Untitled

BY: A GUEST ON SEP 3RD, 2015 | SYNTAX: PYTHON | SIZE: 2.76 KB | VIEWS: 77 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT | QR CODE | CLONE

0

0

TEXT BELOW IS SELECTED. PLEASE PRESS CTRL+C TO COPY TO YOUR CLIPBOARD. (⌘+C ON MAC)

```python
#!/usr/bin/env python2.7

from z3 import *

k = [0] * 16
for i in range(16):
    k[i] = [ 0x11, 0xaa, 0x55, 0x33 ][i//4]

b = [ BitVec('b%d' % i, 32) for i in range(16) ]
v = [ b[i] ^ k[i] for i in range(16) ]
s = Solver()

for i in range(16):
    s.add(b[i] & 0xff == b[i])


#  _   _           _
# | | | | __ _ ___| |__
# | |_| |/ _` / __| '_ \
# |  _  | (_| \__ \ | | |
# |_| |_|\__,_|___/_| |_|
#

S1 = BitVec('s1', 32)
S2 = BitVec('s2', 32)
S3 = BitVec('s3', 32)
S4 = BitVec('s4', 32)

for i in range(16):
    val = v[i]
    s.add(33 <= val <= 122)
    S1 = S1 + val
    S2 = 37 * val + RotateRight(S2, 23)
    S3 = val ^ 8 * S3
    S4 = val + 32 * S4

s.add(S1 == 1720)
s.add(S2 == 0xDCCE74)
s.add(S3 == 0xEBAF1446)
s.add(S4 == 0x9961270E)



#   ____                _ _ _   _
#  / ___|___  _ __   __| (_) |_(_) ___  _ __
# | |   / _ \| '_ \ / _` | | __| |/ _ \| '_ \
# | |__| (_) | | | | (_| | | |_| | (_) | | | |
#  \____\___/|_| |_|\__,_|_|\__|_|\___/|_| |_|
#


# Just copy & paste code from IDA

v12 = b[1] ^ b[0]
v13 = b[2] ^ b[1] ^ b[0]
v14 = b[3] ^ b[2] ^ b[1] ^ b[0]
v15 = b[4] ^ b[3] ^ b[2] ^ b[1] ^ b[0]
```

Public P

Untit
8 sec

Untit
9 sec

Untit
13 se

Untit
22 se

wut
22 se

Untit
26 se

Untit
43 se

Untit
48 se

```
v16 = b[5] ^ b[4] ^ b[3] ^ b[2] ^ b[1] ^ b[0]
v17 = b[6] ^ b[5] ^ b[4] ^ b[3] ^ b[2] ^ b[1] ^ b[0]
v18 = b[7] ^ b[6] ^ b[5] ^ b[4] ^ b[3] ^ b[2] ^ b[1] ^ b[0]
v19 = b[8] ^ b[7] ^ b[6] ^ b[5] ^ b[4] ^ b[3] ^ b[2] ^ b[1] ^ b[0]
v20 = b[9] ^ v19
v21 = b[10] ^ b[9] ^ v19
v22 = b[11] ^ b[10] ^ b[9] ^ v19
v23 = b[12] ^ b[11] ^ b[10] ^ b[9] ^ v19
v24 = b[14] ^ b[13] ^ b[12] ^ b[11] ^ b[10] ^ b[9] ^ v19
v25 = b[13] ^ b[12] ^ b[11] ^ b[10] ^ b[9] ^ v19
v26 = b[15] ^ b[14] ^ b[13] ^ b[12] ^ b[11] ^ b[10] ^ b[9] ^ v19


s.add(0 == 0xff & (b[0] ^ 0x63))
s.add(0 == 0xff & (((v12 << 1) | (v12 >> 1)) ^ 0x2F))
s.add(0 == 0xff & (((v13 << 2) | (v13 >> 2)) ^ 0xDC))
s.add(0 == 0xff & (((v14 << 3) | (v14 >> 3)) ^ 0x20))
s.add(0 == 0xff & (((v15 << 4) | (v15 >> 4)) ^ 0xCD))
s.add(0 == 0xff & (((v16 << 5) | (v16 >> 5)) ^ 0xA0))
s.add(0 == 0xff & (((v17 << 6) | (v17 >> 6)) ^ 0x83))
s.add(0 == 0xff & ((v18 << 7) | (v18 >> 7)))
s.add(0 == 0xff & (v19 ^ 0x30))
s.add(0 == 0xff & (((v20 << 1) | (v20 >> 1)) ^ 0x7D))
s.add(0 == 0xff & (((v21 << 2) | (v21 >> 2)) ^ 0x19))
s.add(0 == 0xff & (((v22 << 3) | (v22 >> 3)) ^ 4))
s.add(0 == 0xff & (((v23 << 4) | (v23 >> 4)) ^ 0xC4))
s.add(0 == 0xff & (((v25 << 5) | (v25 >> 5)) ^ 0x20))
s.add(0 == 0xff & (((v24 << 6) | (v24 >> 6)) ^ 0xC1))
s.add(0 == 0xff & ((v26 << 7) | (v26 >> 7)))


# You need to guess XD
#s.add(v[1] == ord('e'))
#s.add(v[2] == ord('v'))
#s.add(v[6] == ord('i'))

print(s.check())
m = s.model()

res = ""
for i in range(16):
    v = int(str(m[b[i]]))
    c = chr(v ^ k[i])
    print('%d: %d %s' % (i, v, c))
    res += c
print("Key is %s" % res)
```

RAW Paste Data

clone this paste

```
from z3 import *

k = [0] * 16
for i in range(16):
    k[i] = [ 0x11, 0xaa, 0x55, 0x33 ][i//4]

b = [ BitVec('b%d' % i, 32) for i in range(16) ]
v = [ b[i] ^ k[i] for i in range(16) ]
s = Solver()

for i in range(16):
    s.add(b[i] & 0xff == b[i])
```