Easy_RSA

출제의도: RSA는 가장 널리 사용되는 공개키 암호 알고리즘으로 문제를 푸는 과정을 통해 RSA를 접해보았으면 해서 문제를 내봤습니다. 저번 1회 KEEPER CTF에 출제되었기도 해서 1회 CTF를 참가하셨던 분들이라면 복습할 기회가 되었을 것으로 생각합니다.

문제에는 n,e,c가 주어졌습니다.
주어진 숫자 중 n을 이용하여 두 개의 서로 다른 소수의 곱으로 바꾸어주어 p와 q를 구합니다. n을 입력하면 p와 q를 쉽게 구해주는 사이트를 같이 첨부하겠습니다.
http://factordb.com/index.php (>>> n = p*q를 만족하는 p, q를 구하기)
RSA는 모듈러 거듭제곱 연산을 이용하여 동작하기 때문에 이에 맞게 코드를 작성해주셔서 풀어주시면 됩니다. 저는 파이썬을 이용하여 코드를 작성하였습니다.

```python
def zx(a,b):
    if a==0:
        return (b,0,1)
    else:
        g,y,x = zx(b%a, a)
        return (g, x - (b//a)*y, y)


def modi(a,m):
    g,x,y = zx(a,m)
    if g!=1:
        raise Exception('modular inverse does not exist')
    else:
        return x%m


p = ''
q = ''

n = ''
e = ''
c = ''

fi = (p-1)*(q-1)
d = modi(e,fi)

flag = hex(pow(c,d,n))[2:]

print(chr(int(flag,16)))
```

이를 이용해 flag를 구하게 된다면
KEEPER{W0o0o0ooow_h1_ke3eE3eP3R_UnT0oooC_Im_rsA} 를 구할 수 있습니다.

rolling_paper

출제의도: 한 번쯤은 접해보셨을 만한 암호 중 막대기에 종이를 감는 형태인 카이사르 암호입니다. 과거에 사용되었던 고전암호 중 하나입니다.

문제의 파일이 rolling_paper인 점과 쪽지 그리고 나무막대기를 통해 카이사르 암호를 통해 문제를 풀어야 함에 대해 힌트를 드렸습니다. 쪽지의 크기를 주지 않고 막대기의 지름이 6cm인 것으로 실제로 막대기에 종이를 감는 것이 아닌 코드를 짜서 풀어야 문제를 풀 수 있게 유도하였습니다. 이때 지름이 6cm라는 것으로 해당 글자에서 6번째 뒤에 오는 글자가 바로 다음에 오는 글자임을 내포하였습니다.

이를 통해 코드를 짜보면 다음과 같습니다. 저는 파이썬을 이용해 코드를 작성하였습니다.

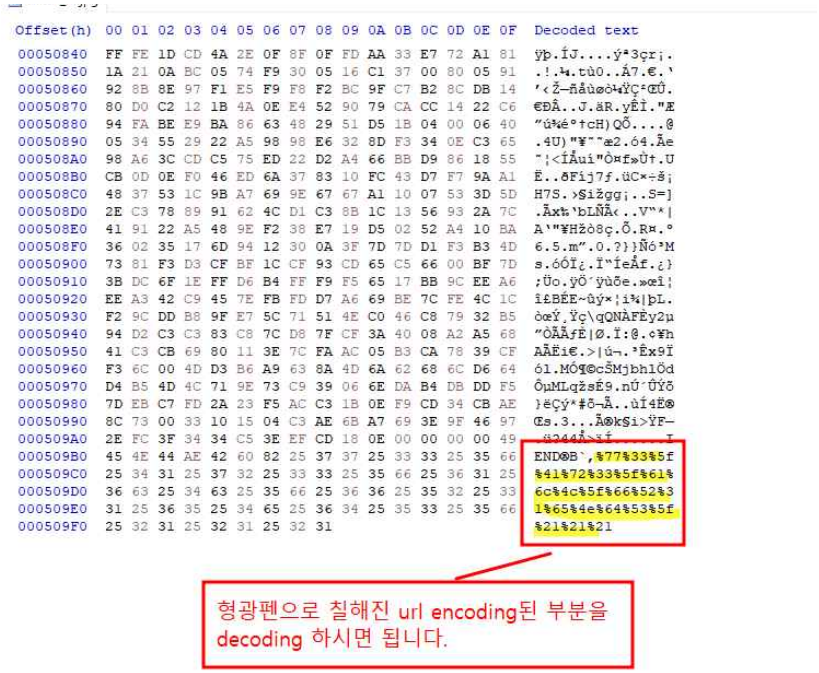
```
1  n = 0
2  x = int(input())
3  y = input()
4  for i in range(6):
5      while n < len(y):
6          print(y[n+i], end = '')
7          n += x
8      n = 0
9
```

flag는 KEEPER{RoL1n9_Pap3r_mAk3_CrYpt0}입니다.

Easy_pokemon

출제의도: url encoding이 어떤 형태로 이루어져 있는지 알아보고자 문제를 출제하였습니다. url encode말고도 base64, ASCII hex, hex, binary 등 다양한 형태의 encoding이 있습니다. 이에 대해 알아두시면 좋을 것 같습니다.

HxD와 같은 Hex Editor 프로그램으로 사진을 열어보아야 푸실 수 있습니다.



flag는 KEEPER{w3_Ar3_alL_fR1eNdS_!!!} 입니다.