JUNE 9, 2017 / CTF

QUADRATHLON 2017 WRITEUP – PART 1

Hello – Trivia 1pt

```
Selamat datang di Quadrathlon 2017~~
Format flag adalah : noob{flag_format}. Silahkan dicoba submit :)
```

Nothing special, tinggal masukin contoh flag.

Flag : noob{flag_format}

NYN 1.0 – Trivia 10pts

```
Now You Know 1.0
Suatu cara untuk mencari tahu apakah file yang dikirim dan yang diterima
dalam transmisi data tetap sama atau tidak (flag dalam huruf kecil semua)
```

Flag : noob{checksum}

NYN 2.0 – Trivia 10pts

```
Now You Know 2.0
Nama kelompok peretas yang berhasil melakukan dumping tools
hacking milik NSA yang kemudian dimanfaatkan seseorang/sekelompok yang
lain untuk membuat WannaCry (flag dalam huruf kecil semua)
```

Flag : noob{shadowbroker}

NYN 3.0 – Trivia 10pts

```
Now You Know 3.0
Nama domain yang digunakan WannaCry sebagai kill-switch
```

Flag : noob{iuqerfsodpgifjaposdfjhgosurijfaewrwergwea.com}

NYN 4.0 – Trivia 10pts

```
Now You Know 4.0
Nomor port yang dimanfaatkan WannaCry
```

Flag : noob{445}

Bas[e]ic – Crypto 50pts

```
Decrypt me please. Hehe
```

Setelah link pada soal dibuka. Ternyata muncul text alphanumeric yang sangat panjang. Lalu dilihat dari ciri-cirinya (diakhiri tanda =), kemungkinan besar text tersebut adalah hasil enkripsi base64. Coba di decrypt lalu didapatkan

Flag : noob{DIAMMM!}

Puter – Crypto 25pts

```
abbo{qnygbx_jrf_vxv_synt_r}
```

Ini adalah kriptografi dengan rot13. Metode ini mengkonfersi setiap string (misalkan) X menjadi (X+13) mod Z. Atau sama dengan di shift 13x dimana dalam shifting tersebut apabila melewati Z, maka kembali ke A.

Flag : noob{daltok_wes_iki_flag_e}

Kembaran – Crypto 100pts

```
Shakijem menemukan sebuah peti harta karun. Di dalam peti itu terdapat sebuah
surat yang mengatakan "Pecahkan misteri yang ada di sini untuk mendapatkan harta
karun". Bantu Shakijem untuk memecahkan misteri tersebut!
```

Halaman yang ada di soal merujuk pada sebuah halaman yang berisi form untuk mengirimkan 2 file ke server. File tersebut meminta 2 file yang kembar. Berarti kita harus mengirimkan 2 file yang identik ke server. Dimana identik disini bukan berarti file yang sama persis.

Sedangkan untuk mengetahui apakah 2 file adalah file yang sama, kita harus melakukan checksum (sudah ada di soal trivia kan, hehe). Checksum dilakukan dengan meg-enkripsi setiap byte yang ada di file dengan suatu algoritma kriptografi modern, misalkan MD5, SHA1, SHA256, dsb. Dengan digunakannya algoritma modern, apabila 2 file memiliki minimal 1 byte yang berbeda, akan menghasilkan checksum yang sangat berbeda di antara keduanya.

Namun bagaimana bisa 2 file yang tidak sama memiliki checksum yang sama persis? Hal inilah yang disebut *collision,* yaitu ketika 2 plain text yang berbeda lalu dienkripsi dengan algoritma yang sama, menghasilkan encrypted text yang sama.

SHA1 sendiri adalah salah satu algoritma yang paling terakhir ditemukan collision nya. Jadi soal ini bertujuan untuk membuat 2 file yang memiliki colliding SHA1 checksum. Bagaimana caranya? Sudah banyak bertebaran online tool untuk men-generate 2 file yang collide. Saya menggunakan website ini. Cukup cari 2 file jpg yang memiliki ukuran lebar dan tinggi yang sama. Lalu akan di generate 2 pdf yang memiliki checksum yang sama. Lalu submit kedua pdf itu.

Flag : noob{sha1_now_ezly_collided}

Kasmaran – Crypto 175pts

```
Via menerima sebuah surat aneh di depan pintu rumahnya. Yang tertulis disana
sangatlah aneh, kecuali nama pengirim yang bernama Kley. Akhirnya Via yang
penasaran memintamu untuk mencari tahu isi sebenarnya surat misterius tersebut
```

Yang ada di dalam attachment soal ini adalah 2 file, yaitu file python dan file yang berekstensi 'out'. Dimana script python tersebut melakukan sebuah enkripsi pada setiap byte dalam file ***uoy_evol*** dan menghasilkan output berupa ***uoy_evol.out***.

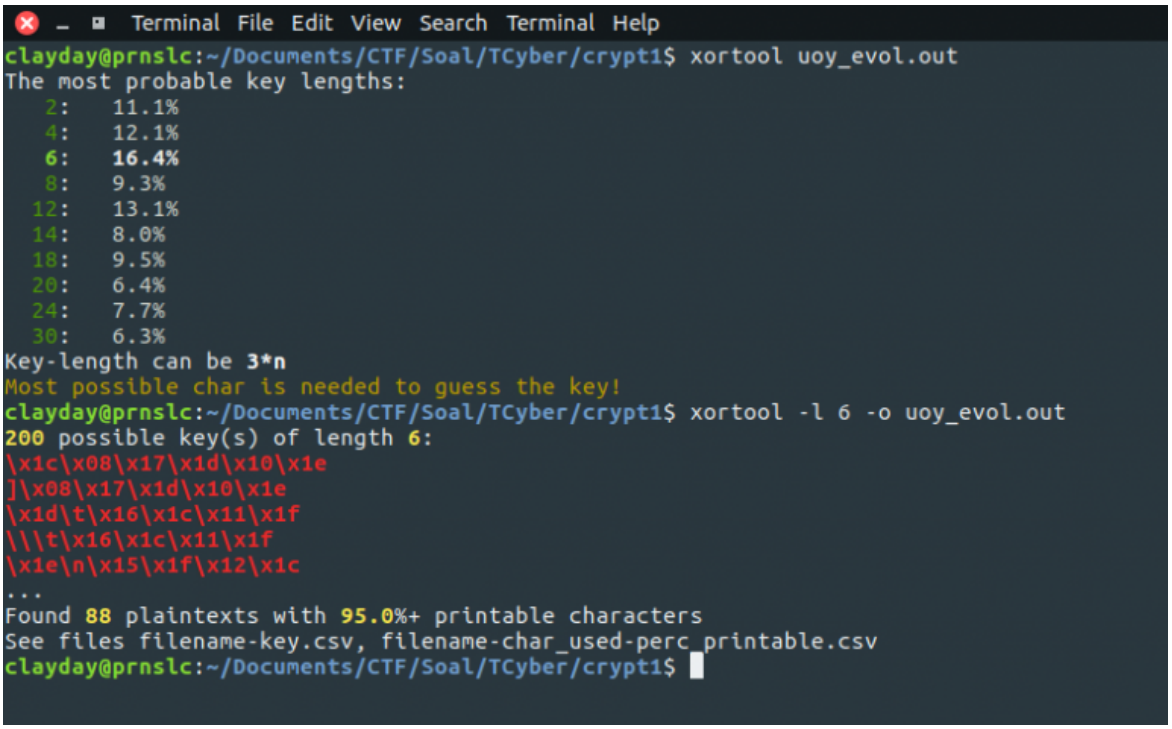
```
import sys, itertools

if(len(sys.argv) != 3):
 print("Cara Pemakaian: [FILE] [KEY]")
 exit(-1)

nama = sys.argv[1]
kunci = sys.argv[2]
```

```
with open(nama, 'rb') as i:
 raw = i.read()
 print(len(raw))
 with open(nama + '.out', 'wb') as jadi:
 for l, r in zip(raw, itertools.cycle(kunci)):
 jadi.write(chr(ord(l) ^ ord(r)))
```

Script ini menerima 2 input melalui argumen, yang pertama adalah nama file yang akan di enkripsi, yang kedua adalah sebuah key yang digunakan untuk mengenkripsi file tersebut. Proses enkripsi file terdapat di iterasi for. Skrip tersebut melakukan XOR di antara byte file dan string key. Jadi misalkan isi file adalah ABCDEFGH, dan di enkripsi menggunakan key NM, maka yang terjadi :

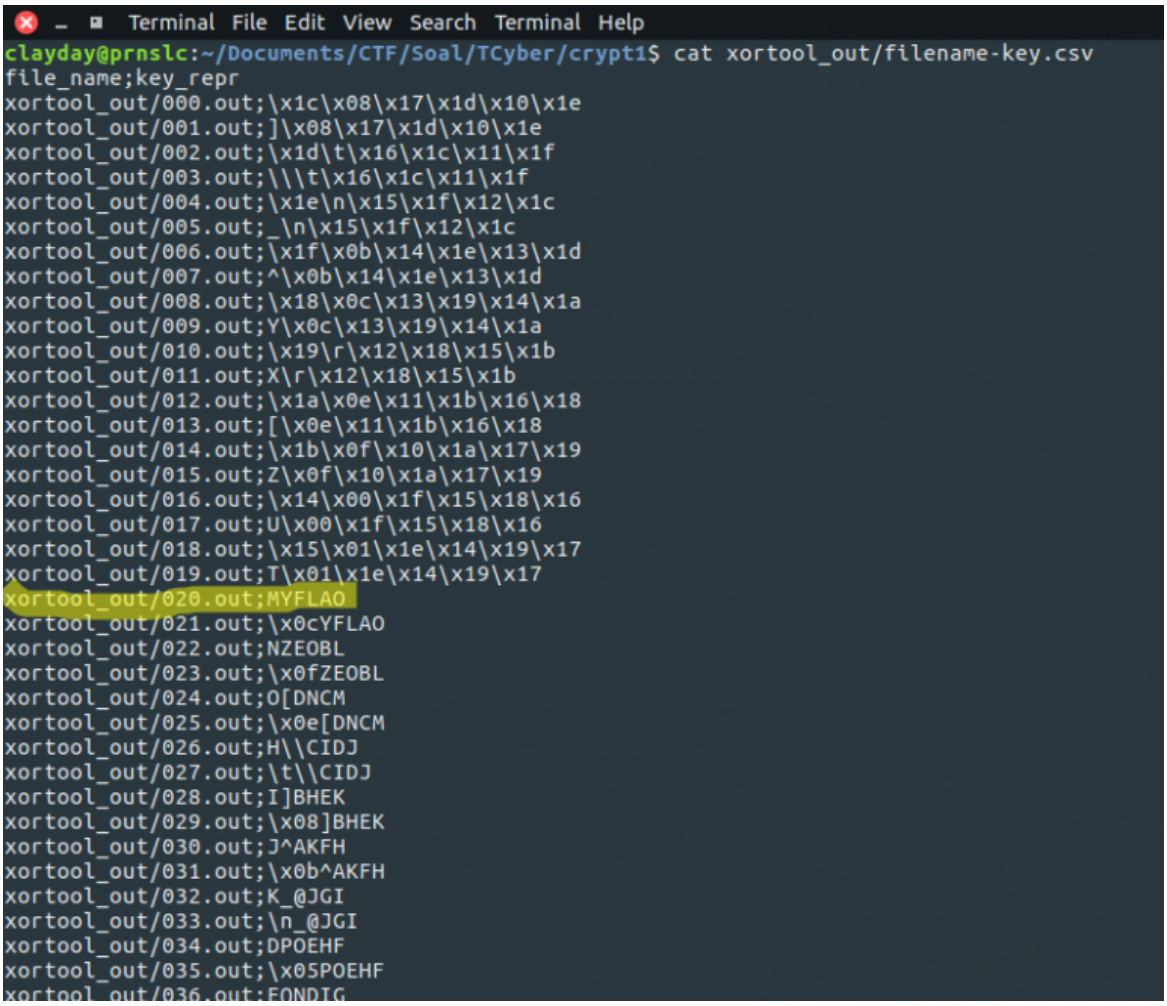
```
A ^ N = ...
B ^ M = ...
C ^ N = ...
D ^ M = ...
......
dan seterusnya hingga H
```

Berarti untuk melakukan decrypt, kita harus terlebih dulu mengetahui kunci apa yang dimasukkan pembuat soal untuk mendekripsi file aslinya. Karena enkripsi ini dilakukan dengan XOR, maka kita bisa menggunakan xortool.

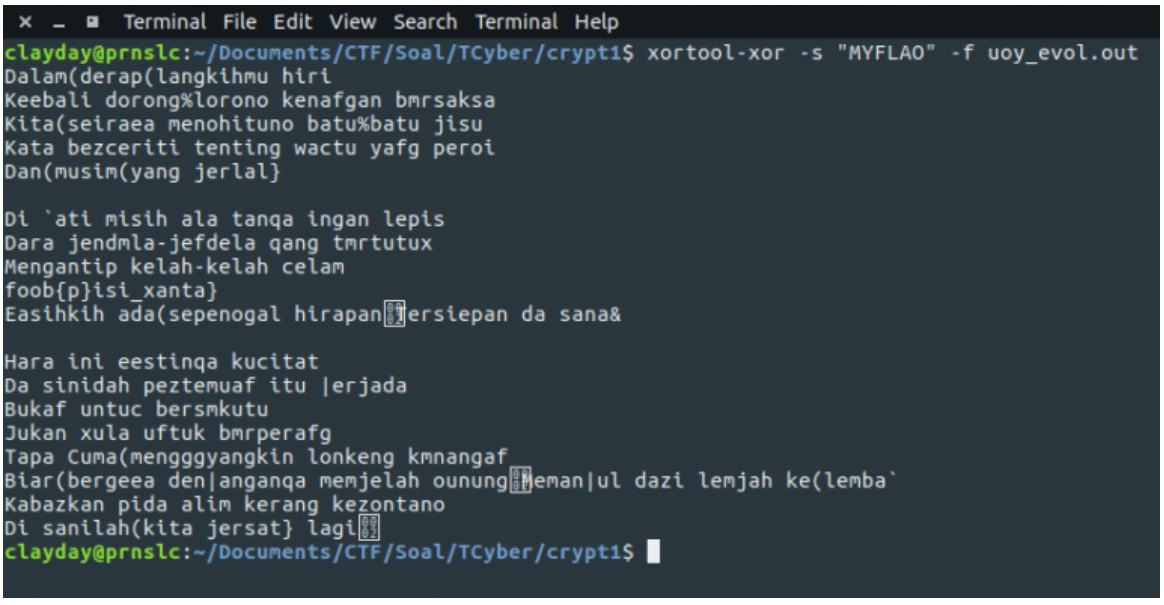


Penjelasan :

```
xortool [namafile] : menebak berapa panjang key yang paling memungkinkan
xortool -l [panjang] : mencari key dengan inputan panjang key
xortool -o : bruteforce dengan printable character yang memungkinkan
```



Kunci yang paling memungkinkan adalah MYFLAO, coba didekripsi dengan key tersebut



Terbaca, namun masih ada yang aneh dengan hasilnya. Coba dengan key MYFLAG

Flag : noob{puisi_xinta}

PREVIOUS POST

QUADRATHLON 2017 WRITEUP – PART 2

NO NEWER POSTS

RETURN TO BLOG

CATEGORIES

CTF

BE FIRST TO COMMENT

Leave a Reply

Your email address will not be published. Required fields are marked *

Enter Your Comment…

Your Name*

Your Email*

Your URL

Post Comment

CLAYDAY BLOG

ARCHIVES

JUNE 2017

MAY 2017

LIFE