HGAME 2022 Week1 writeup by z3

CRYPTO

Block Cipher

该程序将flag分为8个字符的bytes片段末尾补齐，第一段和key，iv异或，剩余和key以及上一段异或。由于异或可逆，易得flag。

Multi Prime RSA

多素数rsa，n的欧拉函数为

$$f(n) = n * \Pi(1 - 1/ai)$$

然后计算d解密即可

RSA Attack 3

n和e都很大，可以尝试维纳攻击。结果证明可行，得出flag。