

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 xored mot CTF{ och översatte resultatet till hex.

The screenshot shows the CyberChef web application interface. On the left, the 'Recipe' panel is active, showing an 'XOR' operation with a key of 'CTF{' and a 'To Hex' operation with a space delimiter. The 'Input' panel on the right contains the text 'VryUmIMq|U`KtUVKgYKFtH`GaySAzMLS'. The 'Output' panel at the bottom displays the resulting hex string: '15 26 3f 2e 2e 1d 0b 0a 3f 01 26 30 37 01 10 30 24 2d 0d 3d 37 1c 26 3c 22 2d 15 3a 39 19 0a 28'. Metadata for the input shows a length of 32 and 1 line, while the output shows a time of 5ms, length of 95, and 1 line.

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

**Recipe**

XOR

Key  
15 26 3f 2e  
HEX ▾

Scheme  
Standard

☐ Null preserving

To Hex

Delimiter  
Space

Bytes per line  
0

start: 32  
end: 32  
length: 0

length: 32  
lines: 1

+  
-  
↩  
🗑️

VryUmIMq|U`KtUVKgyKFtH`GaySAzMLS

start: 32  
end: 32  
length: 0

time: 2ms  
length: 32  
lines: 1

🗑️  
📄  
↩  
🔍

CTF{xor\_is\_easier\_than\_it\_looks}

## FLAG

CTF{xor\_is\_easier\_than\_it\_looks}