HGAME 2022 Week1 writeup by 黎明

CRYPTO

EASY RSA

task.py中的主要函数如下：

```
**def encrypt(c):**
  **p = getPrime(8)**
  **q = getPrime(8)**
  **e = randint(0, p * q)**
  **while gcd(e, (p - 1) * (q - 1)) != 1:**
    **e = int(next_prime(e))**
  **return e, p, q, pow(ord(c), e, p * q)**
```

它的主要功能是输入明文c，输出参数e，p，q与密文m（设密文为m，求m的过程：任取两个素数p，q以及任取一个与(p - 1) * (q - 1)互质的e，即与φ(n)互质（设n=p*q）的e，那么密文m=c^e mod n）。

那么想要解出明文就需要计算出d（设e*d mod φ(n) ≡1），我计算d的方法如下：

因为*ed=φ(n)*k+1（k为正整数），所以设f=φ(n)*k+1（k从1开始，依次往上增加1），当f mod e≡0时即可求出d=f/e

那么明文c=m^d mod n。

整个程序如下：

```
** from math import gcd**
 **def decrypt(ls):**
  **e = int(ls[0])**
  **p = int(ls[1])**
  **q = int(ls[2])**
  **B = int(ls[3])**
  **f = (p-1)*(q-1)**
  **for i in range(e):**
    **if (f*i+1) % e == 0:**
     **d = int((f*i+1)/e)**
  **A = pow(B, d, p*q)**
  **return chr(A)**
if __name__ == '__main__':
```

```
**str = ''**

**flag = [(12433, 149, 197, 104), (8147, 131, 167, 6633), (10687, 211, 197,
35594), (19681, 131, 211, 15710), (33577, 251, 211, 38798), (30241, 157, 251,
35973), (293, 211, 157, 31548), (26459, 179, 149, 4778), (27479, 149, 223, 32728),
(9029, 223, 137, 20696), (4649, 149, 151, 13418), (11783, 223, 251, 14239), (13537,
179, 137, 11702), (3835, 167, 139, 20051), (30983, 149, 227, 23928), (17581, 157,
131, 5855), (35381, 223, 179, 37774), (2357, 151, 223, 1849), (22649, 211, 229,
7348),(1151, 179, 223, 17982), (8431, 251, 163, 30226), (38501, 193, 211, 30559),
(14549, 211, 151, 21143), (24781, 239, 241, 45604), (8051, 179, 131, 7994), (863,
181, 131, 11493), (1117, 239, 157, 12579), (7561, 149, 199, 8960), (19813, 239, 229,
53463), (4943, 131, 157, 14606), (29077, 191, 181, 33446), (18583, 211, 163, 31800),
(30643, 173, 191, 27293), (11617, 223, 251, 13448), (19051, 191, 151, 21676),
(18367, 179, 157, 14139), (18861, 149, 191, 5139), (9581, 211, 193, 25595)]**

**for ls in flag:**

  **str += decrypt(ls)**

**print(str)**
```