SUNDAY 30 APRIL 2017 (2017-04-30) | **Unknown author**

UIUCTF 2017 - 100 - High School Crypto - Crypto

Informations

Version

By	Version	Comment
noraj	1.0	Creation

CTF

- **Name** : UIUCTF 2017
- **Website** : sigpwny.github.io
- **Type** : Online
- **Format** : Jeopardy
- **CTF Time** : link

Description

> Bulljog isn't much harder than this one.
>
> encrypt.py encryptme.txt.out

Solution

encrypt.py is a simple xoring:

```
1 import sys, itertools
2 if(len(sys.argv) != 3):
3 print("Usage: [FILE] [KEY]")
4 exit(-1)
5 filename = sys.argv[1]
6 key = sys.argv[2]
```

```
7  with open(filename, 'rb') as plaintext:
8  raw = plaintext.read()
9  print(len(raw))
10 with open(filename + '.out', 'wb') as ciphertext:
11 for l, r in zip(raw, itertools.cycle(key)):
12 ciphertext.write( (l ^ ord(r)).to_bytes(1, byteorder='big') )
13
14
```

Let's xortool show us some probability:

```
1  $ xortool encryptme.txt.out
2  The most probable key lengths:
3  1: 8.2%
4  3: 11.0%
5  6: 10.0%
6  9: 21.0%
7  12: 7.7%
8  15: 6.9%
9  18: 13.7%
10 27: 9.4%
11 36: 6.8%
12 45: 5.3%
13 Key-length can be 3*n
14 Most possible char is needed to guess the key!
```

xortool tell us there is 21% chances of a 9 bytes length key. So let's try it:

```
1  $ xortool encryptme.txt.out -l 9 -o
2  200 possible key(s) of length 9:
3  \x04EYS[\x06Q^T
4  \x04EYS[CQ^T
5  \x05DXRZ\x07P_U
6  \x05DXRZBP_U
7  \x06G[QY\x04S\\V
8  ...
9  Found 89 plaintexts with 95.0%+ printable characters
10 See files filename-key.csv, filename-char_used-
   perc_printable.csv
```

One key seems nearly good:

```
1 $ cat xortool_out/filename-key.csv | grep 189
2 xortool_out/189.out;\x14UICKSAND
```

So let's try it:

```
1  $ xortool-xor -f encryptme.txt.out -s QUICKSAND
```

```
malfunctioning random number generators, but the extent
to which these problems arise in practice has never been
comprehensively studied at Internet scale. We perform
the largest ever network survey of TLS and SSH servers
and present evidence that vulnerable keys are surprisingly
widespread. We find that 0.75% of TLS certificates share
keys due to insufficient entropy during key generation,
[...]

```

The output is 100% printable text, we have the good key, now I need to find the flag:

```
$ xortool-xor -f encryptme.txt.out -s QUICKSAND | grep -i
flag
flag{st8_of_grac3}
```
