Yusa的密码学课堂-ECB

发表于 2021-03-05 更新于 2021-03-15 分类于 Challenge ， 2020 ， SWPU CTF 2020 ， Crypto
Challenge | 2020 | SWPU CTF 2020 | Crypto | Yusa的密码学课堂-ECB

点击此处获得更好的阅读体验

WriteUp来源

官方WP

解题思路

由于是ECB的模式，所以当我们输入十五个`0`后，服务会将十五个`0+flag`加密，而此时第一组就是十五个'0'和flag的第一个字符。即，返回的明文的第一组是`'0'*15 + flag[0]`的密文。

我们遍历0-255，发送`'0'*15+chr(i)`，看返回的密文是不是和最初获得的密文的第一组一致，如果一致，那么此时的`chr(i)`就是flag的第一位。

有了第一位我们就可以发送`'0'*14+flag[0]`过去，此时返回的第一组密文就是`'0'*14+flag[0]+flag[1]`的密文了，我们继续用第2步的方法就可以恢复flag[1]了。

如此循环往复，逐位爆破flag。

 # Challenge # 2020 # Crypto # SWPU CTF 2020
happy
Yusa的密码学课堂-CBC第一课