VishwaCTF

CHALLENGE NAME : POLY FUN

DEV : REVAK PANDKAR

CATEGORY : CRYPTOGRAPHY

LEVEL : MEDIUM

2024

Looking at the description, we can see that this challenge uses a symmetric key encryption technique to encode the flag. But taking a look at the key, we can see that the key has been encoded as well. We are also given a challenge.py file which contains the script which was used to encode the key.

So, studying the script we see that the actual the key.txt is opened in the bytes format. Also, a polynomial has been declared using the coefficients 4,3,7. Now we can see that the encrypt function takes each character of the key in bytes (which is its ASCII value) and performs a transform() function and the return value is passed to the polynomial 'p'. The y-value of the polynomial is a number which is then converted to a character. This is done for all characters in the key. So, the key has been polynomially encoded.

But what is the transform function? Using a debugger, we can come to know that the transform function actually doesn't do anything. It changes the value of the number passed to it multiple times but the changes are reversed using a combination of addition, subtraction, multiplication and division operations.

So, the only challenge is to reverse the polynomial encoding. The ASCII value of the character after passing it to the polynomial is known to us. So, we simply have to figure out the roots of the polynomial for each character in the encoded key.

Let’s say one of the y-value we get is 160. So, the equation becomes:

$160 = 4x^2 + 3x + 7$

To get the roots of this equation we change the equation as follows:

$4x^2 + 3x + 7 - 160 = 0$

Now we simply get the roots of the equation using the numpy’s roots() function.

We only take the positive root and ignore the negative root.

After getting the root, we convert it to a char to get the ASCII character associated with this ASCII value.

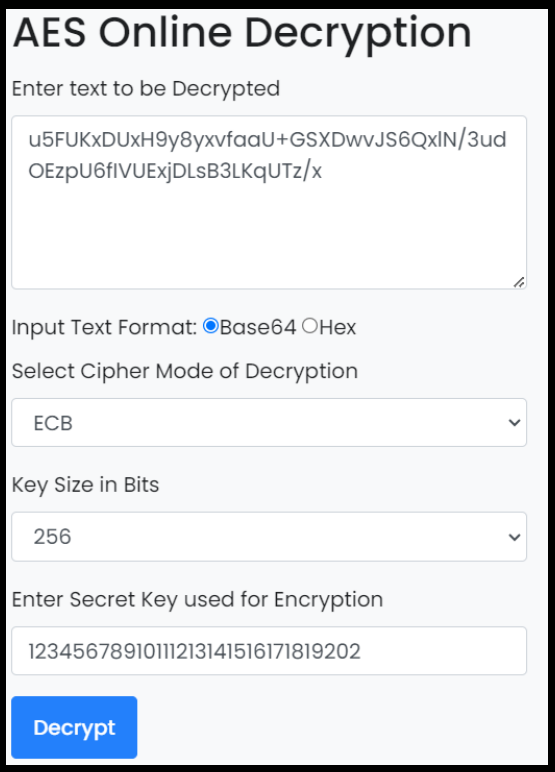
Below is the decrypt function which does the above process for all the characters in the encoded key.

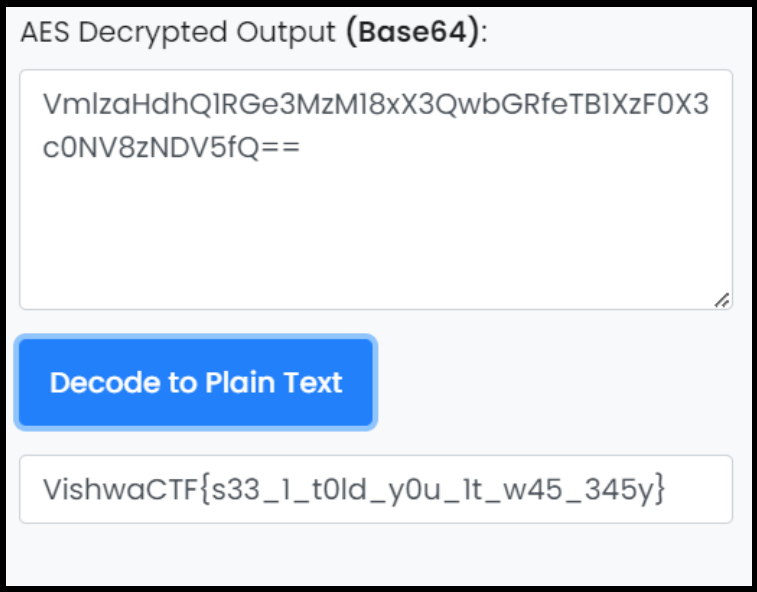
Code:

```
import numpy as np

def decrypt(enc):
    dec = ' '
    for i in enc:
        sol = [4,3,7-ord(i)]
        dec += chr(int(np.roots(sol)[1]))
    print(dec)

enc = '☞➪⇄⫞ʕ□⬚⅍pc☞⒗☞☞☞➪☞⇄☞⫞☞ʕ☞□☞⬚☞⅍☞pc➪⒗➪'
decrypt(enc)
```

The decrypt function iterates through all characters in the encoded key and gets the roots for each character to get the original ASCII value.

Now we think of decrypting the flag. The description says a simple symmetric key encryption was used to encode the flag. AES is a popular symmetric encryption technique. We can use a simple online AES decryption tool to get the flag.





Hooray! We found the flag!

Flag: VishwaCTF{s33_1_t0ld_y0u_1t_w45_345y}