

Homework Number: 1

Name: Tycho Halpern

ECN Login: thalper

Due Date: 1/20/2022

Plaintext quote:

"Time is an illusion. Lunchtime doubly so.

- Douglas Adams"

Recovered encryption key: 29556

Explanation of code:

I started with the file DecryptForFun.py provided, and looked through it to understand what each portion does. I took lines C-H, and T-c and modified them to fit the assignment. I reduced the Blocksize because we are using 16 bit encryption instead of 64 bi encryption. The function takes a BitVector representing an integer key, and the encrypted text file, then decrypts the file using the given key. A separate main function calls the function once for each possible 16 bit integer, and finishes when the output text includes the string "Douglas Adams". The main decryption portion of the code takes place in lines 38-44, where each character in the encrypted string is XORed with the previous decrypted character as well as the appropriate character (I say character because it is an 8 bit block which can be mapped to an ascii character) of the decryption BitVector.