

For printing the certificate cert is filename

openssl x509 -in cert -text -noout

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 12345 (0x3039)

Signature Algorithm: md2WithRSAEncryption

Issuer: CN = PicoCTF

Validity

Not Before: Jul 8 07:21:18 2019 GMT

Not After : Jun 26 17:34:38 2019 GMT

Subject: OU = PicoCTF, O = PicoCTF, L = PicoCTF, ST = PicoCTF, C = US, CN = PicoCTF

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (53 bit)

Modulus: 4966306421059967 (0x11a4d45212b17f)

Exponent: 65537 (0x10001)

Signature Algorithm: md2WithRSAEncryption

Signature Value:

07:6a:5d:61:32:c1:9e:05:bd:eb:77:f3:aa:fb:bb:83:82:eb:

9e:a2:93:af:0c:2f:3a:e2:1a:e9:74:6b:9b:82:d8:ef:fe:1a:

c8:b2:98:7b:16:dc:4c:d8:1e:2b:92:4c:80:78:85:7b:d3:cc:

b7:d4:72:29:94:22:eb:bb:11:5d:b2:9a:af:7c:6b:cb:b0:2c:

a7:91:87:ec:63:bd:22:e8:8f:dd:38:0e:a5:e1:0a:bf:35:d9:

a4:3c:3c:7b:79:da:8e:4f:fc:ca:e2:38:67:45:a7:de:6e:a2:

6e:71:71:47:f0:09:3e:1b:a0:12:35:15:a1:29:f1:59:25:35:

a3:e4:2a:32:4c:c2:2e:b4:b5:3d:94:38:93:5e:78:37:ac:35:

35:06:15:e0:d3:87:a2:d6:3b:c0:7f:45:2b:b6:97:8e:03:a8:

d4:c9:e0:8b:68:a0:c5:45:ba:ce:9b:7e:71:23:bf:6b:db:cc:

8e:f2:78:35:50:0c:d3:45:c9:6f:90:e4:6d:6f:c2:cc:c7:0e:

de:fa:f7:48:9e:d0:46:a9:fe:d3:db:93:cb:9f:f3:32:70:63:

cf:bc:d5:f2:22:c4:f3:be:f6:3f:31:75:c9:1e:70:2a:a4:8e:

43:96:ac:33:6d:11:f3:ab:5e:bf:4b:55:8b:bf:38:38:3e:c1:

25:9a:fd:5f

The screenshot shows the 'Integer factorization calculator' website. The main interface includes a 'Value' input field containing '4966306421059967', a set of 'Actions' buttons (Only evaluate, Is prime?, Factor, Help, Config, Open wizard, From file, Blockly mode, Clear input), and a 'Functions' section with buttons for mathematical operations. Below the input field, it displays the prime factorization:  $4966\ 306421\ 059967 = 67\ 867967 \times 73\ 176001$ . Other statistics shown are: Number of divisors: 4, Sum of divisors: 4966 306562 103936, Euler's totient: 4966 306280 016000, Möbius: 1, and the equation  $n = a^2 + b^2 + c^2 + d^2$  with  $a = 59\ 898021$ . A terminal window is open over the website, showing the command `openssl x509 -in cert -text -noout` and the resulting certificate details for 'PicoCTF'.

```
root@kali: /home/kali/Desktop/pico reverse/cert
(kali@kali)~ /Desktop/pico reverse/cert
$ sudo su
[sudo] password for kali:
$ (root@kali)~ /home/kali/Desktop/pico reverse/cert
$ openssl x509 -in cert -text -noout
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 12345 (0x3039)
    Signature Algorithm: md2WithRSAEncryption
    Issuer: CN = PicoCTF
    Validity
      Not Before: Jul  8 07:21:18 2019 GMT
      Not After : Jun 26 17:34:38 2019 GMT
    Subject: OU = PicoCTF, O = PicoCTF, L = PicoCTF, ST = PicoCTF, C = US, CN = PicoCTF
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (53 bit)
        Modulus:
          4966306421059967 (0x11a4d45212b17f)
        Exponent: 65537 (0x10001)
    Signature Algorithm: md2WithRSAEncryption
    Signature Value:
      07:6a:5d:61:32:c1:9e:05:bd:eb:77:f3:aa:fb:bb:83:82:eb:
```

<https://www.alpertron.com.ar/ECM.HTM>

This screenshot shows the same website but with the 'Functions' section expanded. It includes buttons for mathematical operations like FloorDiv, Mod, ModInv, ModDiv, ModPow, Totient, and Jacobi. The 'Value' input field still contains '4966306421059967'. The prime factorization and other statistics remain the same as in the previous screenshot.