

24th December 2016

3DS-CTF

Hot Sun? (Crypto - Level 1)

Surfing in the Shallowweb, we have discovered a new algorithm that promises to be the newest substitution cipher. The algorithm to encrypt works as following: the user informs the text to be encrypted and a number N . Initially, the algorithm shift all letters one position to the right (e.g. 'A' turns into 'B'). With this result, in the next step, the algorithm now shift the text two positions to the right. And with the text from the previous output, it repeats the shift procedure until N . Your task is quite simple: given an encrypted flag and an N number, discover the flag.

Encrypted flag: 3RG{hv1g_f0h_1g_b0h_g0_V0h} N:11

A crypto warmup question, how lovely. The encrypted flag was obtained after repeated letter shifts. As they mentioned that the N value signified how many times a letter is being shifted, we can easily figure out that each letter is being shifted 66 times. But we know that after 26 shifts, we will end up with the same letter. So, we basically have to shift each letter $66 - 26 - 26 = 14$ times. But what about the direction? As they encrypt by shifting letters in the forward direction, we have to decrypt by shifting letters in the backward direction!

Flag: **3DS{th1s_r0t_1s_n0t_s0_H0t}**

Crypto Master? (Crypto - Level 1)

John says that he is the master of his personal server. He created a script that talks to him as if it was his disciple. The problem is that in order to access the server, one needs to know the logic used by the script. Access the server and get the flag.

Server: 54.175.35.248:8002

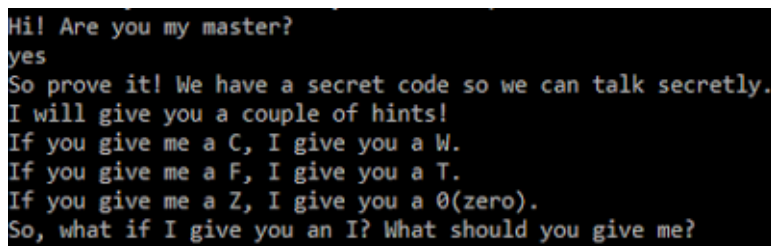
So this time, they haven't given any encrypted flag to work with. On connecting to the server using *netcat*, we are prompted with this:



[[https://3.bp.blogspot.com/-E8-ZrAlfDMU/WFkTPXHL-](https://3.bp.blogspot.com/-E8-ZrAlfDMU/WFkTPXHL-MI/AAAAAAAAAHl/V7jBBG-r5HYRI3pOSQ8ntZXYw6UFTJ4wCLcB/s1600/Capture.PNG)

[MI/AAAAAAAAAHl/V7jBBG-r5HYRI3pOSQ8ntZXYw6UFTJ4wCLcB/s1600/Capture.PNG](https://3.bp.blogspot.com/-E8-ZrAlfDMU/WFkTPXHL-MI/AAAAAAAAAHl/V7jBBG-r5HYRI3pOSQ8ntZXYw6UFTJ4wCLcB/s1600/Capture.PNG)]

Why would anyone say no to this!



[[https://4.bp.blogspot.com/-](https://4.bp.blogspot.com/-jX04JkQhGZQ/WFkTdOyWkbl/AAAAAAAAAHM/aurXfU04psANIAJrliNjchPP4fuoBX4GACLcB/s1600/Capture.PNG)

[jX04JkQhGZQ/WFkTdOyWkbl/AAAAAAAAAHM/aurXfU04psANIAJrliNjchPP4fuoBX4GACLcB/s1600/Capture.PNG](https://4.bp.blogspot.com/-jX04JkQhGZQ/WFkTdOyWkbl/AAAAAAAAAHM/aurXfU04psANIAJrliNjchPP4fuoBX4GACLcB/s1600/Capture.PNG)]

We are now given the logic. So this is what we have till now: