实验 - 密码学基础

实验简介

利用数学知识完成关于对最大公约数以及乘法逆元的求解。同时进阶部分将考察对伪随机生成器LFSR的逆推过程。

基础部分

1. 求解两个数之间的最大公约数（50分）

回顾：最大公因数是指能够整除多个整数的最大正整数。

实验要求：

（1）编程语言不限，但只能使用标准库，即要求手写求解最大公约数的逻辑。

（2）程序要求输入两个正整数，最终输出这两个正整数的最大公约数。

（3）通过测试数据，输入91395511562897和16296857514254，能正确求解这两个数的最大公约数。

注意事项：

（1）如果使用C/C++进行编写，只需要考虑64位大小（即unsigned long long）以内的正整数。

（2）实验报告中只需要对实验结果进行截图以及附带程序源代码。

Hint：

（1）完成本道题的核心是等式：gcd(a,b) = gcd(b,a mod b)

（2）在算法实现上，利用辗转相除法求得最大公约数。

2. 求解乘法逆元（50分）

回顾：若a*b≡1 (mod n), 则称a是b的乘法模n逆元，b是a的乘法模n逆元。a的乘法逆元记作a-1。

实验要求：

（1）编程语言不限，但只能使用标准库，即要求手写求解最大公约数的逻辑。

（2）程序要求输入两个正整数，第一个数是a，第二个数是n，要求最终输出a的乘法模n逆元。

（3）通过测试数据，输入205063029(a)和168897669160271(n)，能正确求解出a的乘法模n逆元。

注意事项：

（1）如果使用C/C++进行编写，只需要考虑64位大小（即unsigned long long）以内的正整数。

（2）实验报告中只需要对实验结果进行截图以及附带程序源代码。

Hint：

（1）求解乘法逆元可以使用欧几里得算法。

（2）当gcd(a,n)!=1时，a的乘法模n逆元不存在。

（3）当a>n时，a的乘法模n逆元等价于a%n的乘法模n逆元。

挑战部分

伪随机生成器LFSR求解

题目：

```
from binascii import hexlify

mask = 0x8bc3210d00331741833ca3c4af14f82293653df561b4b55a5a41
limit = 0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

def LFSR(input):
    output = (input << 1) & limit
    i = (input & mask) & limit
    lsb = 0
    while i != 0:
        lsb ^= (i & 1)
        i = i >> 1
    output ^= lsb
    return (output, lsb)

flag = b'ACTF{....}'

assert len(flag) == 32
R = int(hexlify(flag[5: -1]), 16)

tmp = 0
for i in range(208):
    (R, lsb) = LFSR(R)
    tmp = (tmp << 1) | lsb
print(hex(tmp))

#0x3a7c0143e3e26d1425b5c3d2d2ae4041de5e22f6557836bdae6f
```

说明：

本题来自ACTF2019-Warmup3

变量flag是私密信息，请求解之。

题目脚本无法直接运行，因为变量flag信息是不完整的(其中....的内容需要通过解密恢复出来)。

实验要求：

编程语言不限。

完成求解逻辑，并提交源代码和flag。