

TAREA-2 Criptoanálisis de criptografía híbrida con DHKE

Extraemos del certificado del Comand-and-Control la llave publica, el primo y el generador

```
TAREA-2 — zsh — 112x43
rajkit@RAJKIT TAREA-2 % openssl pkey -pubin -in dhpublishCC.cer -text -noout
PKCS#3 DH Public-Key: (1024 bit)
public-key:
    1d:12:bb:62:34:4d:ac:6d:b5:e1:0c:9d:f4:45:72:
    64:62:65:df:ce:9c:7d:59:a9:a0:2a:7d:88:09:6d:
    64:43:47:39:58:6f:e3:2a:c8:bb:31:5e:a1:f3:2e:
    5c:1a:0a:4a:ff:db:5c:13:ae:f5:3d:07:44:48:ae:
    67:56:8c:a0:3a:69:96:30:34:97:38:61:18:b3:1c:
    1d:1c:29:2a:72:fd:44:eb:7f:f4:34:1d:49:6b:f0:
    11:bf:5a:5b:e0:aa:9b:1a:68:4d:00:d7:9c:e4:e4:
    da:a7:50:47:79:f2:90:7f:bf:3f:e2:02:73:e0:b0:
    80:a7:c5:10:f6:71:9c:aa
prime:
    00:ef:04:06:4e:89:29:35:71:2a:d8:82:11:ba:6c:
    1a:9e:58:a8:45:c7:dc:3e:b5:3d:13:95:7c:20:0e:
    94:6a:f4:94:54:76:7f:fd:45:d1:4a:74:2c:84:09:
    27:df:2e:d7:6c:83:dc:50:f5:ac:2b:45:8d:6b:ed:
    32:a7:a1:bf:4a:12:29:78:38:c5:eb:54:21:e8:f5:
    a7:c5:53:77:12:69:d2:54:4e:29:8b:d1:2f:10:47:
    40:e7:52:13:45:f1:73:2e:f3:f4:d6:b7:d6:fe:94:
    33:85:c9:74:54:d4:68:6d:94:6b:38:80:7a:b3:d8:
    b4:3a:0d:e5:2f:df:69:57:17
generator: 5 (0x5)
rajkit@RAJKIT TAREA-2 %
```

El numero primo usado de 1024bits es vulnerable a algoritmo de Pohlig-Hellman y permite resolver el problema de logaritmo discreto.

```
g=5
h=0x1d12bb62344dac6db5e10c9df44572646265dfce9c7d59a9a02a7d88096d64434739586fe32ac8b1
p=0x00ef04064e892935712ad88211ba6c1a9e58a845c7dc3eb53d13957c200e946af49454767ffd45d
print('El primo p es', p)
F=GF(p)
g1=F(g)
h1=F(h)
N=p-1
qi=[r^N.valuation(r) for r in prime_divisors(N)]
print('Los divisores de p-1: ',qi)
lqi=len(qi)
Nqi=[N/q for q in qi]
gi=[g1^r for r in Nqi]
hi=[h1^r for r in Nqi]
xi=[discrete_log(hi[i],gi[i]) for i in range(lqi)]
print('Logaritmos discretos x i=',xi)
x=CRT(xi,qi)
print('El resultado es log g(h)=' ,x)
```

Nos devuelve:

0x67ECB71B030AC696DD6C244E197BBF91BAD4A1DF53892B383F03247A3FAFF905E886169515CC9A94323BBAEF1F8675E5CBAA87DBCE664F4565265D19A46C590462A1AC5791262DA063DDA5450E686D6EE5672134A6B6DCC14E1FEB52C6691BA0992D3E1ABCD1011BE7A8DDB1AF9DDBBB01601CEB43BA8E710211F876FBDD2011

Aplicando el anterior algoritmo hemos obtenido la private-key, con los datos que ya tenemos generamos un certificado con la llave privada:


```
TAREA-2 — -zsh — 112x43
rajkit@RAJKIT TAREA-2 % openssl pkeyutl -derive -inkey dhCC.pem -peerkey dhpública.cer -out secretoGON.bin
rajkit@RAJKIT TAREA-2 % hexdump secretoGON.bin
00000000 abc9 1b9d e6b9 e013 7a8d 6847 8aa2 85f6
00000010 f6d0 d634 6384 fa8c a504 fc8d 69e7 4bcf
00000020 12ad 34e5 b407 ede3 c8e7 f167 b601 6f6a
00000030 314f 406a 5b89 422d e594 55e0 0c99 3409
00000040 aa1d 6a7c 2058 a7a3 9e40 d289 3076 1cf3
00000050 777e b04a b0cc bf47 e2c0 a717 ddb5 70dc
00000060 c19a cfa3 c7b4 0931 b84f e98a 17e2 1704
00000070 efb7 30c5 2b43 f816 9593 d239 4905 0511
00000080
rajkit@RAJKIT TAREA-2 %
```

Una vez tenemos el secreto compartido, generamos una clave de 32bytes usando una funcion hash SHA2-256 sin SALT y con una etiqueta info: “shared key”

```
openssl kdf -keylen 32 -kdfopt digest:SHA-256 -kdfopt
hexkey:C9AB9D1BB9E613E08D7A4768A28AF685D0F634D684638CFA04A58DFCE769CF4BA
D12E53407B4E3EDE7C867F101B66A6F4F316A40895B2D4294E5E055990C09341DAA7C6A58
20A3A7409E89D27630F31C7E774AB0CCB047BFC0E217A7B5DDDC709AC1A3CFB4C731094
FB88AE9E2170417B7EFC530432B16F8939539D205491105 -kdfopt info:"shared key" hkdf
```

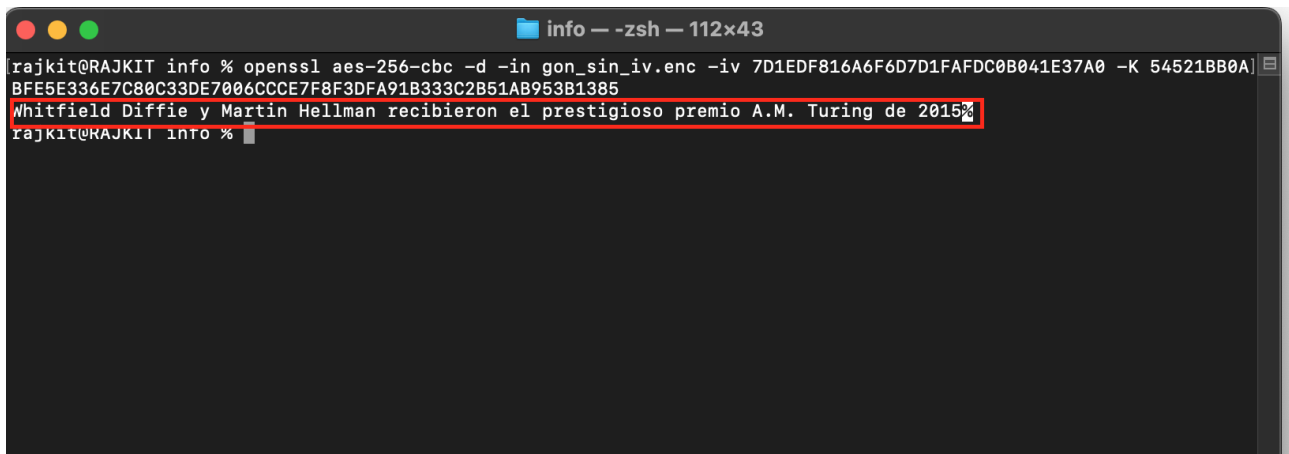
La clave generada a partir del secreto compartido es:

```
0x54521BB0ABFE5E336E7C80C33DE7006CCCE7F8F3DFA91B333C2B51AB953B1385
```

Una vez obtenida la clave procedemos a extraer los primeros 16bytes del archivo gon.enc que contienen el Vector de inicialicacion con el que el malware a encriptado el archivo con AES-256-CBC

```
0x7D1EDF816A6F6D7D1FAFDC0B041E37A0
```

Por ultimo con todos los datos necesarios sobre la mesa descryptamos el archivo con los primeros 16bytes extraidos:



```
info — zsh — 112x43
rajkit@RAJKIT info % openssl aes-256-cbc -d -in gon_sin_iv.enc -iv 7D1EDF816A6F6D7D1FAFDC0B041E37A0 -K 54521BB0A
BFE5E336E7C80C33DE7006CCCE7F8F3DFA91B333C2B51AB953B1385
Whitfield Diffie y Martin Hellman recibieron el prestigioso premio A.M. Turing de 2015
rajkit@RAJKIT info %
```