

CTF HACKON 2021

CRYPTO – DRAGONS



<https://www.hackon.es/>
@HackOnURJC

ENUNCIADO

¡Estamos en un mundo raro y rodeado de fuego! A lo lejos podemos ver una llanura con lo que parecen huevos, igual dentro de ellos se encuentra la forma de salir de tan sofocante lugar...

FLAG

HackOn{5pyr0_Th3_Dr4g0n}

SOLUCIÓN

En este reto se nos da un documento con un texto cifrado.

Podemos intuir que se trata de un cifrado Vigenère, pero para comprobarlo lo llevamos a alguna página que nos lo confirme.

En <https://www.boxentriq.com/code-breaking/> podemos identificar de qué tipo de cifrado se trata (acierta la mayoría de las veces) pulsando en “Cipher identifier”.

BOXENTRIQ HOME ABOUT CODE BREAKING FAQ HALL OF FAME CONTACT

Analysis Tools

These tools will help you identify the types of encodings and ciphers used.

- Binary analysis
- Hex analysis
- Cipher identifier**
- Text analysis
- Frequency analysis

Classic Ciphers

In cryptography, a cipher (or cypher) is a method for protecting data through encryption and decryption. Most ciphers require a specific key for encryption and decryption, but some ciphers like the ROT13 or Atbash ciphers have fixed keys. Many of the ciphers listed here were for military or other significant use during an earlier time, but today mostly are used only by puzzle makers.

- Adfgvx cipher
- Atbash cipher
- Bifid cipher
- Cryptogram
- Four-square cipher
- One-time pad
- Rail fence cipher
- Trifid cipher
- Adfgx cipher
- Baconian cipher
- Caesar cipher
- Double transposition
- Gronsfeld cipher
- Pigpen cipher
- Rot13
- Variant beaufort cipher
- Affine cipher
- Beaufort cipher
- Columnar transposition
- Enigma machine
- Keyed caesar cipher
- Playfair cipher
- Route transposition
- Vigenere cipher

Enter Ciphertext here

Enter text to analyze here...

Analyze Text

Copy

Paste

Text Options...

Note: To get accurate results, your ciphertext should be at least 25 characters long.

Introducimos nuestro texto cifrado y vemos que, con mayor probabilidad, se trata de un cifrado Vigenère.

Analysis Results

Hjppgz xwy Uglkdh vh fr kcutznjyxd oi efriljdldpd htmrgesafrsz tdl Zcdsbhzn Kpgvh j tjvcxnesi gdc Wd...

Your ciphertext is likely of this type:

Vigenere Cipher (click to read more)

Votes

- [Vigenere Cipher](#) (94 votes)
- [Caesar Cipher](#) (3 votes)
- [Beaufort Cipher](#) (2 votes)
- [Bifid Cipher](#) (1 votes)

For further text analysis and statistics, [click here](#).

Pulsamos en “Vigenere Cipher” y nos salen dos opciones para este cifrado:

Vigenère Cipher

The Vigenère cipher was invented in the mid-16th century and has ever since been popular in the cryptography and code-breaking community. Despite being called the Vigenère cipher in honor of Blaise de Vigenère, it was actually developed by Giovan Battista Bellaso. The Vigenère cipher is an improvement of the Caesar cipher, by using a sequence of shifts instead of applying the same shift to every letter.

A variant of the Vigenère cipher, which uses numbers instead of letters to describe the sequence of shifts, is called a Gronsfeld cipher. Gronsfeld ciphers can be solved as well through the Vigenère tool.

- [Vigenère Cipher Tool](#)

Vigenère Autokey Cipher

The Vigenère Autokey Cipher is a more secure variant of the ordinary Vigenère cipher. It encrypt the first letters in the same way as an ordinary Vigenère cipher, but after all letters in the key have been used it doesn't repeat the sequence. Instead it begins using letters from the plaintext as key.

- [Vigenère Cipher Tool](#)

Como no tenemos ninguna clave de descifrado tenemos que optar por el segundo enlace.

Ahí, volvemos a introducir nuestro texto cifrado y, pulsando en el botón de Auto Solve, por “fuerza bruta” vamos a obtener el texto en claro y la clave que se usó para cifrarlo.

Vigenere Tool

wrczgxrr dhwrikp oi efriljdldpd ic jcpjwiukxrr yoeiz e kirns rpnuxnsan, p szw nytjpppm, kxeyauupa wesia z: cment n
Cevy p Hacgi: Ptlv dz kwf Hguxdy, wt frckegie blw iuisp tplr EwenMkpmhd vc 1999 j 2000, vtmgtnxprbpriy. Rjyujy
Zcdsbhzn vthlcndm u cdd htlvrssh xv spwplidwpx al wtlzt Dtnlf spweovh oia nvgnig dltrs, tf vmtxd xv azw
ickjwsh xv EwenMkpmhd jt avtmkd l ycu jtcmt wfcmcor sp njyxd ic prgteh jcpueuiiblw. Tf ajpkd, dlces rie hfw sij
hfgtmfpgw, hy itxehvgtdd grh eegxv rzqd jrgei sy Jejvd Lvrxrxnvs Evxffvj ic 2018.

Copy

Paste

Text Options...



Type key here...



Standard Mode



English

Decode

Encode

Auto Solve (without key)

Instructions

El resultado que más puntuación tiene es el primero, con clave "purple". Además, se puede ver el texto en claro.

Auto Solve results

Score	Key	Text
23855	purple	spyro the dragon es un videojuego de plataformas desarrollado por insomniac games y publicado por sony computer entertainment para playstation el de septiembre de el primer juego de la serie spyro esta protagonizado por el personaje principal un joven dragon purpura llamado spyro y su amigo libelula sparx quien debe viajar a traves del reino del dragon para derrotar a gnasty gnorc quien ha superado a los mundos del dragon atrapando a los otros dragones en cristal y convirtiendo su tesoro de gema
11301	purplepur	spyro the drrtow rs la videojuego ur puntrsormas desariblindf cor insomniat tavrs p cublicado poi fowl cfzputer enterkniwzeeg para playstrgixa ec qe septiembrv qe ny pivmer juego de cn sneiv fpyro esta prfgapbnzmado por el peifownjv principal un abvna dingon purpura cyavndf fpyro y su amixb lroechla sparx quiva dnoe mvajar a travej qeu eezao del dragon gnry qeieotar a gnastp tnxec hchien ha superqo j yoj zundos del drrtow ntinpando a los okeob qrrtones en crisknl h poeiirtiendo su krsxoe ur gema
10733	pleplepur	sylo the dragow rs la vrqeojuego de puntrsozas desarrolundf coa vnsomniac gavrs p cukyicado por sowl cfzpdger entertaiwzeeg pjea playstatixa ec qe brptiembre de ny pivmne juego de la sneiv fpheo esta protapbnzmamb por el persownjv crracipal un jovna

Como no nos sale el texto entero, repetimos el proceso anterior pero esta vez introduciendo la clave que ya sabemos y pulsando el botón Decode.

Vigener Tool

Cevy p Hacgi: Ptlv dz kwp Hguxdy, wt frckegie blw iuisp tplr EwenMkpmndh vc 1999 j 2000, vtmgtnxprbpriy. Rjyujy Zcdsbhzn vthlcnmd u cdd htlvrssh xv spwplidwpd xv al wtlzt Dtnlf spweovh oia nvgnig dltrs, tf vmtxd xv azw ickjwsh xv EwenMkpmndh jt avtmkd l ycu jtcmt wfcemcor sp njyxdd ic prgteh jcpeeuiiblw. Tf ajpkd, dlces rie hfw sij hfgtmfgpw, hy itxehngtdd grh eegxv rzqd jrgei sy Dejvd Lvrxrxnvs Evxffvj ic 2018.

Copy Paste Text Options...

Standard Mode English

Decode Encode Auto Solve (without key) Instructions

Por último, vemos el texto descifrado y observamos que ahí está la flag que buscábamos.

Results

Decoded message:

Spyro the Dragon es un videojuego de plataformas desarrollado por Insomniac Games y publicado por Sony Computer Entertainment para PlayStation el 10 de septiembre de 1998. El primer juego de la serie Spyro, esta protagonizado por el personaje principal, un joven dragon purpura llamado Spyro y su amigo libelula, Sparx, quien debe viajar a traves del Reino del Dragon para derrotar a Gnasty Gnorc, quien ha superado a los 5 Mundos del dragon atrapando a los otros dragones en cristal y convirtiendo su tesoro de gemas en un ejercito de secuaces para su orden. Spyro the Dragon es un videojuego de plataformas en 3D de mundo abierto, que presenta niveles grandes y extensos en los que el jugador debe encontrar elementos coleccionables, entre los que se encuentran piedras preciosas, dragones cristalizados y huevos de dragon robados. Las habilidades de Spyro como dragon incluyen aliento de fuego, un ataque de carga frontal y un planeo en el aire que puede usar para viajar a grandes distancias, todo lo cual debe usarse estrategicamente para encontrar objetos y derrotar enemigos.

Spyro the Dragon comenzo a desarrollarse tras el lanzamiento del juego debut de Insomniac, Disruptor, que se vendio mal pero en general fue elogiado por los criticos, lo que impresiono a Universal Interactive lo suficiente como para alentarlos a hacer un segundo juego. El artista Craig Stitt sugirio un juego sobre un dragon, y se comenzo a trabajar en un nuevo juego. Inspirandose en la pelicula Dragonheart, el juego comenzo como un titulo mas maduro con un enfoque oscuro y realista, pero la direccion se cambio para tener un tono mas fantastico y alegre para atraer a un mercado mas amplio de consumidores. El videojuego fue uno de los primeros en PlayStation en utilizar niveles de detalle cambiantes entre los objetos renderizados, gracias a un motor panoramico desarrollado por **HackOn{5pyr0_Th3_Dr4g0n}** Alex Hastings que permitio que la naturaleza abierta del juego se realizara completamente. Stewart Copeland, el ex baterista de The Police, compuso la musica del juego, y el personaje principal fue la voz de Carlos Alazraqui, junto con las voces adicionales de Clancy Brown, Michael Gough y Jamie Alcroft.

Copy Text Options...