Boston Key Party CTF 2014 Crypto 200 Xorxes the Hash

Mon, 03 March 2014 in crypto,
0 Comments

BKPCTF , collision

這題出的有點爛
限制太少導致 flag 可能有很多種
卻要 match md5sum 的才是正解
有點無言 ORZ

Crypto 200，這題是一個 python script
此題敘述如下：

> *Xorxes is a hash collision challenge. The goal is to find a second preimage for the input string "Klaatubaradanikto". Submit it as the flag. UPDATE: It has been pointed out that there are multiple solutions. The flag is the one with md5sum '7179926e4253a0b405090df67f62c543'. (Use `echo -n FLAG | md5sum'.) UPDATE THE SECOND: The solution is short.*

簡單的說我們要找到另一個字串做 Xorxes 後的結果會與 `Klaatubaradanikto` 相同
但是因為結果不只一種
flag的結果做md5後會是 `7179926e4253a0b405090df67f62c543`

題目很好心的把hash的示意圖給我們了：

```
# Xorxes Hash uses message blocks of 8-bits, with a 224-bit chaining variable.
#
#   (m_0)       (m_1)         ... (m_n)  = input message blocks
#     |           |                 |
#   SHA224      SHA224        ... SHA224
#     |           |                 |
#  V-(+)-[>>>56]-(+)-[>>>56]- ... --+--- = chaining variable
#
#  chaining variable + (message length mod 24) = hash output
```

一個block就是一個字元
V指的是 Initail Vector
Xorxes 的流程是：

1. c = IV
2. x = sha224(str[i]) //每次取一個字元做sha224
3. c = RROT(c,56) //將目前的結果做 right rotate 56 bit
4. c = x ^ c
5. result = c + (len(str) % 24) //最後加上字串長度

這題的關鍵是這種 hash 的方式是 **stream cipher**
且不會產生 avalanche effect
此外 sha224 會將字元 hash 成 224 bit 的結果
而 rotate 56bit 剛好是 1/4 的長度
根據這些特性...
我就想出來至少三種可以產生有同樣 hash 結果的方式 = =

1. 找到 -24 內的 hash 加上固定的 4n 個相同字元，以長度調整 hash value
   4 個相同字元 hash 出來的結果會是 0 (忽略IV)
   xor 的特性是 `a^a=0` 雖然這題有做 shift 但是四個相同字元將無視這個限制
   理論上是可行但是要找到符合條件似乎太過嚴苛
   加上 hint "The solution is short" 讓我否定了這個猜想

2. `KlaXtubXradXnikto`
   xor 還有一個特性是滿足交換率
   如果中間有相同的字元，且 index%4 相同
   這兩個字元在 hash 的過程中可以相互抵銷
   `Klaatubaradanikto` 這個字串有三個位置滿足這條件
   我嘗試填入 *[a-zA-Z0-9]*
   C3取 2*62 共 186 種組合 拿去做 md5 check
   結果都不是正確的結果 ORZ

3. 將 `Klaatubaradanikto` 內的字元做交換
   用xor交換率的特性
   index%4 相同的字元可以交換卻不影響 hash 的結果
   但是這可能性就有點多....
   一共約有 `5!\*4!\*4!\*4!=1658880` 種 (字元相同我懶得扣掉了 XD)
   我跑了將近一個小時最後才得到結果 = =
   不知道是不是我還有什麼沒考慮到的?

flag: `radaniktKlaatubao`