# CriptoReto. El alienígena

*"A veces pienso que la prueba más fehaciente de que existe vida inteligente en el universo es que nadie ha intentado contactar con nosotros."*

***Bill Watterson***

Antes de huir hacia un destino desconocido, de paso por Madrid y temiendo por su vida, un investigador de la NASA deja en la estación del metro de Atocha un papel con 4 criptogramas, una figura que se asemeja a un alienígena, el número +300. Investigadores de la policía llegan a la conclusión de que podría tratarse de una pista sobre la fecha de llegada a nuestro mundo de alienígenas, supuestamente un viernes, y se proponen descubrir qué misterio hay detrás de esos cuatro criptogramas.

**Criptograma 1:**

DWÑSDWFSBOUÑDHYDZOAHQMÑEÑEYLOEMSCINUHJMSQIFLDKOFCSW
KHTÑHFVUEZCNWFYCKZZUFYEHVÑIHMTVYMÑJZXEEUSZFVTAGWUBG
WUBFVTAEUSZJZXE

**Criptograma 2:**

bCx4ZmbFBkLywi1EopC/O3YFyziPHJc0LeeNpD8dPF0o1u9mvwWpCTwAVknYfK
3u

**Criptograma 3:**

ACAB3A5DD339ED41F92709367A324E744DAAC74CF1419108FAA93194069B66
F0A3AF2E3C7B273353

**Criptograma 4:**

192685F83D5D9C7113EA36FD838C5D2D

Tras un análisis estadístico, por la frecuencia de letras, da la impresión de que el criptograma 1 se trata de una cifra elemental, es el punto de partida. ¿Serán estos mensajes cifrados la prueba definitiva de la existencia de vida extraterrestre? ¿Dónde y cuándo aterrizarán?

Design by
Dr. Jorge Ramió/Dr. Alfonso Muñoz
@criptored, @mindcrypt

**Posible Solución:**

El criptoreto, y por tanto su premio, queda desierto al no haberse comunicado a Criptored ninguna solución completa al mismo. A continuación, adjuntamos una de las posibles soluciones al criptoreto. Cualquier duda o comentario pueden escribirnos a la información de contacto adjuntada.

**Criptograma 1:**

DWÑSDWFSBOUÑDHYDZOAHQMÑEÑEYLOEMSCINUHJMSQIFLDKOFCSW
KHTÑHFVUEZCNWFYCKZZUFYEHVÑIHMTVYMÑJZXEEUSZFVTAGWUBG
WUBFVTAEUSZJZXE

El criptograma 1 es un cifrado clásico (pista dada) del que puede deducirse que posiblemente se trate de una cifra de Vigenère. Por ejemplo, utilizando el programa CriptoclasicosV2.1 (http://www.criptored.upm.es/software/sw_m001c.htm), se hace un ataque estadístico por el método de Kasiski, y se obtiene la clave = ZEUT. Con un poco de imaginación y viendo el texto descifrado, se deduce que la clave es ZEUS y se obtiene el siguiente texto en claro:

ESTAESLACLAVEDELALGORITMOAESPARADESCIFRARELSEGUNDOCRIPT
OGRAMAYSEGUIRAVANZANDOENTURETOFFFFAAAABBBBCCCCCCCCBB
BBAAAAFFFF

Es decir:

ESTA ES LA CLAVE DEL ALGORITMO AES PARA DESCIFRAR EL SEGUNDO
CRIPTOGRAMA Y SEGUIR AVANZANDO EN TU RETO
FFFFAAAABBBBCCCCCCCCBBBBAAAAFFFF

Clave = FFFFAAAABBBBCCCCCCCCBBBBAAAAFFFF (128 bits)

**Criptograma 2:**

bCx4ZmbFBkLywi1EopC/O3YFyziPHJc0LeeNpD8dPF0o1u9mvwWpCTwAVknYfK3u

Es sencillo apreciar que el criptograma 2 está en base64. Como en el paso anterior nos dicen que el criptograma 2 está cifrado con el algoritmo AES y la clave obtenida es la encontrada anteriormente, podemos descifrar usando, por ejemplo, el programa AESPhere (http://www.criptored.upm.es/software/sw_m001p.htm).

Descifrando el criptograma se obtiene:

c2e1aa3154513d95f2c2557f2012ec666f9f6dc8f7ddf954d89da135858536056842b20baff9b821

Este número está compuesto por 80 valores hexadecimales, o lo que es lo mismo, 320 bits. Por la pista +300 del reto, el atacante tendría que deducir que se trata de un módulo RSA que podría intentar factorizar. Por ejemplo, utilizando msieve153 es factible en poco tiempo.

```
C:\Criptolab\msieve153>msieve153
0xc2e1aa3154513d95f2c2557f2012ec666f9f6dc8f7ddf954d89da135858536056842b20baff9b821 -v
```

p49 factor: 114291908775641756720529136956163946606473616165 9
p49 factor: 142270147609963771250529727967771969982750445313 9

Una vez obtenidos los factores primos, es sencillo crearse una clave RSA estándar. Por ejemplo con software genRSA (http://www.criptored.upm.es/software/sw_m001d.htm) o bien con OpenSSL.

p = C83243AFC2F6C30A5E5B286AD666EDA8B4480F7B (160 bits)
q = F93423FE27755C9DA90B86A34C3FCF56D0241613 (160 bits)
n = C2E1AA3154513D95F2C2557F2012EC666F9F6DC8F7DDF954D89DA135858536056842B20BAFF9B821 (320 bits)
e = 010001 (valor estándar, F4, 17 bits)
d = 1DD89BCD2441B0F1E714F62D1B076AE7214F446BCF1EAED2E705F3F66C8B56564675E528B0FEE4A5 (317 bits)

**Criptograma 3:**

ACAB3A5DD339ED41F92709367A324E744DAAC74CF1419108FAA93194069B66F0A3AF2E3C7B273353

Descifrando el criptograma 3 con la clave privada se obtiene:

C = ACAB3A5DD339ED41F92709367A324E744DAAC74CF1419108FAA93194069B66F0A3AF2E3C7B273353

M = 13012017

Dado que estamos buscando una fecha, la solución podría ser: 13 de enero de 2017 (13/01/2017)

**Criptograma 4:**

192685F83D5D9C7113EA36FD838C5D2D

Por el tamaño de este número, 128 bits, podría deducirse que se trata de un hash con el algoritmo MD5. Para resolverlo es posible hacer un ataque inverso mediante diccionario, por ejemplo utilizando la web CrackStation (https://crackstation.net/), siendo la solución "Albacete".

MD5 (Albacete) = 192685F83D5D9C7113EA36FD838C5D2D

Por tanto, la solución al reto:

**Viernes 13 de enero de 2017, Albacete**.

P.D.: *Es decir, los alienígenas han aterrizado el fin de semana pasado*.

Madrid, 17 de enero de 2017

**Contacto:**

- Dudas o comentarios: cryptoreto@criptored.com
- Síguenos en Twitter: @criptored | @mindcrypt
- Únete al grupo en Linkedin Criptored – Seguridad informática, Formación e investigación (+2.000 profesionales): https://www.linkedin.com/grp/home?gid=8387069