

Walkthrough – Descramble

Challenge

Upon reading the question description, you might think that the acronym CVA could stand for something else, instead of counter villainy agency. You would be correct, each letter in the acronym is a hint towards all the cipher decryption schemes you would need to employ to successfully decrypt the cipher text. These ciphers are, in the order needed to apply them: Caesar, Vigenère, and Autoclave. We can apply these ciphers in a more efficient manner by using an online decoder: <https://www.dcode.fr>

Solution

1. Although the cipher techniques are now known to us, there is still something else we need to consider for the Caesar cipher. We need to figure out the specific shift number that will lead us on the correct path. Through some trial and error, you would find that the correct shift number is denoted by the number of spaces in between every string in the encrypted text.



The image shows a screenshot of the 'CAESAR CIPHER DECODER' interface on the website dcode.fr. The page has a parchment-like background. At the top, it says 'CAESAR CIPHER' in a bold, serif font, with a breadcrumb trail below it: 'Cryptography > Substitution Cipher > Caesar Cipher'. Below this is a section titled 'CAESAR CIPHER DECODER'. Inside this section, there is a sub-header '★ CAESAR SHIFTED CIPHERTEXT' followed by a text input field containing the encrypted text 'MkF'd uyqtc dj fpxh.'. Below the input field are two radio button options: 'KNOWING THE SHIFT:' (which is selected) and 'TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)'. At the bottom of the section is a button labeled 'DECRYPT CAESAR CODE'.

2. Get the result of the Caesar cipher decryption and input it into the Vigenère cipher for decryption. This is where the answers to the riddles will come into play. They serve as a key/password for the cipher to properly decrypt the results from the Caesar cipher decryption that we did earlier. This password entered will be dependent on which of the three descramble challenges is being attempted.

VIGENERE DECODER

★ VIGENERE CIPHERTEXT
Kid'b sworabh dnvf.

PARAMETERS

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

AUTOMATIC DECRYPTION

DECRYPTION METHOD

KNOWING THE KEY/PASSWORD: FAIR

KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

KNOWING ONLY A PARTIAL KEY: KE?

KNOWING A PLAINTEXT WORD: CODE

VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

3. Once we have the result of the Vigenère decryption we put it into the autoclave cipher for decryption, like so:

AUTOCLAVE CIPHER

Cryptography › Poly-Alphabetic Cipher › Autoclave Cipher

AUTOKEY (VIGENERE) DECODER

★ VIGENERE AUTOKEY CIPHERTEXT
Fiv'k nwgavbz mixx.

WITHOUT KNOWING THE KEY (BRUTEFORCE ATTACK)

INITIAL KEYWORD FAIR

OPTIONAL PARAMETER

★ CUSTOM ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

DECRYPT

This should give us the flag.

Results

Ain't nothing fair.

Note that the steps for all the descramble challenges are the same with different keys for each.

The keys can be found below:

	Descramble 1	Descramble 2	Descramble 3
Caesar	2	12	7
Vigenère	Fair	Mind	Dear
Autoclave	Fair	Mind	Dear

Final Answer	QCTF- {Ain't_nothing_fair.}	QCTF- {Dream,_not_of_what_you_are,_but_of_what_you_want_to_be.}	QCTF- {Frankly,_my_dear,_I_don't_give_a_damn.}
--------------	--------------------------------	--	---