Challenge Name: World's Strongest Cipher

Category: Crypto

Flag: STMCTF{L1n3@r_c1ph3rs_@re_b@D}

User is given the following webpage.

-We got the ciphertext, decrypt it immediately!

-0x255472592e2ce4f26fe40110de9d57fd0bbe31052d61b086923851c0f3eed79c

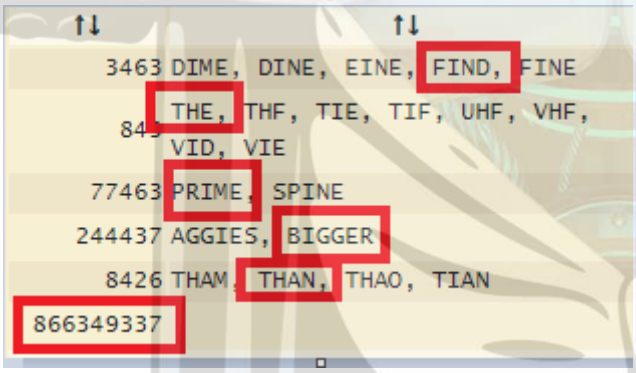
-I will text what you need

-3463008430077463002444370084260086634933 7

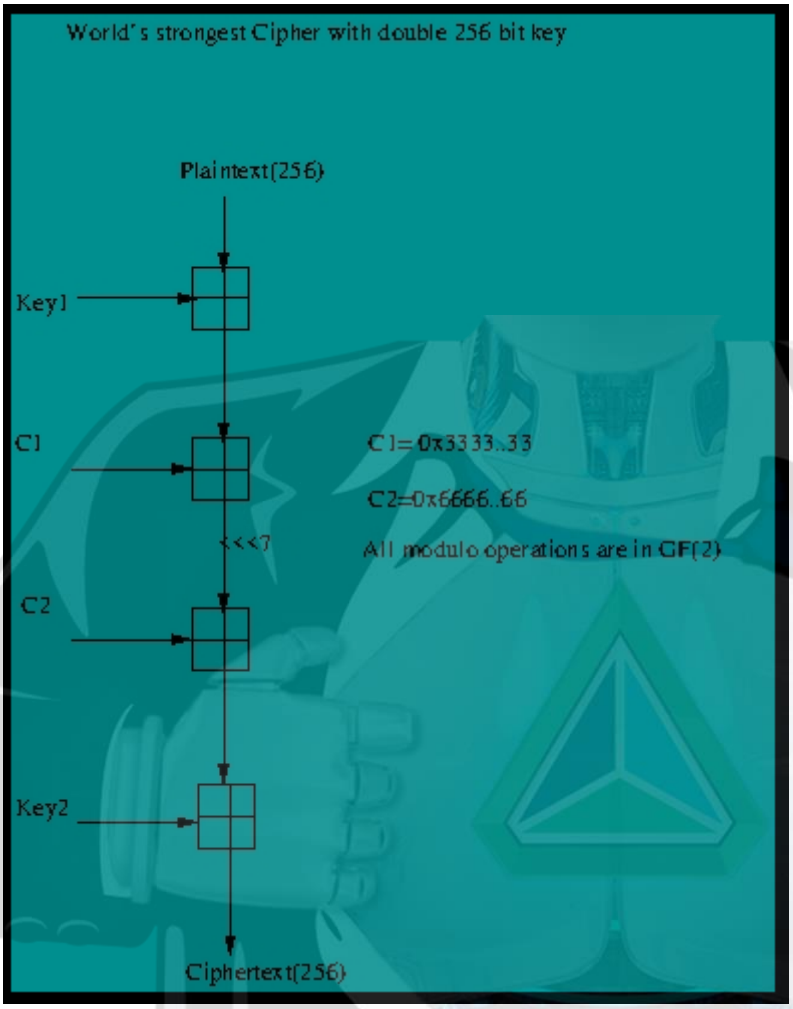
Top Secret
Encryptor
Decryptor

Clearly the user must decrypt the long hex value. There are 3 links in the page. First one links to topsecret.rar file which is also encrypted. The page title "Tnine" and "I will text …" gives a hint about T9 keyboard on old phones.

3463008430077463002444370084260086634933 7 can be decrypted using online decoders like this:



The decrypted value is clear: Find the prime bigger than 866349337. 866349337 is an composite number, 866349338 is also even, continuing this way and using online prime testers gives the next prime integer as 866349347. Using this as the rar password gives the following picture:



This is the encryption function used in the question. This is a toy linear cipher since all the modulo operations are in GF(2) which is indeed just an XOR. So the ciphertext value can be get;

$$C = (P \oplus K_1 \oplus C_1)_{rot7} \oplus C_2 \oplus K_2$$

Since this is a linear cipher with respect to XOR operation we can rewrite the equation as:

$$C = P_{rot7} \oplus C_{1rot7} \oplus C_2 \oplus K_{1rot7} \oplus K_2$$

Now the constant $C_{1rot7} \oplus C_2$ simply equals to 0xFFF…FF. So simply giving the plaintext value of all one, these cancels each other and you get $K_{1rot7} \oplus K_2$ as the ciphertext value!

You don't need to implement the algorithm since encryptor is already given in the question. Simply encrypt 0xFFFF..FF and you will get the sum of the keys!

Welcome to Encryption Oracle, give the plaintext and get the ciphertext!

Plaintext(hex)
Submit
Plaintext: 0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
Ciphertext: 0xda8227807079383036034 9f6815b87b36cf9fae36ba7e0d954f5018e2c3316e3

Now we get the sum of keys as ciphertext and in order to solve the question you just need xoring the following values and rotate it 7 bits right!

$$P_{rot7} = C \oplus 0xFFFF..FF \oplus K_{1rot7} \oplus K_2$$

Which gives the plaintext as:
0x53544d4354467b4c316e3340725f633170683372735f4072655f6240447d

A simple Hex to Ascii conversion gives the flag: **STMCTF{L1n3@r_c1ph3rs_@re_b@D}**