Recovered Plaintext Quote

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

- Mark Twain

The Encryption Key

Key : 25202

Code Explanation:

First, set blockset to 16. Then reduce the PassPhrase to the size of BLOCKSIZE.

Open file and load the string into bitvector. Last, carry out differential XORing of bit blocks and decryption.

Code Hard Copy

```
from BitVector import *
import sys
import string

def cryptBreak(ciphertextFile,key_bv):
    PassPhrase = "Hopes and dreams of a million years"
    BLOCKSIZE = 16 #(D)
    numbytes = BLOCKSIZE// 8
    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)
    FILEIN = open(ciphertextFile) #(J)
    encrypted_bv = BitVector( hexstring = FILEIN.read() )
    msg_decrypted_bv = BitVector( size = 0 )
    previous_decrypted_block = bv_iv #(U)
    for i in range(0, len(encrypted_bv) // BLOCKSIZE): #(V)
        bv = encrypted_bv[i*BLOCKSIZE:(i+1)*BLOCKSIZE] #(W)
        temp = bv.deep_copy() #(X)
        bv  ^= previous_decrypted_block #(Y)
        previous_decrypted_block = temp #(Z)
        bv ^= key_bv #(a)
        msg_decrypted_bv += bv
    outputtext = msg_decrypted_bv.get_text_from_bitvector() #(c)
    return outputtext
```