

## 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  $n, e, c$ 가 주어졌습니다.

주어진 숫자 중  $n$ 을 이용하여 두 개의 서로 다른 소수의 곱으로 바꾸어주어  $p$ 와  $q$ 를 구합니다.  $n$ 을 입력하면  $p$ 와  $q$ 를 쉽게 구해주는 사이트를 같이 첨부하겠습니다.

<http://factordb.com/index.php> ( >>>  $n = p \cdot q$ 를 만족하는  $p, q$ 를 구하기)

RSA는 모듈러 거듭제곱 연산을 이용하여 동작하기 때문에 이에 맞게 코드를 작성해주셔서 풀어주시면 됩니다. 저는 파이썬을 이용하여 코드를 작성하였습니다.

```
1 def zx(a,b):
2     if a==0:
3         return (b,0,1)
4     else:
5         g,y,x = zx(b%a, a)
6         return (g, x - (b//a)*y, y)
7
8
9 def modi(a,m):
10     g,x,y = zx(a,m)
11     if g!=1:
12         raise Exception('modular inverse does not exist')
13     else:
14         return x%m
15
16
17 p = ''
18 q = ''
19
20 n = ''
21 e = ''
22 c = ''
23
24 fi = (p-1)*(q-1)
25 d = modi(e,fi)
26
27 flag = hex(pow(c,d,n))[2:]
28
29 print(chr(int(flag,16)))
30
```

이를 이용해 flag를 구하게 된다면

KEEPER{W0o0o0ooow\_h1\_ke3eE3eP3R\_UnT0oooC\_lm\_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 encode 말고도 base64, ASCII hex, hex, binary 등 다양한 형태의 encoding이 있습니다.  
이에 대해 알아두시면 좋을 것 같습니다.

HxD와 같은 Hex Editor 프로그램으로 사진을 열어보아야 풀 수 있습니다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00050840	FF	FE	1D	CD	4A	2E	0F	8F	0F	FD	AA	33	E7	72	A1	81	yp.IJ....y*3qxi.
00050850	1A	21	0A	BC	05	74	F9	30	05	16	C1	37	00	80	05	91	..!.4.tu0..A7.e.'
00050860	92	8B	8E	97	F1	E5	F9	F8	F2	BC	9F	C7	B2	8C	DB	14	'<Z-ââûøôYÇ²GÜ.
00050870	80	D0	C2	12	1B	4A	0E	E4	52	90	79	CA	CC	14	22	C6	ëDÄ..J.aR.yēI..E
00050880	94	FA	BE	E9	BA	86	63	48	29	51	D5	1B	04	00	06	40	"ú%é*+cH)QÖ...@
00050890	05	34	55	29	22	A5	98	98	E6	32	8D	F3	34	0E	C3	65	.4U)"¥""a2.ô4.Äe
000508A0	98	A6	3C	CD	C5	75	ED	22	D2	A4	66	BB	D9	86	18	55	"!<IAui"Ôhf»Ü†.U
000508B0	CB	0D	0E	F0	46	ED	6A	37	83	10	FC	43	D7	F7	9A	A1	È..øFij7f.ûC*-s;
000508C0	48	37	53	1C	9B	A7	69	9E	67	67	A1	10	07	53	3D	5D	H7S.}§iZggi..S=}
000508D0	2E	C3	78	89	91	62	4C	D1	C3	8B	1C	13	56	93	2A	7C	.Äx%`bLÄ<..V""
000508E0	41	91	22	A5	48	9E	F2	38	E7	19	D5	02	52	A4	10	BA	A'"#H2ô8ç.Ö.RH.°
000508F0	36	02	35	17	6D	94	12	30	0A	3F	7D	7D	D1	F3	B3	4D	6.5.m".0.?)}Nô*M
00050900	73	81	F3	D3	CF	BF	1C	CF	93	CD	65	C5	66	00	BF	7D	s.ôÖIç.I"iÄf.ç;
00050910	3B	DC	6F	1E	FF	D6	B4	FF	F9	F5	65	17	BB	9C	EE	A6	;Üo.yÖ'yûöe.æi;
00050920	EE	A3	42	C9	45	7E	FB	FD	D7	A6	69	BE	7C	FE	4C	1C	iÄBEE-ûy*!iç pL.
00050930	F2	9C	DD	B8	9F	E7	5C	71	51	4E	C0	46	C8	79	32	B5	ôæY.Yç\qQNAFëy2µ
00050940	94	D2	C3	C3	83	C8	7C	D8	7F	CF	3A	40	08	A2	A5	68	"ÖÄÄfE ø.I:ø.c¥h
00050950	41	C3	CB	69	80	11	3E	7C	FA	AC	05	B3	CA	78	39	CF	ÄÄEiE.> û~.*Ëx9I
00050960	F3	6C	00	4D	D3	B6	A9	63	8A	4D	6A	62	68	6C	D6	64	ô1.MÔgøc5Mjbh1ôd
00050970	D4	B5	4D	4C	71	9E	73	C9	39	06	6E	DA	B4	DB	DD	F5	ÔµMLqZsE9.nÜ'ÜYô
00050980	7D	EB	C7	FD	2A	23	F5	AC	C3	1B	0E	F9	CD	34	CB	AE	!æçy*#ô-Ä..ûi4Eø
00050990	8C	73	00	33	10	15	04	C3	AE	6B	A7	69	3E	9F	46	97	Qs.3...Äøk§1>YF-
000509A0	2E	FC	3F	34	34	C5	3E	EF	CD	18	0E	00	00	00	00	49	g2æÄ>st
000509B0	45	4E	44	AE	42	60	82	25	37	37	25	33	33	25	35	66	END0B",%77%33%5f
000509C0	25	34	31	25	37	32	25	33	33	25	35	66	25	36	31	25	%41%72%33%5f%61%
000509D0	36	63	25	34	63	25	35	66	25	36	36	25	35	32	25	33	6c%4c%5f%66%52%3
000509E0	31	25	36	35	25	34	65	25	36	34	25	35	33	25	35	66	1%65%4e%64%53%5f
000509F0	25	32	31	25	32	31	25	32	31								%21%21%21

형광펜으로 칠해진 url encoding된 부분을  
decoding 하시면 됩니다.

flag는 KEEPER{w3\_Ar3\_alL\_fR1eNdS\_!!!} 입니다.