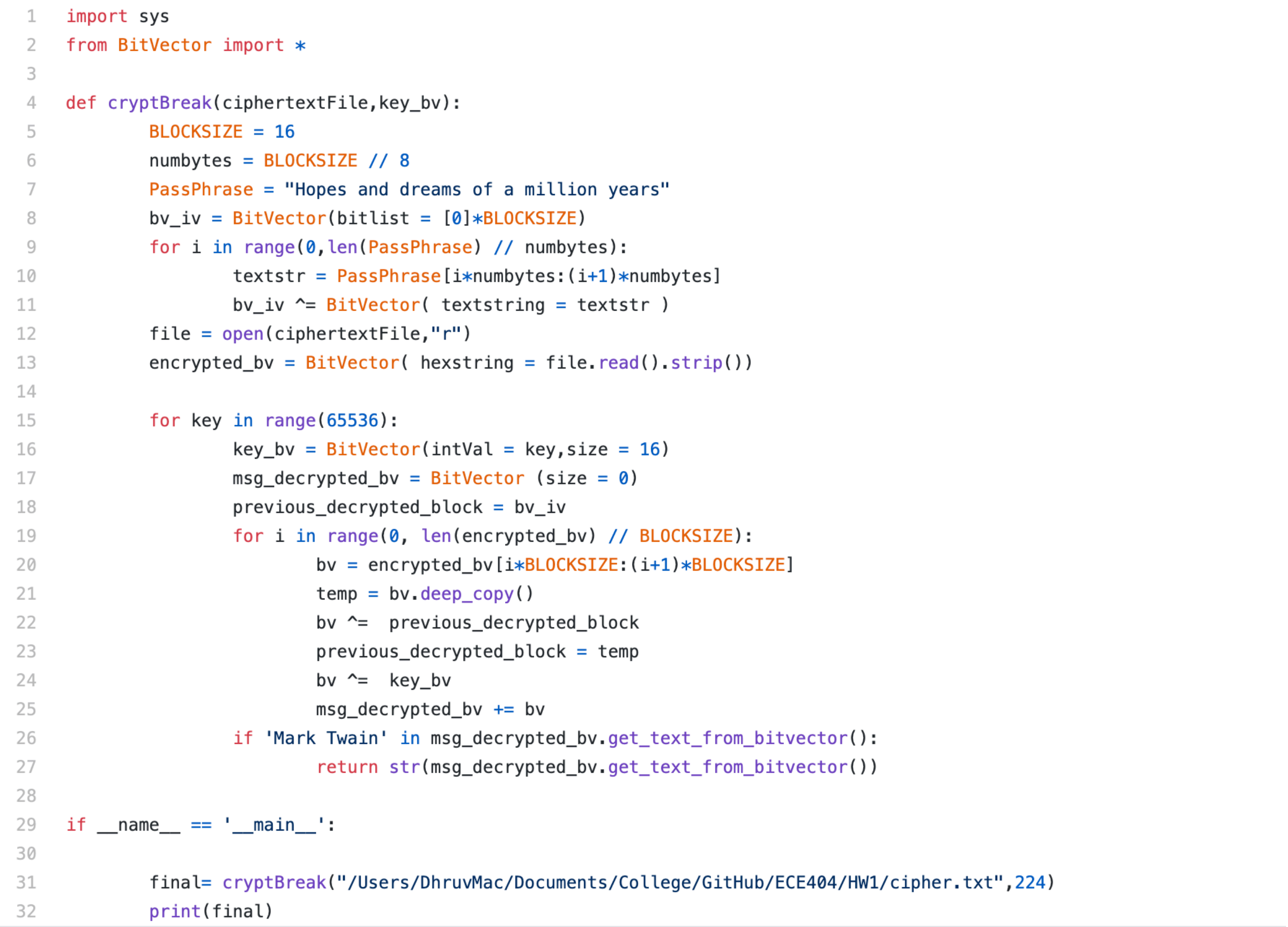
Dhruv Aggarwal HW1



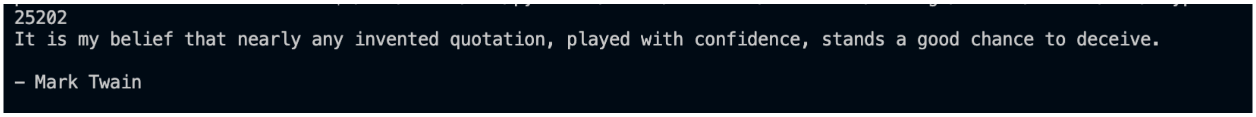
```python
import sys
from BitVector import *

def cryptBreak(ciphertextFile,key_bv):
        BLOCKSIZE = 16
        numbytes = BLOCKSIZE // 8
        PassPhrase = "Hopes and dreams of a million years"
        bv_iv = BitVector(bitlist = [0]*BLOCKSIZE)
        for i in range(0,len(PassPhrase) // numbytes):
                textstr = PassPhrase[i*numbytes:(i+1)*numbytes]
                bv_iv ^= BitVector( textstring = textstr )
        file = open(ciphertextFile,"r")
        encrypted_bv = BitVector( hexstring = file.read().strip())

        for key in range(65536):
                key_bv = BitVector(intVal = key,size = 16)
                msg_decrypted_bv = BitVector (size = 0)
                previous_decrypted_block = bv_iv
                for i in range(0, len(encrypted_bv) // BLOCKSIZE):
                        bv = encrypted_bv[i*BLOCKSIZE:(i+1)*BLOCKSIZE]
                        temp = bv.deep_copy()
                        bv ^=  previous_decrypted_block
                        previous_decrypted_block = temp
                        bv ^=  key_bv
                        msg_decrypted_bv += bv
                if 'Mark Twain' in msg_decrypted_bv.get_text_from_bitvector():
                        return str(msg_decrypted_bv.get_text_from_bitvector())

if __name__ == '__main__':

        final= cryptBreak("/Users/DhruvMac/Documents/College/GitHub/ECE404/HW1/cipher.txt",224)
        print(final)
```



```
25202
It is my belief that nearly any invented quotation, played with confidence, stands a good chance to deceive.

- Mark Twain
```

My code results in the above answers. The way I did this is by reading the lecture slides and also going through the professor's code line by line. I set the block size to 16 and then create a bit vector for the pass phrase as well as for the key. I then use the decryptforfun code to decrypt it and then I check for mark twain after each key is used and once it finds it, it breaks the code. In my main I am simply just calling my cryptBreak function by giving it the cipher text along with a random key_bv which essentially doesn't matter.