CTF NAME

Krypto 5

CHALLENGE DESCRIPTION

Med endast en 4 tecken lång nyckel har jag gjort texten oigenkännlig. Exklusivt eller hur?

VryUmIMq|U`KtUVKgyKFtH`GaySAzMLS

TOOLS USED

- https://gchq.github.io/CyberChef/

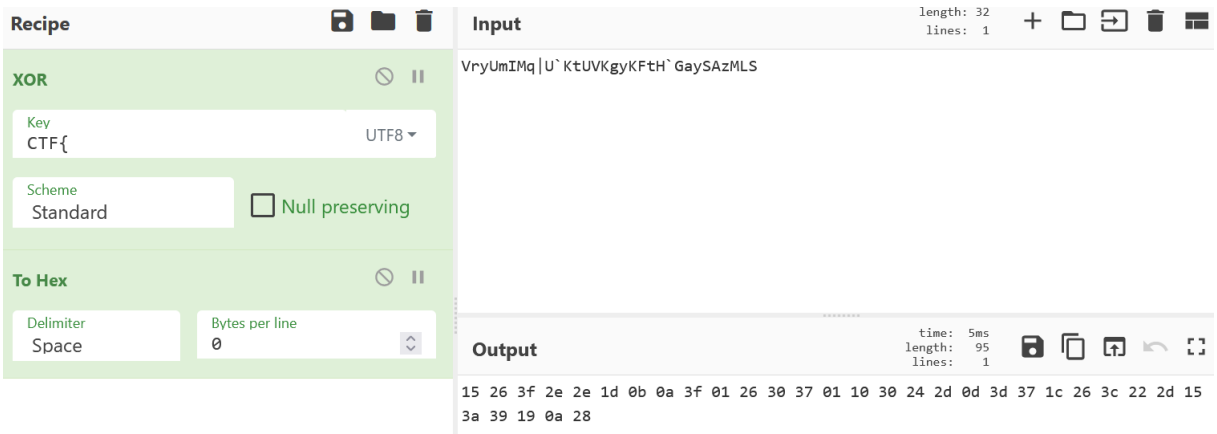
SOLUTION

I texten står det att det krypteringen är ”Exklusivt eller hur?”, vilket leder tankarna till XOR-kryptering. Där används en nyckel för att göra en matematisk operation på texten. Hela nyckelns längd jämförs med texten och utsätts för en xor, om nyckeln är kortare än texten så kommer nyckeln köras om och om igen.

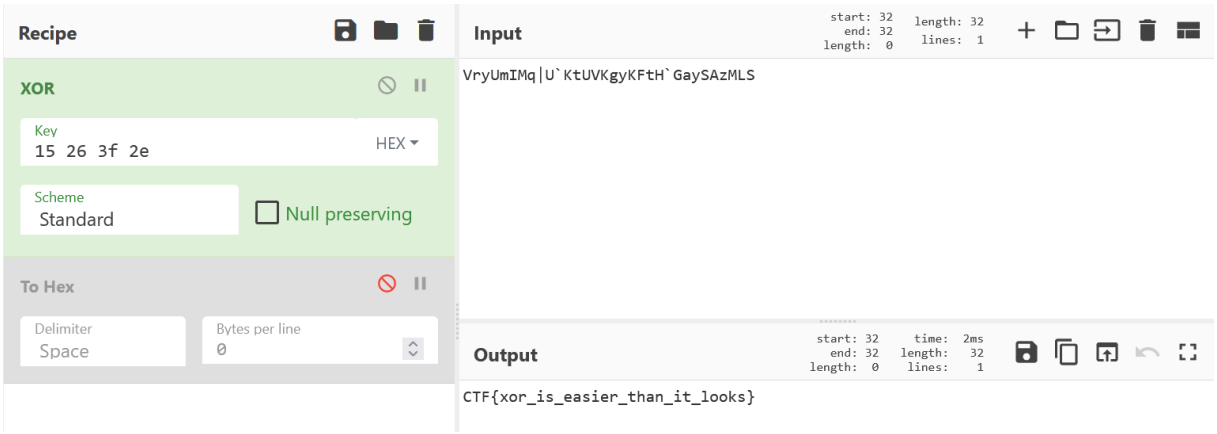
Säg att vi har 1010 som nyckel och 1111 0000 som text. Då kommer först 1111 xoras med 1010, sedan kommer 0000 xoras med 1010.

Eftersom vi vet att flaggformatet är CTF{<flagga>} och CTF{ är fyra karaktärer kan vi xora den krypterade texten mot CTF{ för att få fram nyckeln. Detta kallas för en known plaintext attack, går att läsa mer om här https://blog.didierstevens.com/2016/01/01/xor-known-plaintext-attack/.

Jag öppnade upp cyberchef och la in strängen xorad mot CTF{ och översatte resultatet till hex.



Sedan tar vi de 4 första, 15 26 3f 2e och xorar mot den krypterade texten.



FLAG

CTF{xor_is_easier_than_it_looks}