Daniel O. Furry
ECE 40400
Homework 1

The recovered plaintext quote:
Always go to other people's funerals, otherwise they won't go to yours.

- Yogi Berra

The encryption key:
Decimal: 30053
Hex: 7565

Explanation:

My cryptBreak.py function starts with the main function by initializing a test key, preparing to brute force through all potential keys between 0 and 65536 (2^16). A while loop implements Bitvector and calls cryptBreak function to decompose the ciphertext along with the key.

The cryptBreak function imports a file of cipher text and after the block size and passphrase are set it begins by reducing the passphrase to block size. From there it converts the hexstring ciphertext into a bitvector. Finally, it performs differential XORing of bit blocks. The cryptBreak function returns the decryptedMessage back to the main function. The while loop in the main function iterates by one until it provides the cryptBreak function with the correct key, that is that the string ‘Yogi Berra’ is found in the decrypted plaintext.