

Nombre:

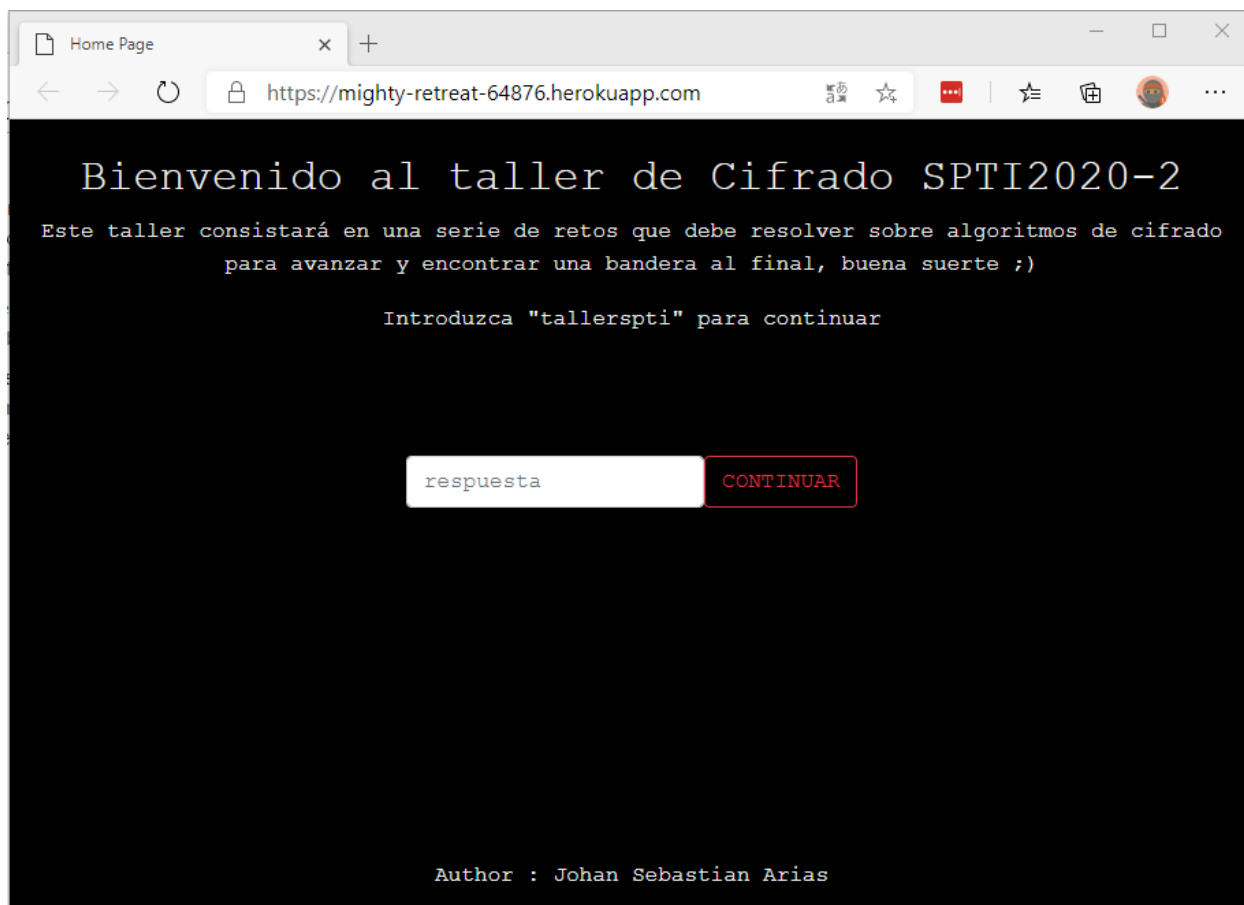
- Angie Daniela Ruiz Alfonso
- Angi Paola Jiménez Pira
- Juan Sebastián Díaz Salamanca

Fecha: 26/09/2020

Taller de Cifrado parte 1

El sitio web mencionado a continuación, cuenta con una serie de desafíos en conceptos básicos de Cifrado y algunos de los mecanismos clásicos utilizados, se debe enfrentar cada uno de estos y aportar evidencia en capturas de pantalla de la respuesta de cada uno de ellos.

Link: <https://mighty-retreat-64876.herokuapp.com/>



Home Page

https://mighty-retreat-64876.herokuapp.com

Bienvenido al taller de Cifrado SPTI2020-2

Este taller consistirá en una serie de retos que debe resolver sobre algoritmos de cifrado para avanzar y encontrar una bandera al final, buena suerte ;)

Introduzca "tallerspti" para continuar

respuesta CONTINUAR

Author : Johan Sebastian Arias

First Challenge ROT47 + ROT13

Inicial: \$CJGAGB?BC7 J3E6?78C BCAGD6?6 CJ KC27?HC G2863B9AC QF3J? K92B3Q 4?6? A328G29?6

ROT47: Sryvpvqnqrqf ybtenfgr qrpvsene ry zrafnwr vagebqhpr "ubyn zhaqb" cnen pbagvahne

Resultado anterior en **ROT13:** Felicidades lograste decifrar el mensaje introduce "**hola mundo**" para continuar

!!BASE64!!

Inicial:

SG9sYSBhbWlnbyBOZWNIc2l0byBxdWUgbWUgY2lmcmVzIGVzdGUgbWVuc2FqZSAiQUxFTUFOIEITIF
RIRSBORVcgUk9NQW4iIGNvbiBlbCBhbGdvcmI0bW8gZGUgUmF
pbCBGZW5jZSBjaXB0ZXlglKDMgY2FycmlsZXMPiGx1ZWdvlGluZ3Jlc2FsbyBTSU4gRVNQQUJNT1MhISB
5IHVZHLhcyBjb250aW51YXIK

Base64: Hola amigo Necesito que me cifres este mensaje "ALEMAN IS THE NEW ROMAN" con el algoritmo de Rail Fence cipher (3 carriles) luego ingresalo SIN ESPACIOS!! y podrs continuar.

Rail Fence: AATEMLMNSHNWOAEIERN (respuesta)

SHA256 + COLUMNAR

Inicial: Mtqf ij szjat, sjhxnryt vzj rj hnkwxj jxyj rjsxfoj "RJ LZXYF HNKWFW RJSXFOJX" js jq fqltwnyrt
Htqzrsfw ywfsxutxnynts.
Qf ufqfgwf hqfaj jx EJGWFX, htruqjyf qf rfywne hts qfx qjywx FGH j nsywtizhj jq rjsxfoj hnkwnit ufwf
htsynszfw xjufwit utw jxufhntx

Cesar con llave 5: Hola de nuevo, necesito que me cifres este mensaje "ME GUSTA CIFRAR MENSAJES"
en el algoritmo Columnar transposition.
La palabra clave es ZEBRAS, completa la matriz con las letras ABC e introduce el mensaje cifrado para continuar separado por espacios.

Columnar: SRSB GIES ECME UFNA TAAC MARJ (respuesta)

HEXADECIMAL!!

Inicial: 45 6e 20 6c 61 20 69 6d 61 67 65 6e 20 76 65 72 e1 73 20 65 6c 20 63 69 66 72 61 64
6f 20 64 65 20 22 70 69 67 70 65 6e 20 63 69 70 68 65 72 22 20
61 72 6d 61 20 65 6c 20 6d 65 6e 73 61 6a 65 20 79 20 70 6f 64 72 61 73 20 63 6f 6e 73 65 67
75 69 72 20 74 75 20 62 61 6e 64 65 72 61 21 21

Hexadecimal: En la imagen verás el cifrado de "pigpen cipher" arma el mensaje y podras conseguir tu bandera!!

Pigpen Cipher: no debo dormir en clase de seguridad (respuesta)

FELICITACIONES, ERES EL MEJOR CRACKEANDO ALGORITMOS DE CIFRADO!!!