Description

Sometimes RSA certificates are breakable

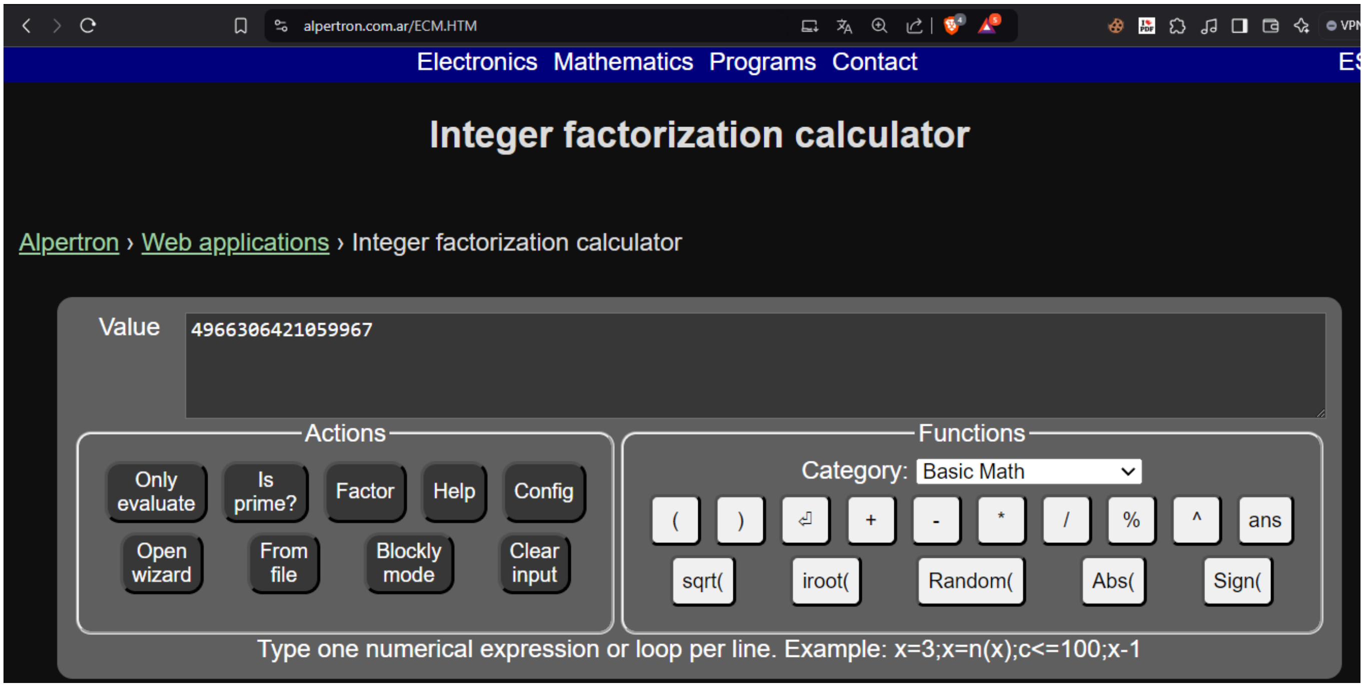
Hints

- The flag is in the format picoCTF{p,q}
- Try swapping p and q if it does not work

Solución

```
┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$ ls
cert  john_pollard.md

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$ file cert
cert: PEM certificate

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$ cat cert
-----BEGIN CERTIFICATE-----
MIIB6zCB1AICMDkwDQYJKoZIhvcNAQECBQAwEjEQMA4GA1UEAxMHUGljb0NURjAe
Fw0xOTA3MDgwNzIxMThaFw0xOTA2MjYxNzM0MzhaMGcxEDAOBgNVBAsTB1BpY29D
VEYxEDAOBgNVBAoTB1BpY29DVEYxEDAOBgNVBAcTB1BpY29DVEYxEDAOBgNVBAgT
B1BpY29DVEYxCzAJBgNVBAYTAlVTMRAwDgYDVQQDEwdQaWNvQ1RGMCIwDQYJKoZI
hvcNAQEBBQADEQAwDgIHEaTUUhKxfwIDAQABMA0GCSqGSIb3DQEBAgUAA4IBAQAH
al1hMsGeBb3rd/Oq+7uDguueopOvDC864hrpdGubgtjv/hrIsph7FtxM2B4rkkyA
eIV708y31HIplCLruxFdspqvfGvLsCynkYfsY70i6I/dOA6l4Qq/NdmkPDx7edqO
T/zK4jhnRafebqJucXFH8Ak+G6ASNRWhKfFZJTWj5CoyTMIutLU9lDiTXng3rDU1
BhXg04ei1jvAf0UrtpeOA6jUyeCLaKDFRbrOm35xI79r28yO8ng1UAzTRclvkORt
b8LMxw7e+vdIntBGqf7T25PLn/MycGPPvNXyIsTzvvY/MXXJHnAqpI5DlqwzbRHz
q16/S1WLvzg4PsElmv1f
-----END CERTIFICATE-----

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$ openssl x509 -pubkey -in cert -out cert.pub

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$ openssl rsa -pubin -in cert.pub
writing RSA key
-----BEGIN PUBLIC KEY-----
MCIwDQYJKoZIhvcNAQEBBQADEQAwDgIHEaTUUhKxfwIDAQAB
```

```
-----END PUBLIC KEY-----

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$ openssl rsa -pubin -in cert.pub -text
Public-Key: (53 bit)
Modulus: 4966306421059967 (0x11a4d45212b17f)
Exponent: 65537 (0x10001)
writing RSA key
-----BEGIN PUBLIC KEY-----
MCIwDQYJKoZIhvcNAQEBBQADEQAwDgIHEaTUUhKxfwIDAQAB
-----END PUBLIC KEY-----

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_01_crypto_01/john_pollard]
└─$
```

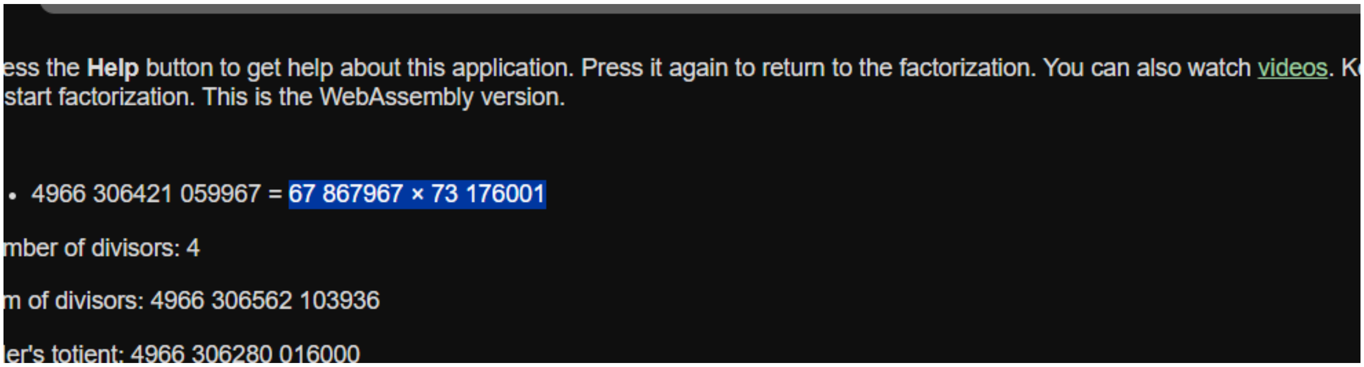


Integer factorization calculator

Alpertron › Web applications › Integer factorization calculator

Value 4966306421059967

Type one numerical expression or loop per line. Example: x=3;x=n(x);c<=100;x-1



ess the **Help** button to get help about this application. Press it again to return to the factorization. You can also watch videos. K
start factorization. This is the WebAssembly version.

- 4966 306421 059967 = 67 867967 × 73 176001

mber of divisors: 4

m of divisors: 4966 306562 103936

ler's totient: 4966 306280 016000

Bandera

```
flag: picoCTF{73176001,67867967}
```

Notas Adicionales

Referencias

- Calculadora-Factores