

Write-up: HackTheBox - Crypto - Classic, yet complicated!

SEBASTIÁN SEPÚLVEDA @PIBLACK

18 de mayo de 2019

Información: Categoría Crypto, 10 points.

Descripción: Find the plaintext, the key is your flag! Flag format : HTBkey in lowercase

WRITEUP

Cuando archivo .zip nos entrega el siguiente texto cifrado:

```
alp gwcsepul gtavaf, nlv prgpbpsu mb h jcpbyvdlq, ipltga rv glniypfa we ekl 16xs nsjhlecb. px td o lccjdstsl-
pahzn fptsfp xstlxzi te iosj ezv sc xcns ttsoic lzlvrmhaw ez sjqijsa xsp rwhr. tq vxspf sciov, alp wsphvcv
pr ess rwxpqlvp nwlvcv dyi dswbhvo ef htqtafvyw hqzfbpg, ezutewwm zcep xzmyr o scio ry tscoos rd
woi pyqnmgelvr vpm . qbctnl xsp akbflowllmspwt nlwpcg, lccjdstslpahzn fptsfp oip qvx dfgysgelipp ec
bfvbxlrnj ojocjvpw, ld akfv ekhr zys hskehy my eva delluxpih yoe mh yiacsoseehk fj l gebxwh sieesn we ekl
iynfudktru. xsp yam zd woi qwoc.
```

Para saber qué tipo de cifrado es, ocupamos [MTH911](#).

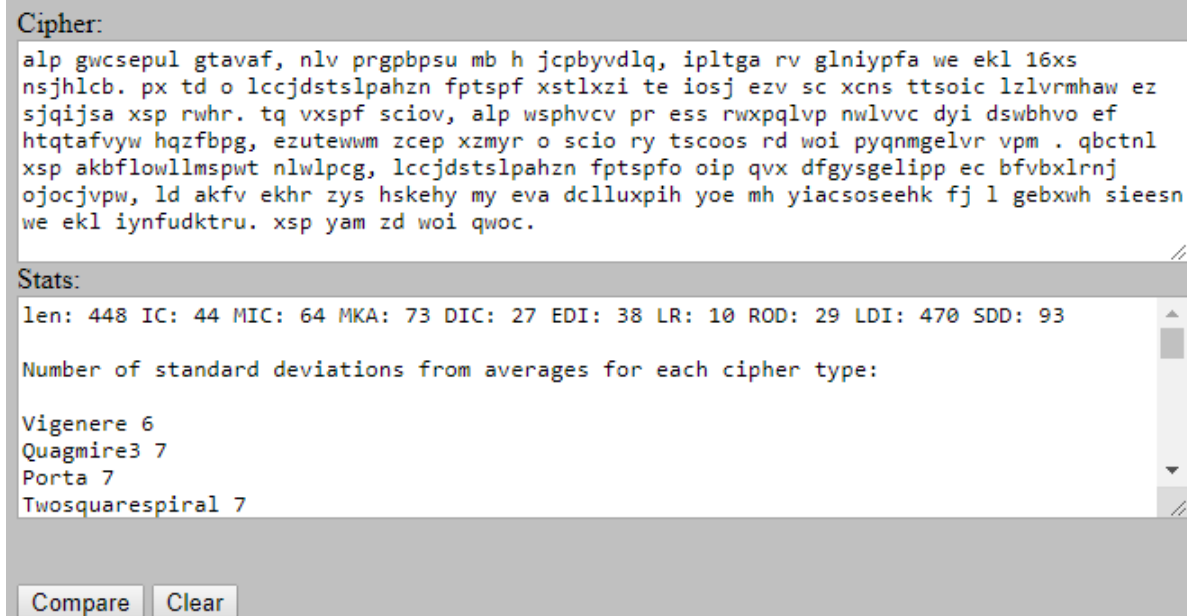


Figura 1. Return Cipher Statics

Nos dice que es un cifrado **Vigenere**. Buscando en google, es posible encontrar el siguiente **Vigener Cipher**, el que nos facilita las cosas al tener una opción de descripción automática. Al insertar el texto, colocamos **THE** en “KNOWING A PLAINTEXT WORD”, pues inferimos en el primer intento que el texto está en inglés. la flag en el primer resultado que nos entrega la decodificación. Ver Figura 2:

Results

Vigenere ?

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

↑↓

THEVIGENERECIPHERWASINVENTEDBYAFRENCHM

ANBLAISEDEVIGENEREINTHETHCENTURYITISAP

HELL OLYALPHABETICCIPHERBECAUSEITUSESTWOORM

OWOR ORECIPHERALPHABETSTOENCRYPTTTHE DATAINOT

LD HERWORDSTHELETTERSINTHEVIGENERECIPHERA

RESHIFTEDBYDIFFERENTAMOUNTSNORMALLYDON

EUSINGAWORDORPHRASEAST

THEVIGENEVECIPHERWAWINVENTEDBCAFRENCHM

ARBLAISEDEVMGENEREINTLETHCENTURCITISAP

HELL OLYELPHABETICGIPHERBECAUSEITUSESTAOORM

OWOR ORECITHERALPHABITSTOENCRYPTTTHE DATAIROT

LZ HERWORDWTHELETTERWINTHEVIGERERECIPHERE

RESHIFTEDFYDIFFERENXAMOUNTSNOMALLYDON

EYSINGAWORDSRPHRASEASX

THEVIGENSRECIPHERWOSINVENTEDPYAFRENCHM

SUB-ALPHABETICINVENTEDBYAFRENCHM

↑↓

DataCamp

Buy Now

Vigenere Decoder

★ VIGENERE CIPHERTEXT

sjqijsa xsp rwhr. tq vxspf sciov, alp wspgvv pr ess
 rwxpqlv nwlvvv dyi dswbhvo ef htqtafvw hqzfbpg,
 ezutewwm zcep xzmyr o scio ry tscos rd woi pyqnmgelvr
 ypm . qbctnl xsp akbflowllmspw nwlpcg, lccjdtslpahzn
 fptspfo oip qvx dfgysgelipp ec bfvbxlrnj ojocjvpw, ld
 akfv ekhr zys hskchy my eva dclluxpih yoe mh yiacsoseehk
 fj l gebxwh sieesn we ekl iynfudktru. xsp yam zd woi
 qwoc.

☐ KNOWING THE KEY:

☐ KNOWING THE KEY-LENGTH, SIZE:

☐ KNOWING ONLY A PARTIAL KEY:

☒ KNOWING A PLAINTEXT WORD:

☐ TRY A COMMON-WORDS DICTIONARY ATTACK

★ DICTIONARY

☐ TRY TO DECRYPT AUTOMATICALLY (STATISTICAL ANALYSIS CRACKER)

★ ALPHABET

DECRYPT VIGENERE

Figura 2. Flag encontrada

Flag: HTB{helloworld}