb e9  |%G^...,6........|
00000060  4f c3 ec f4 ce cd e7 2a  eb e3 78 3a d0 5d ce bb  |O......*..x:.]..|
00000070  05 ca da da e4 23 e3 04  a3 45 c3 4e 15 43 0c c7  |.....#...E.N.C..|
00000080  c7 b5 e6 55 0a 5b 79 73  21 69 f2 b6 34 20 77 21  |...U.[ys!i..4 w!|
00000090  51 3e 15 05 2b 6d eb 5e  6e d7 ef 4f 4b 1c cb 41  |Q>..+m.^n..OK..A|
000000a0  9e 5e c9 8d 74 45 7b b7  e7 99 eb 18 99 d2 64 01  |.^..tE{.......d.|
000000b0  b0 70 57 35 cc 24 69 52  28 2c 04 d8 8d 82 14 c7  |.pW5.$iR(,......|
000000c0
seed@seedlab:/home/a0320506/Labsetup$ hexdump -C out2.bin
00000000  48 65 6c 6c 6f 20 77 6f  72 6c 64 00 00 00 00 00  |Hello world.....|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000040  b2 1d 2a ef a6 14 12 af  57 cb 22 38 b6 6f ba 9d  |..*.....W."8.o..|
00000050  25 47 5e 17 1a e6 2c 36  09 02 82 02 d0 0f bb e9  |%G^...,6........|
00000060  4f c3 ec f4 ce cd e7 2a  eb e3 78 3a d0 dd ce bb  |O......*..x:....|
00000070  05 ca da da e4 23 e3 04  a3 45 c3 ce 15 43 0c c7  |.....#...E...C..|
00000080  c7 b5 e6 55 0a 5b 79 73  21 69 f2 b6 34 20 77 21  |...U.[ys!i..4 w!|
00000090  51 3e 15 85 2b 6d eb 5e  6e d7 ef 4f 4b 1c cb 41  |Q>..+m.^n..OK..A|
000000a0  9e 5e c9 8d 74 45 7b b7  e7 99 eb 18 99 52 64 01  |.^..tE{......Rd.|
000000b0  b0 70 57 35 cc 24 69 52  28 2c 04 58 8d 82 14 c7  |.pW5.$iR(,.X....|
000000c0
```

Task 2: Understanding MD5's Property

```
seed@seedlab:/home/a0320506/Labsetup$ md5sum out1.bin
00ce275f922617dfcd5ae22c4d427d40  out1.bin
seed@seedlab:/home/a0320506/Labsetup$ md5sum out2.bin
00ce275f922617dfcd5ae22c4d427d40  out2.bin
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo echo "some more text" > additional.txt
```

```
seed@seedlab:/home/a0320506/Labsetup$ cat out1.bin additional.txt | md5sum
c965fde1d13ad9ff816263a1fa7f98ba  -
seed@seedlab:/home/a0320506/Labsetup$ cat out2.bin additional.txt | md5sum
c965fde1d13ad9ff816263a1fa7f98ba  -
```

Task 3: Generating Two Executable Files with the Same MD5 Hash

識別前綴

```
seed@seedlab:/home/a0320506/Labsetup$ sudo gcc -o task3 task3.c
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo md5sum task3
e117c52af1cc1561e11918928e7192fc  task3
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo xxd task3 | grep 4141
00003020: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003030: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003040: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003050: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003060: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003070: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003080: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003090: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030e0: 4141 4141 4141 4141 4743 433a 2028 5562  AAAAAAAAGCC: (Ub
```

0x3020 = 12320

提取前綴

```
seed@seedlab:/home/a0320506/Labsetup$ sudo head -c 12320 task3 > prefix
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo ./md5collgen prefix -o out1.bin out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out1.bin' and 'out2.bin'
Using prefixfile: 'prefix'
Using initial value: 7edd42a14d8826e933ea044a7c15a1d2

Generating first block: ...........
Generating second block: S10.........
Running time: 12.3512 s
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo cmp -lb out?.bin
12372 210 M-^H  10 ^H
12398 377 M-^? 177 ^?
12399 140 `    141 a
12412  64 4    264 M-4
12436 237 M-^_  37 ^_
12462 363 M-s  163 s
12476   2 ^B   202 M-^B
```

使用 dd 取代數據

12320+128 = 12448

```
seed@seedlab:/home/a0320506/Labsetup$ sudo dd if=out1.bin of=out1 bs=12448 count=1 conv=notrunc
1+0 records in
1+0 records out
12448 bytes (12 kB, 12 KiB) copied, 0.000278374 s, 44.7 MB/s
seed@seedlab:/home/a0320506/Labsetup$ sudo dd if=out2.bin of=out2 bs=12448 count=1 conv=notrunc
1+0 records in
1+0 records out
12448 bytes (12 kB, 12 KiB) copied, 0.000280086 s, 44.4 MB/s
```

驗證並執行修改後的二進位文件

```
seed@seedlab:/home/a0320506/Labsetup$ sudo md5sum task3 out1 out2
e117c52af1cc1561e11918928e7192fc  task3
b72891152f86e9fd125e754a74de0de9  out1
2602ffa349c3a9da120f727219115b9a  out2
```

```
seed@seedlab:/home/a0320506/Labsetup$ ./task3
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141414141
seed@seedlab:/home/a0320506/Labsetup$ ./out1
000000000000000000000000000000000b34ae157417ee9597336e11e5f7f235ecb4a8810ec9a9e11e446a2d24affed2e9abe8eedea384768
4292d5ff601ba1668d2dc7b764c4e321341973395293449 4edcb360b0c328c1a6d3aa24fcd7f399f449a121bb510e82b6088c70000000000
00000000000000000000000000000000000000000000000000000000000000000000
```

Task 4: Making the Two Programs Behave Differently

```
seed@seedlab:/home/a0320506/Labsetup$ xxd task4 | grep 4141
00003020: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003030: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003040: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003050: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003060: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003070: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003080: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003090: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030c0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030d0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000030e0: 4141 4141 4141 4141 0000 0000 0000 0000  AAAAAAAA........
00003100: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003110: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003120: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003130: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003140: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003150: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003160: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003170: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003180: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
00003190: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000031a0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000031b0: 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAA
000031c0: 4141 4141 4141 4141 4743 433a 2028 5562  AAAAAAAAGCC: (Ub
```

0x3020 = 12320

```
seed@seedlab:/home/a0320506/Labsetup$ sudo head -c 12320 task4 > prefix4
seed@seedlab:/home/a0320506/Labsetup$ sudo wc -c prefix4
12320 prefix4
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo ./md5collgen prefix4 -o task4_out1.bin task4_out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'task4_out1.bin' and 'task4_out2.bin'
Using prefixfile: 'prefix4'
Using initial value: 3c7eacca898c88720a1a3a09caf54270

Generating first block: ...........
Generating second block: W..........................
Running time: 7.95231 s
```

```
seed@seedlab:/home/a0320506/Labsetup$ ls -l prefix task4_out*
-rwxrwxrwx 1 root root 12320 May 18 03:08 prefix
-rw-r--r-- 1 root root 12480 May 18 04:27 task4_out1.bin
-rw-r--r-- 1 root root 12480 May 18 04:27 task4_out2.bin
```

```
seed@seedlab:/home/a0320506/Labsetup$ cmp -lb task4_out1.bin task4_out2.bin
12372 242 M-"   42 "
12398 223 M-^S  23 ^S
12399  63 3     64 4
12412 150 h    350 M-h
12436 247 M-'   47 '
12462   4 ^D   204 M-^D
12463 127 W    126 V
12476 171 y    371 M-y
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo tail -c 128 task4_out1.bin > P
seed@seedlab:/home/a0320506/Labsetup$ sudo tail -c 128 task4_out2.bin > Q
```

```
seed@seedlab:/home/a0320506/Labsetup$ ls -l P Q
-rwxrwxrwx 1 root root 128 May 18 04:36 P
-rwxrwxrwx 1 root root 128 May 18 04:36 Q
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo dd if=P of=task4_good bs=1 count=128 seek=12320 conv=notrunc
128+0 records in
128+0 records out
128 bytes copied, 0.000504657 s, 254 kB/s
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo dd if=Q of=task4_bad bs=1 count=128 seek=12320 conv=notrunc
128+0 records in
128+0 records out
128 bytes copied, 0.000524562 s, 244 kB/s
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo md5sum task4_good task4_bad
c041a12f3f76281693e553b1c9a5ad1c  task4_good
823d035f77149d43e9b6c97ce4e85a94  task4_bad
```

3.5 Lab: MD5 Collision Attack Lab (15 pts)

dcup -d 跑在背景

Task 1: Becoming a Certificate Authority (CA)

密碼 0000

```
seed@seedlab:/home/a0320506/Labsetup$ sudo openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
> -keyout ca.key -out ca.crt
Generating a RSA private key
.....................................................................................................
.....................................................................................++++
.....................++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:TW
State or Province Name (full name) [Some-State]:Taipei
Locality Name (eg, city) []:ws
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ntnu
Organizational Unit Name (eg, section) []:cs
Common Name (e.g. server FQDN or YOUR name) []:Tosha
Email Address []:a0320506@gmail.com
```

```
seed@seedlab:/home/a0320506/Labsetup$ openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \
> -keyout ca.key -out ca.crt \
> -subj "/CN=www.modelCA.com/O=Model CA LTD./C=US" \
> -passout pass:dees
Generating a RSA private key
.........++++
.....................................++++
writing new private key to 'ca.key'
-----
```

```
seed@seedlab:/home/a0320506/Labsetup$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7e:85:6a:a6:cb:5f:0c:34:8d:fe:52:d9:b5:7b:93:5e:22:c3:23:f6
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May 18 07:38:02 2024 GMT
            Not After : May 16 07:38:02 2034 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:aa:5a:71:25:3f:cf:4e:4b:47:44:0b:fa:36:27:
                    16:39:e5:06:97:09:4d:f9:9c:6d:f0:ea:64:dc:bc:
                    6e:09:d7:f0:c2:ea:07:4b:1f:e9:26:f6:3a:99:ae:
                    90:e5:0f:0d:98:31:f2:2a:22:fd:3e:2e:ce:e4:5e:
                    98:78:5a:ad:95:89:b5:3f:d2:30:0f:64:5c:be:06:
                    96:8b:33:24:9e:4d:d1:ad:64:5b:5f:17:7d:90:37:
                    54:cd:a5:4f:3a:89:c6:8c:33:7a:22:e4:24:98:84:
                    83:f3:01:34:c1:98:de:c0:93:32:96:07:cb:16:a0:
                    e3:58:68:9e:4a:94:cc:98:f0:1e:83:84:4c:f5:a5:
                    48:d2:ff:95:31:5d:ce:a7:87:2e:92:c8:6c:1c:9e:
                    80:01:de:2b:82:e5:dd:45:c8:ca:94:29:e3:f8:bd:
                    71:0b:c2:b3:fd:15:3c:db:50:4d:4b:e1:b0:32:ad:
                    db:32:c6:2d:d7:e6:c5:7a:54:ab:16:aa:75:96:78:
                    9a:ee:37:bc:14:fe:e8:f1:a8:a7:cb:1d:f4:ab:1e:
                    df:04:31:9b:df:b2:26:08:ec:2b:6b:7f:2b:43:84:
                    f9:7b:17:35:2b:9f:3b:da:fe:95:57:3c:db:c1:9f:
                    26:7d:53:3a:a3:70:6e:95:51:a6:9a:20:b1:b7:45:
                    0f:0e:a6:56:92:0a:57:53:ad:48:26:e8:a3:0f:8e:
```

```
                    bc:42:ae:52:94:f8:d9:b8:d9:1a:9a:13:95:a2:60:
                    33:b3:41:a1:d7:e2:04:9c:9d:46:86:d9:3d:ae:07:
                    d7:69:03:8a:c0:47:69:04:49:49:39:e2:92:cb:0c:
                    e1:98:71:42:55:f8:38:a2:95:b1:f0:fa:5a:31:54:
                    0a:70:9f:c5:a3:fa:ef:dc:77:6e:44:09:68:1d:7b:
                    8d:22:bc:7f:8a:3a:25:b6:92:78:b5:a9:5c:44:97:
                    94:d4:ba:75:bf:93:7e:4f:46:73:06:74:d2:d0:d7:
                    24:cc:1e:f4:13:53:dd:dc:8b:2f:2d:f3:34:69:b8:
                    7c:ae:47:a9:be:d6:1d:ed:8f:b1:3e:12:0f:f3:a1:
                    b4:c9:37:a2:74:8b:94:4d:fb:df:45:8d:6f:7f:17:
                    ee:5e:57:fe:2c:60:ae:2e:a2:97:ee:d7:97:19:25:
                    c1:93:10:c4:01:2e:de:b8:bd:c5:1d:15:b4:c4:d1:
                    b9:2f:79:8e:31:90:22:65:6c:bb:5a:25:e8:61:b7:
                    21:f1:d1:9e:b4:c0:33:7a:58:9a:4e:4c:1f:51:2d:
                    27:e7:17:da:42:e5:36:78:b5:28:28:18:50:c7:bc:
                    05:b8:f6:58:f3:97:d3:24:3d:ed:4c:f5:2e:51:51:
                    22:e5:e3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                B7:AA:B2:BF:56:6B:BD:73:90:71:5B:0C:C1:C9:91:DF:09:64:CB:85
            X509v3 Authority Key Identifier:
                keyid:B7:AA:B2:BF:56:6B:BD:73:90:71:5B:0C:C1:C9:91:DF:09:64:CB:85

            X509v3 Basic Constraints: critical
                CA:TRUE
```

```
    Signature Algorithm: sha256WithRSAEncryption
         42:a3:81:40:2c:94:86:68:4b:50:a6:84:03:cd:3a:02:9a:b1:
         fd:40:84:69:b9:22:32:9c:18:8c:04:ea:42:1b:e9:c8:a5:53:
         4b:a3:88:16:94:c6:cc:e5:c6:4f:f1:a9:c5:de:53:ef:9c:59:
         fd:6b:6a:85:de:e5:e3:6d:3e:75:5c:7f:26:f2:ee:d6:3e:6e:
         a5:c8:43:bb:a0:12:fa:aa:73:f0:25:ba:c6:6f:5f:07:d6:88:
         3e:07:5b:3b:bb:fa:ce:09:26:63:04:15:d0:aa:39:7f:47:3c:
         f0:35:07:fc:24:28:66:8c:82:9b:82:e4:43:03:d4:0a:34:30:
         9b:76:49:4c:56:8b:71:21:9d:31:31:b4:7a:91:02:b4:4b:ff:
         ea:de:59:96:01:73:af:42:cd:0d:59:f7:2e:66:d4:89:51:20:
         7a:5d:a1:2f:08:c7:b2:c6:88:be:ca:7f:80:83:b3:b4:2a:b3:
         47:d4:b9:ba:2e:06:62:a9:56:63:ee:c1:6d:83:dc:49:9b:af:
         14:67:d4:b3:85:35:4d:fe:91:eb:81:8c:c0:96:02:b0:44:6a:
         9a:a8:54:e2:dc:a1:c9:fe:2a:7a:c8:0b:d3:66:1d:4a:aa:d4:
         ce:76:48:24:82:2e:af:04:c6:d2:2c:52:91:1a:f6:c9:05:09:
         f5:f1:34:6c:11:73:b9:cc:83:58:9c:ad:b1:52:b8:81:f5:aa:
         96:90:ab:b6:b3:6a:92:eb:33:ef:ad:2c:ec:23:3c:36:e4:af:
         5c:5a:a5:8a:0f:87:9c:ce:4e:41:62:f6:f5:09:7a:f1:2e:90:
         f1:2e:4f:49:62:80:a5:d7:75:6f:de:98:8d:1c:a5:8e:6d:8b:
         90:80:68:17:a9:ab:20:b8:56:b5:6b:e5:17:0a:2e:34:c3:12:
         e1:77:08:7c:de:ec:60:6d:b8:e9:2f:62:7b:af:2e:1e:a7:0f:
         91:14:4f:65:30:1f:56:78:d8:89:d3:85:2b:93:78:8b:c8:0c:
         b8:a6:4d:a4:a5:8e:b3:01:47:f1:44:5e:3f:d2:00:a2:15:6c:
         9e:74:f9:16:45:35:56:b0:d4:e4:a4:9a:a7:c3:29:7f:6b:10:
         0e:d0:89:f2:29:10:3b:69:44:ed:b2:60:3c:0a:f4:9c:8a:25:
         73:e6:89:0d:ca:3b:9e:40:f0:ba:4e:07:40:e2:bb:ed:ee:e3:
         79:e3:25:88:6f:71:b5:8f:e6:a3:68:56:92:19:5b:8e:f6:7c:
         8b:15:78:e5:8c:7b:18:f5:a0:9f:89:63:b3:81:91:80:7e:d2:
         46:20:0c:e5:28:d7:53:b9:79:f9:5e:ce:fa:be:e8:44:72:a8:
         63:2f:df:48:83:51:b0:16
```

密碼 dees

```
seed@seedlab:/home/a0320506/Labsetup$ sudo openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:aa:5a:71:25:3f:cf:4e:4b:47:44:0b:fa:36:27:
    16:39:e5:06:97:09:4d:f9:9c:6d:f0:ea:64:dc:bc:
    6e:09:d7:f0:c2:ea:07:4b:1f:e9:26:f6:3a:99:ae:
    90:e5:0f:0d:98:31:f2:2a:22:fd:3e:2e:ce:e4:5e:
    98:78:5a:ad:95:89:b5:3f:d2:30:0f:64:5c:be:06:
    96:8b:33:24:9e:4d:d1:ad:64:5b:5f:17:7d:90:37:
    54:cd:a5:4f:3a:89:c6:8c:33:7a:22:e4:24:98:84:
    83:f3:01:34:c1:98:de:c0:93:32:96:07:cb:16:a0:
    e3:58:68:9e:4a:94:cc:98:f0:1e:83:84:4c:f5:a5:
```

```
    ee:5e:57:fe:2c:60:ae:2e:a2:97:ee:d7:97:19:25:
    c1:93:10:c4:01:2e:de:b8:bd:c5:1d:15:b4:c4:d1:
    b9:2f:79:8e:31:90:22:65:6c:bb:5a:25:e8:61:b7:
    21:f1:d1:9e:b4:c0:33:7a:58:9a:4e:4c:1f:51:2d:
    27:e7:17:da:42:e5:36:78:b5:28:28:18:50:c7:bc:
    05:b8:f6:58:f3:97:d3:24:3d:ed:4c:f5:2e:51:51:
    22:e5:e3
publicExponent: 65537 (0x10001)
privateExponent:
    00:8f:80:86:85:91:5e:29:9f:22:56:81:1c:72:97:
    b4:92:6a:8a:85:9a:d1:f3:ae:41:b2:cb:50:d1:dd:
    6d:78:9f:4e:72:73:40:57:99:77:07:5a:2e:7d:1d:
    5f:73:85:9d:b7:12:83:e3:d8:fb:a9:71:36:d9:8b:
    92:36:f8:73:f7:5f:3c:ae:99:79:e0:cd:73:8e:a3:
    f0:17:2c:aa:f1:2b:ae:b0:b8:b4:7b:c3:47:03:c0:
```

```
    72:b9:f5:2a:a0:09:86:2a:67:e6:c6:33:86:3d:9c:
    9e:3c:3e:8d:fb:59:56:72:b3:c9:f2:94:f1:09:98:
    3a:77:dd:f2:59:f2:d9:38:42:cc:88:b2:17:28:ed:
    6c:14:49
prime1:
    00:d3:6a:ea:7f:a1:7f:b2:b2:53:e9:79:23:4b:6c:
    f1:3e:f0:d9:c5:12:24:aa:8d:f8:e8:c5:e2:70:2f:
    06:68:75:7b:4e:34:a3:11:a3:4f:50:35:81:72:87:
    91:14:47:ba:06:e0:f6:38:12:68:f7:37:cb:59:68:
    63:d0:1a:f9:e7:8b:9c:e1:d8:6c:27:e3:bc:8d:a4:
```

```
    7c:19:a1:7b:e5:f3:83:e6:bf:1a:30:2f:c3:ec:55:
    c5:5f:a7:09:ee:8c:9a:0a:1f:ad:84:83:cf:61:2d:
    77:29:85:81:9c:11:41:44:47:b4:50:d2:08:bf:77:
    dd:f5
prime2:
    00:ce:46:b9:85:64:70:14:d0:2f:b1:d1:fa:06:e9:
    1a:d5:de:c8:06:a2:51:6b:1b:13:2c:d2:e9:a4:53:
    34:d5:e3:e6:2d:fa:b1:23:44:53:f5:a5:53:58:db:
    be:85:d3:eb:e3:59:2a:f3:1b:0f:71:7f:e1:0e:12:
    68:3c:e6:80:20:b4:2a:57:79:b4:5f:45:50:4a:7c:
    35:c9:5c:05:1c:84:3e:4c:c2:6e:f3:37:cc:17:7f:
```

```
    2a:72:90:55:f6:61:b2:a9:36:5d:a3:44:62:ff:5b:
    f7:f5:04:ee:cb:64:46:f1:09:67:1b:0f:bb:f8:3b:
    35:77
exponent1:
    00:96:07:3a:2f:a6:40:83:63:ef:0e:30:8b:ae:5b:
    b9:fa:eb:59:ee:72:88:98:8b:b5:46:22:1f:25:73:
    09:7e:19:58:8e:4f:e6:24:7f:1a:aa:95:bd:ad:b3:
    ac:6d:92:d4:dd:4a:c9:0f:53:69:2f:7e:65:8c:a5:
    fa:a6:d4:6d:e1:35:7e:f7:f9:e8:0e:8a:9a:e4:7d:
```

```
    dd:87:9a:76:fe:d4:c1:ff:4b:29:8c:6f:29:3c:11:
    d2:8d:21:93:af:57:c3:54:1b:fa:46:9c:35:df:01:
    c5:fd
exponent2:
    28:a5:83:15:27:ef:76:0a:77:fb:80:36:d6:79:c4:
    91:f4:2e:52:30:55:fe:d6:fc:f6:4e:31:3f:f2:2d:
    6d:20:55:51:26:1f:15:a5:f7:2d:66:80:7f:f7:fd:
    18:fd:e3:73:8f:34:89:67:01:aa:09:da:dd:1c:ff:
```

```
    54:58:89:d5:df:e5:48:71:2b:e5:4b:82:a5:e8:7e:
    a6:c8:8e:47:d8:84:8e:17:6a:68:2b:a7:9e:4e:0f:
    14:36:fe:9f:11:89:71:21:bb:31:77:ee:40:41:da:
    8d
coefficient:
    6d:a7:35:76:2e:d8:23:03:b6:55:e8:71:83:22:79:
    04:78:fe:ee:ef:85:63:32:a4:2e:03:2e:0e:5f:dd:
    de:e6:76:a0:96:d5:24:e5:2f:08:2c:d8:8b:1c:a6:
    56:1a:cf:b3:d2:ec:75:66:04:48:65:55:b2:35:10:
```

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

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

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

```
Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
Validity
    Not Before: May 18 07:38:02 2024 GMT
    Not After : May 16 07:38:02 2034 GMT
Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
```

Issuer 和 Subject 相同，表示這是一個自簽名憑證

- 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.

在憑證檔案中，公有指數(e)和模數(n)是公鑰的一部分，可以在 Subject Public Key Info 找到

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
        Modulus:
            00:aa:5a:71:25:3f:cf:4e:4b:47:44:0b:fa:36:27:
            16:39:e5:06:97:09:4d:f9:9c:6d:f0:ea:64:dc:bc:
            6e:09:d7:f0:c2:ea:07:4b:1f:e9:26:f6:3a:99:ae:
            90:e5:0f:0d:98:31:f2:2a:22:fd:3e:2e:ce:e4:5e:
            98:78:5a:ad:95:89:b5:3f:d2:30:0f:64:5c:be:06:
```

(中間省略)

```
        27:e7:17:da:42:e5:36:78:b5:28:28:18:50:c7:bc:
        05:b8:f6:58:f3:97:d3:24:3d:ed:4c:f5:2e:51:51:
        22:e5:e3
    Exponent: 65537 (0x10001)
```

私有指數 (d)、秘密數 (p 和 q) 通常在私鑰檔案中

d

```
privateExponent:
    00:8f:80:86:85:91:5e:29:9f:22:56:81:1c:72:97:
    b4:92:6a:8a:85:9a:d1:f3:ae:41:b2:cb:50:d1:dd:
    6d:78:9f:4e:72:73:40:57:99:77:07:5a:2e:7d:1d:
    5f:73:85:9d:b7:12:83:e3:d8:fb:a9:71:36:d9:8b:
    92:36:f8:73:f7:5f:3c:ae:99:79:e0:cd:73:8e:a3:
```

p

```
prime1:
    00:d3:6a:ea:7f:a1:7f:b2:b2:53:e9:79:23:4b:6c:
    f1:3e:f0:d9:c5:12:24:aa:8d:f8:e8:c5:e2:70:2f:
    06:68:75:7b:4e:34:a3:11:a3:4f:50:35:81:72:87:
    91:14:47:ba:06:e0:f6:38:12:68:f7:37:cb:59:68:
```

```
prime2:
    00:ce:46:b9:85:64:70:14:d0:2f:b1:d1:fa:06:e9:
    1a:d5:de:c8:06:a2:51:6b:1b:13:2c:d2:e9:a4:53:
    34:d5:e3:e6:2d:fa:b1:23:44:53:f5:a5:53:58:db:
    be:85:d3:eb:e3:59:2a:f3:1b:0f:71:7f:e1:0e:12:
```

q

Task 2: Generating a Certificate Request for Your Web Server

```
seed@seedlab:/home/a0320506/Labsetup$ sudo openssl req -newkey rsa:2048 -sha256 \
> -keyout server.key -out server.csr \
> -subj "/CN=www.bank32.com/O=Bank32 Inc./C=US" \
> -passout pass:dees \
> -addext "subjectAltName = DNS:www.bank32.com,DNS:www.bank32A.com,DNS:www.bank32B.com"
Generating a RSA private key
.....................................+++++
.........+++++
writing new private key to 'server.key'
-----
```

```
seed@seedlab:/home/a0320506/Labsetup$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.bank32.com, O = Bank32 Inc., C = US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ca:1e:83:29:9d:fb:2f:37:e6:60:c7:ae:ee:0b:
                    7b:1d:ff:0b:c1:f2:67:6e:b4:04:dc:55:06:05:b8:
                    6e:cc:6d:ed:e1:a1:40:89:78:4a:4f:70:90:b6:6d:
                    d9:c4:e0:3c:23:4b:0e:1a:b4:ec:25:dd:c5:98:45:
                    b5:0c:8d:95:a2:82:ee:5a:8b:fc:63:1f:9b:29:e7:
                    4a:87:2b:5d:17:6a:fa:54:9d:6e:30:a1:89:a0:04:
                    20:52:f2:97:4f:aa:20:e8:01:bb:85:18:60:51:0e:
                    ff:8c:62:5d:fa:fb:ce:c9:50:f2:2e:05:07:05:ef:
                    f0:0b:bb:39:0a:f0:09:60:2a:e0:85:88:59:e3:09:
                    70:ff:00:2c:d1:62:6a:97:73:d4:77:a7:0e:4c:d1:
                    c8:e5:50:bb:f9:0e:51:dd:0f:cb:a4:41:21:3e:1c:
                    72:77:d8:a9:ad:72:2b:91:25:fe:a1:94:07:74:80:
                    41:00:31:9b:63:4d:97:47:c2:40:0b:1a:ec:c7:1d:
                    cc:ae:a1:67:e1:e8:a1:9a:09:39:dc:5f:00:99:2d:
                    06:72:62:a8:6d:3e:91:db:2d:c4:8b:d5:45:0c:cc:
                    07:3b:6e:1f:96:c9:a2:d4:9b:84:88:dc:44:6c:eb:
                    e2:39:e7:2b:72:1d:64:9e:69:18:bf:92:11:33:76:
                    8b:e1
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com
```

```
Signature Algorithm: sha256WithRSAEncryption
     a1:40:f7:7c:01:eb:32:e5:e9:ad:16:b9:6b:8a:ad:5d:3f:70:
     0c:9b:0c:da:6b:51:98:d1:ae:59:87:90:36:28:7f:5c:4c:bc:
     c5:8b:c6:b0:03:f8:09:d6:19:ee:08:a9:72:c2:1b:4e:45:66:
     d1:0d:57:35:81:b7:55:f4:f4:58:a9:a1:cc:ca:6c:cd:3f:b2:
     57:46:f7:64:ba:e3:0b:4d:51:d7:2c:8e:93:5a:6b:67:1f:55:
     2e:66:9d:f3:c1:a6:9d:e0:bd:95:09:8d:7e:a2:09:65:a3:2a:
     b1:f5:6b:19:da:2c:a9:0d:89:14:aa:81:3c:88:18:89:5c:73:
     07:e6:03:ff:70:61:bd:aa:93:fb:26:c3:7d:bf:75:d1:d3:e6:
     c3:d7:a5:29:fd:ea:e5:e9:09:4b:fb:eb:51:89:74:51:ad:2c:
     3d:19:41:ef:fd:1f:5f:67:e3:77:cd:1d:e5:6a:89:96:fe:cf:
     f1:62:94:0b:c0:73:83:02:06:01:6b:f9:3a:60:0a:b7:38:df:
     f5:dc:72:09:5f:3a:02:6d:95:4a:47:60:29:d9:22:7a:1e:c9:
     db:f5:5d:80:a5:db:4a:e1:f9:e0:89:b8:9c:b3:8e:7d:a1:ac:
     df:65:f2:d1:10:8c:60:97:97:a8:fd:29:50:59:08:3d:b7:82:
     d8:6d:07:6b
```

```
seed@seedlab:/home/a0320506/Labsetup$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:ca:1e:83:29:9d:fb:2f:37:e6:60:c7:ae:ee:0b:
    7b:1d:ff:0b:c1:f2:67:6e:b4:04:dc:55:06:05:b8:
    6e:cc:6d:ed:e1:a1:40:89:78:4a:4f:70:90:b6:6d:
    d9:c4:e0:3c:23:4b:0e:1a:b4:ec:25:dd:c5:98:45:
    b5:0c:8d:95:a2:82:ee:5a:8b:fc:63:1f:9b:29:e7:
    4a:87:2b:5d:17:6a:fa:54:9d:6e:30:a1:89:a0:04:
    20:52:f2:97:4f:aa:20:e8:01:bb:85:18:60:51:0e:
    ff:8c:62:5d:fa:fb:ce:c9:50:f2:2e:05:07:05:ef:
    f0:0b:bb:39:0a:f0:09:60:2a:e0:85:88:59:e3:09:
    70:ff:00:2c:d1:62:6a:97:73:d4:77:a7:0e:4c:d1:
    c8:e5:50:bb:f9:0e:51:dd:0f:cb:a4:41:21:3e:1c:
    72:77:d8:a9:ad:72:2b:91:25:fe:a1:94:07:74:80:
    41:00:31:9b:63:4d:97:47:c2:40:0b:1a:ec:c7:1d:
    cc:ae:a1:67:e1:e8:a1:9a:09:39:dc:5f:00:99:2d:
    06:72:62:a8:6d:3e:91:db:2d:c4:8b:d5:45:0c:cc:
    07:3b:6e:1f:96:c9:a2:d4:9b:84:88:dc:44:6c:eb:
    e2:39:e7:2b:72:1d:64:9e:69:18:bf:92:11:33:76:
    8b:e1
publicExponent: 65537 (0x10001)
```

```
privateExponent:
    00:a8:ec:f3:86:b6:e9:16:bf:cb:a6:1b:7e:52:a9:
    f9:ce:4a:39:93:71:7b:8d:04:9c:03:62:74:54:17:
    9f:52:f0:95:9e:bc:5c:ea:08:45:63:3b:9b:57:3d:
    5c:82:b5:3e:cd:e8:8e:f3:37:3f:1f:2e:c9:54:c8:
    fd:d6:6e:07:1f:f9:fa:28:67:53:1b:ad:70:cb:86:
    e9:bd:2b:3a:f4:b5:8e:5f:65:ec:90:6c:92:4f:d0:
    e3:0b:30:81:d2:2d:48:af:5f:b3:50:3b:dd:54:22:
    0a:e7:53:d7:64:4b:4c:ba:e9:12:5f:f0:07:bc:a8:
    9a:a1:d3:6a:8b:7f:ae:f6:55:a1:d3:f9:90:5f:7f:
    77:90:b8:22:b7:3b:ee:2d:b3:d4:96:06:74:77:b2:
    6e:6b:0a:50:f5:2e:a9:12:22:a5:17:78:22:fe:72:
    f2:ab:45:23:95:b4:9f:99:61:be:5a:09:07:91:01:
    48:58:71:98:33:06:d1:5d:ec:83:ab:6f:1e:f3:07:
    e1:7f:30:3e:36:76:45:c8:65:81:0d:a3:2e:56:fe:
    f5:2c:1a:80:c5:40:7c:bd:51:f6:e8:5d:3f:93:4c:
    a8:79:27:b2:89:47:3d:16:4e:47:9d:9b:39:4d:02:
    8a:0c:de:d5:7b:3c:cf:89:5e:9a:90:74:3c:37:7a:
    c5:21
```

```
prime1:
    00:f9:6f:fc:07:3e:7e:58:65:29:6b:e9:2c:8c:74:
    99:55:1f:8f:a2:94:f3:7b:3c:ee:1b:ab:19:98:53:
    42:67:82:f3:74:0b:17:1d:31:00:50:8e:d9:d7:f0:
    ad:14:3d:26:22:da:2e:74:e3:09:1b:32:96:7a:98:
    4c:dc:9d:75:4c:88:e4:11:eb:d3:65:0b:47:c1:7d:
    e8:24:4b:81:61:26:ba:d7:c4:e8:f5:7c:83:d4:dc:
    8e:12:e0:7a:d3:e9:d9:06:c3:c2:6b:93:d5:5e:ee:
    40:5f:40:ab:f4:70:7e:2d:3e:8a:09:5e:56:c7:9e:
    9f:f4:df:9b:57:64:f3:4e:c5
prime2:
    00:cf:6f:d4:42:72:aa:73:b5:cc:74:8a:7a:e2:10:
    56:08:5c:46:38:ae:1f:c3:6b:87:93:ad:aa:b3:62:
    48:4b:b1:f8:0d:21:45:2b:db:60:b6:fe:15:5c:b1:
    a3:2d:48:b7:81:a4:02:47:fa:99:cc:7d:b4:b5:39:
    49:ba:65:cf:61:23:2b:82:6f:f0:bb:02:47:6b:30:
    2e:d6:44:c4:40:fa:fa:99:56:46:29:81:54:53:bb:
    ba:d4:28:fb:a3:ce:87:e6:33:ad:1b:53:2c:eb:31:
    b5:8e:16:31:c1:cf:39:8a:fe:e4:9d:38:8c:2b:49:
    35:ac:9d:4f:f6:98:46:1a:6d
```

```
exponent1:
    00:b6:cd:0f:f9:cb:1d:d2:f0:48:5b:f2:25:98:c5:
    b6:bd:80:84:c6:54:bc:df:9b:36:b1:06:42:9a:b4:
    a1:dc:b4:46:70:cb:d3:e3:ab:ce:9c:3b:24:81:31:
    bb:d6:32:3e:29:9a:96:23:49:63:9a:10:07:e1:ce:
    8d:bd:bc:93:83:44:6b:48:8a:f8:80:7b:b4:d9:a3:
    c9:26:18:43:b8:0c:27:30:0b:f9:e2:36:9f:72:b7:
    34:53:b7:39:ac:e6:1b:0b:ef:19:23:b7:d2:ce:60:
    72:c2:9b:e5:a9:1d:6c:0b:02:63:2d:1c:7b:22:8e:
    28:91:cf:f1:cb:29:8b:7a:35
exponent2:
    04:a1:73:74:94:48:b7:d2:8c:20:e1:e2:82:5f:68:
    fc:40:cb:14:82:d6:94:af:36:d4:96:20:e4:66:42:
    44:e6:51:2a:41:de:e0:6e:c2:46:f3:7f:18:95:a2:
    95:e5:34:ab:81:34:c7:d4:91:50:5e:52:05:65:a4:
    fe:b3:3d:20:e6:ff:16:a7:57:11:65:a8:a0:7c:ef:
    de:ba:a4:42:eb:17:63:0a:e9:00:0e:32:0a:b8:7b:
    20:37:55:fe:bf:22:8b:82:05:d0:41:58:14:5c:04:
    b8:8a:48:4c:12:4b:2f:8e:27:1e:57:5f:d1:ab:8d:
    b6:2f:c0:d4:39:6b:ff:35
```

```
coefficient:
    00:89:90:36:37:48:3d:0f:43:3f:d8:36:5f:3e:25:
    a7:c1:1e:72:de:77:20:6e:15:01:2b:74:95:70:c1:
    d8:54:12:38:39:6d:10:c8:c8:e4:56:b3:30:52:88:
    48:0e:ce:64:ca:42:ec:41:55:5c:9b:0b:49:14:90:
    e0:ca:05:2a:95:9d:1c:2f:82:04:4c:47:db:16:d1:
    f1:eb:8f:e9:01:8a:e3:27:be:ca:25:7b:54:a9:45:
    37:0b:ba:4d:95:4b:2e:bc:8b:a8:8f:86:40:1c:75:
    1a:f0:2f:cf:10:31:b6:95:cf:81:c9:e2:64:3d:84:
    42:eb:b2:ca:2d:5f:96:f2:89
```

Task 3: Generating a Certificate for your server

```
seed@seedlab:/home/a0320506/Labsetup$ sudo cp /usr/lib/ssl/openssl.cnf ./openssl.cnf
```

```
seed@seedlab:/home/a0320506/Labsetup$ sudo openssl ca -config myCA_openssl.cnf -policy policy_anything \
> -md sha256 -days 3650 \
> -in server.csr -out server.crt -batch \
> -cert ca.crt -keyfile ca.key
Using configuration from myCA_openssl.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: May 18 08:58:05 2024 GMT
            Not After : May 16 08:58:05 2034 GMT
        Subject:
            countryName               = US
            organizationName          = Bank32 Inc.
            commonName                = www.bank32.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                E1:13:0A:F3:14:BB:82:8A:42:F9:DD:E9:D6:D1:71:31:EF:38:52:3E
            X509v3 Authority Key Identifier:
                keyid:B7:AA:B2:BF:56:6B:BD:73:90:71:5B:0C:C1:C9:91:DF:09:64:CB:85

Certificate is to be certified until May 16 08:58:05 2034 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

```
seed@seedlab:/home/a0320506/Labsetup$ 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 08:58:05 2024 GMT
            Not After : May 16 08:58:05 2034 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:fc:8f:3f:de:0b:e5:81:e0:32:0b:a8:15:09:2a:
                    c7:98:5a:d6:9d:a2:37:e8:00:af:51:58:3b:d5:3c:
                    a1:15:18:67:51:b0:39:00:6d:68:3e:f4:e8:c3:87:
                    da:c4:61:46:b9:98:61:26:05:c5:be:b8:06:9c:06:
                    3c:82:94:2e:71:6b:84:e8:c3:9d:5e:5c:db:f7:51:
                    20:8b:b9:5b:8c:38:fb:46:7a:6f:ac:49:1d:6c:c8:
                    16:53:5b:0a:2a:1d:08:7d:d4:a5:ab:ac:35:0f:1e:
                    46:07:fd:71:0c:80:a3:21:c5:00:91:89:15:f2:a7:
                    e8:7f:d1:3f:76:a0:43:fc:dd:9e:be:41:65:97:45:
                    76:05:c6:be:00:51:a3:a0:17:13:09:d8:41:65:d6:
                    f7:9f:0a:a3:9b:ed:fa:11:3a:85:0d:88:5c:83:39:
                    b3:e3:8e:9b:2f:9f:44:73:c3:35:e7:2d:c4:93:4a:
                    03:ed:57:d3:1f:11:4a:94:4c:c9:4f:d4:ea:36:45:
                    13:0b:ab:47:a3:97:ff:ec:92:f6:89:b1:f3:ea:4f:
                    09:96:68:0f:ef:6b:84:d4:12:22:3b:78:24:ac:b6:
                    09:73:12:c8:f4:3e:95:d5:4f:5a:98:51:77:b5:4e:
                    55:03:a8:16:8a:aa:d2:8e:71:a5:f3:3b:6b:2d:c1:
                    b9:49
                Exponent: 65537 (0x10001)
```

```
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            E1:13:0A:F3:14:BB:82:8A:42:F9:DD:E9:D6:D1:71:31:EF:38:52:3E
        X509v3 Authority Key Identifier:
            keyid:B7:AA:B2:BF:56:6B:BD:73:90:71:5B:0C:C1:C9:91:DF:09:64:CB:85

Signature Algorithm: sha256WithRSAEncryption
     31:23:15:92:e2:de:b7:bd:1e:b3:e1:90:7c:53:19:f8:cd:08:
     20:7d:17:3d:d5:9c:28:7a:0e:2b:40:20:81:89:8e:44:15:07:
     53:76:51:20:ab:b6:22:41:c0:02:d7:41:5d:d5:9d:2a:8d:6e:
     a7:da:6e:32:77:52:8c:af:eb:5b:0f:90:b4:51:c9:c2:df:8c:
     c2:6c:2d:45:e6:9e:81:8f:c1:5a:44:c5:2f:2d:f9:30:d8:ff:
     8a:a4:2a:a1:8d:1d:75:ab:a3:95:df:c5:64:55:22:1b:4a:14:
     06:15:18:29:f4:4b:e9:61:40:a6:7c:c7:d7:f7:7e:05:d8:c0:
     91:eb:b5:bf:5f:d2:55:a7:5f:9e:0b:72:f9:fe:3f:cf:92:98:
     13:6c:c5:eb:2c:54:20:27:d2:0e:bd:88:92:f9:24:9c:56:9f:
     51:75:00:79:bf:d3:bd:81:18:4b:03:7c:a6:95:ec:ad:a5:e9:
     53:de:21:50:f9:72:f9:e5:d7:fd:79:00:04:b9:17:8a:50:87:
     90:97:61:f6:31:ff:f7:91:48:1b:c4:1c:8f:05:1c:e6:98:45:
     c7:9a:2c:91:f7:9b:a2:e0:ba:4b:91:85:17:82:75:40:68:e2:
     7d:2d:e1:b9:a5:ba:30:1a:2a:76:5e:0f:83:9b:b6:21:c5:68:
     ca:b2:70:59:bf:df:38:e9:11:90:8c:30:e3:1d:d8:96:af:8e:
```

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

```
seed@seedlab:/home/a0320506/Labsetup$ a2ensite bank32_apache_ssl
ERROR: Site bank32_apache_ssl does not exist!
seed@seedlab:/home/a0320506/Labsetup$ service apache2 start
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to start 'apache2.service'.
Authenticating as: Ubuntu (ubuntu)
Password:
polkit-agent-helper-1: pam_authenticate failed: Authentication failure
==== AUTHENTICATION FAILED ===
Failed to start apache2.service: Access denied
See system logs and 'systemctl status apache2.service' for details.
```

網頁無法開啟