LOGCAESAR - CRYPTO 100

The satellite communications have stopped working – suddenly they're sending back unknown algorithms. Help R-boy decipher them.

The encryption function was:

```
for i in range(0,256):
    new_pos = (3**(key+i)) % 257
    ciphertext[new_pos-1] = ((content[i])^i)^(new_pos-1)
```

So the original file content is xored with the index of the for and (new_pos-1), if we want to retrieve the flag we only have xor the encrypted_message[new_pos-1] with the two indexes (i and [new_pos-1]) and put it at index i.

The only problem is that we didn't have the key so we tried all possible values between 0 and 256 as it is used in an operation with a modulus of 257.

So the function to decrypt the flag will be:

```
for k in range(256):
    for i in range(0,256):
        new_pos = (3**(k+i)) % 257
        decrypted_mex[i] = encrypted_mex[new_pos-1]^i^(new_pos-1)
```

{FLG:but_1_th0ught_Dlog_wa5_h4rd}