

JulesDT / ctfWriteUps

Watch 2 Star 1 Fork 0




<> Code ⓘ Issues 0 🔄 Pull requests 0 📁 Projects 0 Insights ▾

Branch: master ▾ ctfWriteUps / Junior CTF 2016 / Southern Cross - Crypto - 300 /

Create new file Find file History

 JulesDT Fixed image extension

Latest commit 691e9c7 on Nov 28 2016

..		
 README.md	Fixed image extension	6 months ago
 southernCross.png	Added first Junior CTF 2016 write up	6 months ago
 vigenere.jpg	Added first Junior CTF 2016 write up	6 months ago

 README.md

Junior CTF 2016 - Southern Cross

Crypto - 300 pts

[Challenge Code](#)



This challenge is about the "Southern Cross Cipher". A quick look to the Southern Cross makes us think of the Vigenere Cipher.

The Vigenere cipher is based on the Caesar Cipher. We choose a code, and then have a different ceasar cipher for each letter depending on the key. More information can be found [on the wikipedia page](#). Here is the Vigenere Cipher shift table :

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

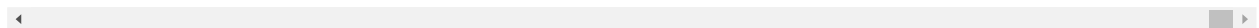
Many different algorithms exist on Internet to solve this cipher.

I didn't code my own tool to solve this kind of cipher, but I will explain briefly the cryptanalysis to solve this.

The first goal is to find same letters group or patterns. The different offset between common words will give us hints about the key length. Once the key length is found, we have as many Caesar Cipher as the number of letters in the key. This kind of cipher is then solved with a letter frequency analysis.

I used the famous [dcode](#) web tool. We ask him to entirely solve the cipher and he finds that the key should be `bolivar`. But this tool doesn't decode the whole ciphertext and I had to use another tool to have the end of the plaintext. I used this [french web tool](#) which worked very well too. It gave me this plaintext :

SELF FOR A MOMENT LIKE AN EVIL FACE IN THE WINDOW OF A REPUTABLE HOUSE HE WILL SETTLE AT ONE EIGHTY FIVE SAID DODSON BOLIVAR CANNOT CARRY DOUBLE



Looking at the end of the cipher, I had to guess that only the four last words were good. The flag was

BOLIVAR CANNOT CARRY DOUBLE

I was pretty disappointed that not flag format was given. They could easily add in the cipher text something like "THE FLAG IS" before the actual Flag to help people know instead of maybe bruteforcing the scoreboard, which, luckily I didn't have to do.

