Homework Number: 01
Name: Yi Qiao
ECN Login: qiao22
Due Date: 1/17/2019

## Answer

**msg**: You go back home and everything you wished was different is still the same and everything you wished was the same is different.

-Cormac McCarthy, Cities of the Plain

**key**: binary: 0110100101110110 decimal: 26998

## Code

```
#!/usr/bin/python3

import sys
from BitVector import *
from progress.bar import FillingSquaresBar

BLOCKSIZE = 16
PassPhrase = "Hopes and dreams of a million years"

def decrypt(msg, keyBv, bv_iv):
    msgDecryptedBv = BitVector(size=0)
    previousBlock = bv_iv
    encryptedBv = BitVector(hexstring=msg)

    for i in range(0, len(encryptedBv) // BLOCKSIZE):
        bv = encryptedBv[i*BLOCKSIZE:(i+1)*BLOCKSIZE]
        temp = bv.deep_copy()
        bv ^= previousBlock
        previousBlock = temp
        bv ^= keyBv
        msgDecryptedBv += bv

    decryptedMsg = msgDecryptedBv.get_text_from_bitvector()
    if "Cormac McCarthy" in decryptedMsg:

        with open("msg.txt","w") as fp:
            print("msg : "+decryptedMsg, file=fp)
            print("key : binary: ", keyBv, "decimal:", keyBv.int_val(), file=fp)
```

```
        print("Successfully decrypted!")
        sys.exit()


if __name__ == "__main__":

    if len(sys.argv) != 2:
        print("Usage: python3 cryptBreak.py <encrypted file>")
        sys.exit()

    try:
        with open(sys.argv[1], "r", encoding="utf-8") as fp:
            encryptedMsg = fp.read()
    except FileNotFoundError:
        print("file not found")
        sys.exit()

    bv_iv = BitVector(bitlist = [0]*BLOCKSIZE)
    for i in range(len(PassPhrase) // (BLOCKSIZE // 8)):
        textstr = PassPhrase[i*2:(i+1)*2]
        bv_iv ^= BitVector(textstring = textstr)

    bar = FillingSquaresBar('Processing', max=2**16-1)
    for i in range(2**16):
        decrypt(encryptedMsg, BitVector(intVal=i, size=16), bv_iv)
        bar.next()
    bar.finish()
```