Boston Key Party 2016: des ofb

Published: Wed 09 March 2016
Updated: Wed 23 March 2016
By *lenerd*
In Writeups.
tags: des crypto ctf

Given was an encryption procedure and the resulting ciphertext.

```
from Crypto.Cipher import DES

f = open('key.txt', 'r')
key_hex = f.readline()[:-1] # discard newline
f.close()
KEY = key_hex.decode("hex")
IV = '13245678'
a = DES.new(KEY, DES.MODE_OFB, IV)

f = open('plaintext', 'r')
plaintext = f.read()
f.close()

ciphertext = a.encrypt(plaintext)
f = open('ciphertext', 'w')
f.write(ciphertext)
f.close()
```

When we looked at the ciphertext, we did notice some strange patterns. It does not look random.

```
00000000: 702b 7bef 9327 53d3 4313 5c5b 4116 4357  p+{..'S.C.\[A.CW
00000010: 0426 3ea1 d67f 1bdd 4513 5b47 1542 5f5d  .&>.....E.[G.B_]
00000020: 0435 2ee8 857f 1ad3 5f09 3863 5d53 4350  .5......_.8c]SCP
00000030: 4136 7baa 8262 009c 7f5c 5058 5044 1751  A6{..b...\PXPD.Q
00000040: 4a64 2fe5 932b 1ed5 5f57 1240 5a16 444d  Jd/..+.._W.@Z.DM
00000050: 4222 3eff fc5f 1bd9 1160 5e5d 5b51 4418  B">.._...`^][QD.
...
00000600: 431b 34f9 862a 0eb6                      C.4..*..
```

DES has some so called weak keys. The usage of them results in the same round key in every round of DES; the encryption and the decryption procedures are identical.

- 0x0101010101010101
- 0xfefefefefefefefe
- 0xe0e0e0e0f1f1f1f1
- 0xf1f1f1f1e0e0e0e0

We tried to decrypt the ciphertext with the first key and english words appeared.

```
00000000: f8a5 4b39 835c ed14 7220 6e6f 7420 746f  ..K9.\..r not to
00000010: 8ca8 0e77 c604 a51a 7420 6973 2074 6865  ...w....t is the
00000020: 8cbb 1e3e 9504 a414 6e3a 0a57 6865 7468  ...>....n:.Wheth
00000030: c9b8 4b7c 9219 be5b 4e6f 626c 6572 2069  ..K|...[Nobler i
00000040: c2ea 1f33 8350 a012 6e64 2074 6f20 7375  ...3.P..nd to su
...
```

Decrypting with 0xe0e0e0e0f1f1f1f1 results in a Shakespeare quote and the flag.

To be, or not to be, that is the question:
Whether 'tis Nobler in the mind to suffer
The Slings and Arrows of outrageous Fortune,
Or to take Arms against a Sea of troubles,
...
The fair Ophelia? Nymph, in thy Orisons
Be all my sins remembered. BKPCTF{so_its_just_a_short_repeating_otp!}