

Cryptography Challenge

3rd Time's the Charm

The first one is simple. Then its shifted further. But after that its uniform.

69 68 69 87 73 124 98 115 121 96 103 102 117 121 97 120 107 107 96 116 108 96 110 113 118 106
117 117 105 126

Approach

Ciphertext:

69 68 69 87 73 124 98 115 121 96 103 102 117 121 97 120 107 107 96 116
108 96 110 113 118 106 117 117 105 126

Hint:

The first one is simple. Then its shifted further. But after that its uniform.

This suggests that there are **3 parts** to deciphering. If we analyze the original ciphertext, we can deduce that it *could* be converted to ASCII, and this would make sense as the first part of the cipher is "simple".

Converting into ASCII

Output: EDEWI|bsy`gfuyaxkk`tl`nqvjuui~

Next hint is the "its shifted further" which indicates we need to shift the characters. However, keep in mind that we know the flag format is CBCTF{...}. We also know flags usually have _ to separate words. This gives us a clue on what shift is required.

Let's make the following assumptions:

E	D	E	W	I		b	s	y	`	g	f	u	y	a	x	k	k	`	t	l	`	n	g	v	j	u	u	i	~
C	B	C	T	F	{				_									_			_								}

This would relate to the second hint where the characters are "shifted further". So lets look at the pattern.

Ciphertext	Expected	Required shift
E	C	-2
D	B	-2
E	C	-2
W	T	-3
I	F	-3
	{	-1
`	-	-1
~	}	-1

We can deduce that **symbols** are shifted by -1.

However, the **letters** are not shifted to the same amount, only a few are.

We know case sensitivity must be kept (because of the flag format CBCTF), so let's use ROT13 as it shifts only letters and preserves the case sensitivity.

We also know that the first **3 letters** shifted the same amount.

Let's take out the symbols and review the shifts again:

[illegible]

Perhaps we can try to shift them by **blocks of 3 letters**, and by a decreasing amount (24 -> 23 -> 22 -> 21 -> etc...)

[illegible]

Looks like we are finally getting somewhere

E	D	E	W	I		b	s	y		g	f	u	y	a	x	k	k		t	l		n	g	v	j	u	u	i	
24	24	24	23	23		23	22	22		22	21	21	21	20	20	20	19		19	19		18	18	18	17	17	17	16	
C	B	C	T	F		y	o	u		c	a	p	t	u	r	e	d		m	e		f	i	n	a	l	l	y	

From EDEWI|bsy`gfuyaxkk`tl`nqvjuui~

To CBCTF|you`captured`me`finally~

Then just shift all symbols by -1

CBCTF{you_captured_me_finally}

Based on the hint:

“The first one is simple.” : convert to ASCII

“Then its shifted further.” : ROT13 blocks of 3 letters in decreasing shifts

“But after that its uniform.” : shift all symbols by -1

Flag

CBCTF{you_captured_me_finally}