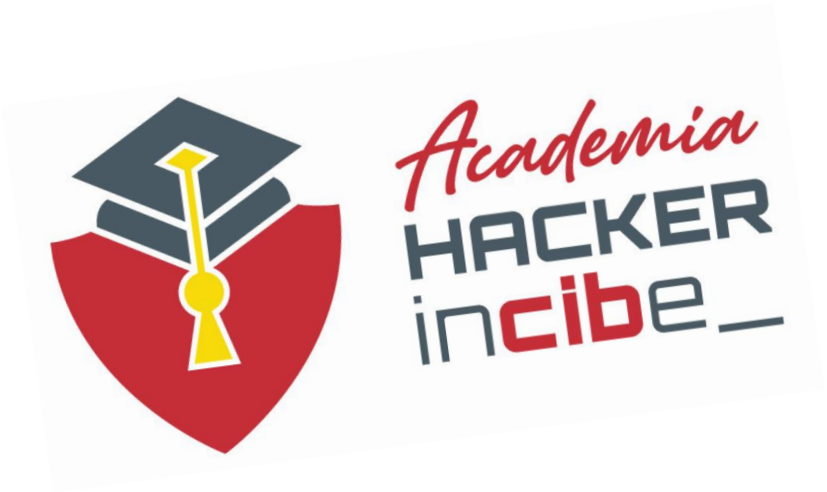
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL




# Academia Hacker INCIBE

## MagicCrypto

Dificultad: **Fácil**

Categoría de Reto: **Criptografía**

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD

# ÍNDICE



# ÍNDICE DE FIGURAS

No se encuentran elementos de tabla de ilustraciones.

# ÍNDICE DE TABLAS

No se encuentran elementos de tabla de ilustraciones.

# 1. CONTEXTO

Cripto sencillo para obtener puntos fáciles.

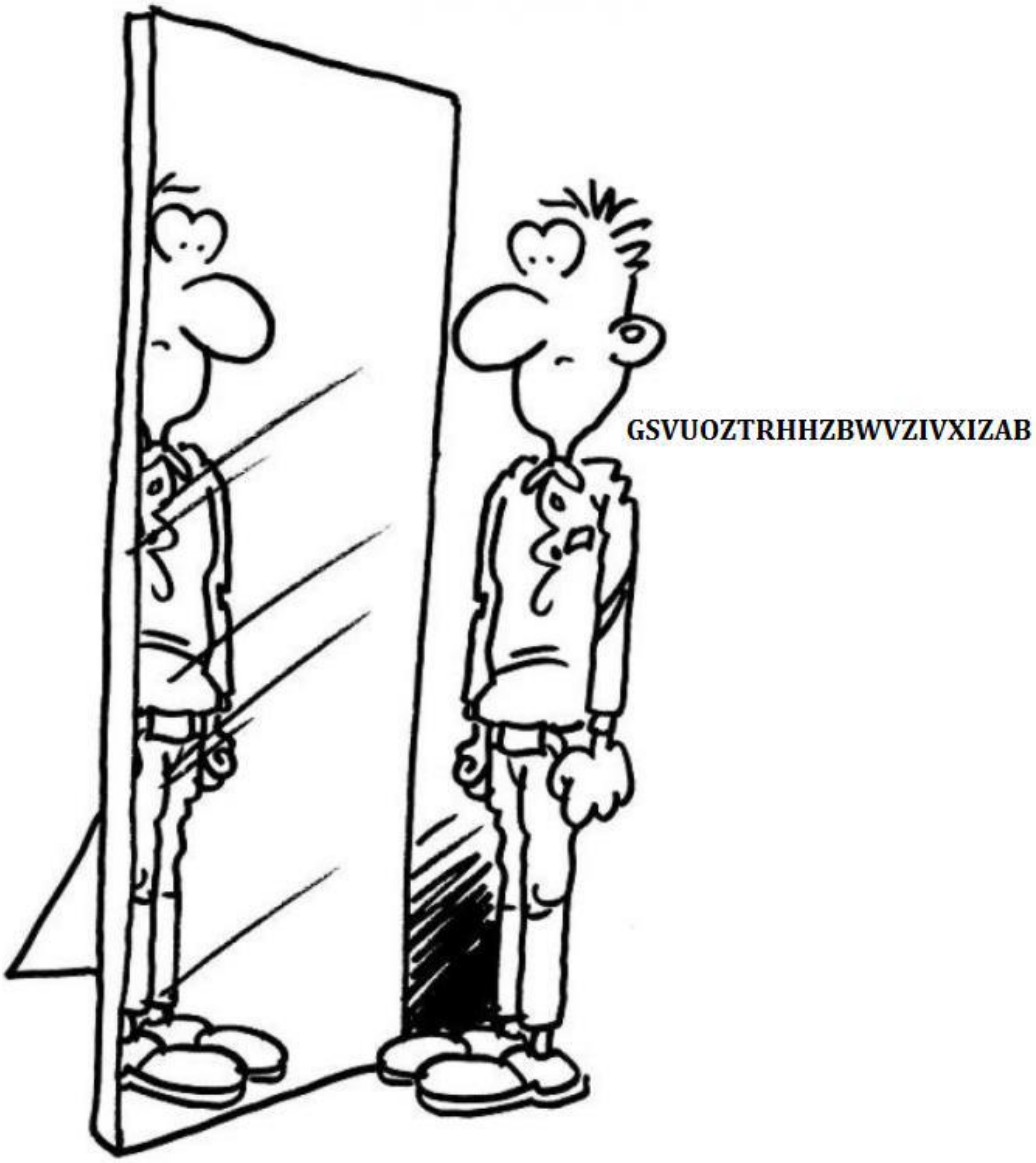
Flag: **SAYWEARECRAZY**

Datos proporcionados:

Fichero .jpg

# 2. DESCRIPCIÓN PARA PARTICIPANTES

Descifra el mensaje oculto en la imagen MagicCrypto.jpg.



## 3. PISTAS

1. En criptografía, El cifrado por sustitución es un método de cifrado por el que unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular.
2. Existe un tipo de cifrado denominado espejo.
3. Este método es conocido como atbash.

# 4. SOLUCIÓN

En la imagen que tenemos a disposición, se puede observar un espejo y el string o cadena “GSVUOZTRHHZBWVZIVXIZAB”

Conociendo los cifrados por sustitución se puede deducir que se trata de un cifrado de tipo espejo o atbash.

El cual puede ser descifrado sustituyendo cada carácter con el que le sea correspondiente siguiendo la tabla:

| ORIGINAL | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ATBASH | Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Re-ordenando los datos según la matriz para descifrar el mensaje obtenemos el texto:**THEFLAGISSAYWEARECRAZY**

# 5. REFERENCIAS

Atbash es un método muy común de cifrado (criptografía) del alfabeto hebreo. Pertenece a la llamada criptografía clásica y es un tipo de cifrado por sustitución. Se le denomina también método de espejo, pues consiste en sustituir la primera letra (álef) por la última (tav), la segunda (bet) por la penúltima (shin) y así sucesivamente. Uno de sus usos más célebres se da en el libro de Jeremías, donde a fin de no nombrar Babilonia (לבב, Babel) se utiliza el término, en atbashSesac (ששך, Sheshakh).

La tabla de sustitución de atbash para el alfabeto hebreo es la siguiente:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Original | א | ב | ג | ד | ה | ו | ז | ח | ט | י | כ | ל | מ | נ |
| | ס | ע | פ | צ | ק | ר | ש | ת | | | | | | |
| Clave | ת | ש | ר | ק | צ | פ | ע | ס | נ | מ | ל | כ | י | ט | ח |
| | ז | ו | ה | ד | ג | ב | א | | | | | | | |

Una tabla de atbash para el alfabeto español sería así:

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Original | a | b | c | d | e | f | g | h | i | j | k | l | m | n |
| | ñ | o | p | q | r | s | t | u | v | w | x | y | z | |
| Clave | Z | Y | X | W | V | U | T | S | R | Q | P | O | Ñ | N |
| | M | L | K | J | I | H | G | F | E | D | C | B | A | |

En todo caso, hay que tener presente que este método de cifrado se ideó para un abyad en el que solo se escriben las consonantes, que luego se vocalizan de manera más o menos arbitraria y, así, prácticamente cualquier palabra hebrea es pronunciable al cifrarse en atbash. En idiomas con escritura alfabética, como el español, es infrecuente que una palabra codificada en atbash sea pronunciable.

Atbash

https://pedrocarrasco.org/projects/criptografia/atbash.php?text=holamundo

https://gchq.github.io/CyberChef/#recipe=Atbash_Cipher()&input=aG9sYW11bmRvCg