HW01 ECE 404

Matteo Miglio

January 28, 2021

The recovered plaintext quote is: ”Always go to other people’s funerals, otherwise they won’t go to yours.”
-Yogi Berra

The recovered encryption key is: 30,053

The purpose of the main function is to read in the encrypted.txt file, then using the read text, we obtain the encrypted cipher. It is stated that our BLOCKSIZE is set to 16, therefore we need to brute force analyze all keys from 0-65,535. This roughly took 5 minutes, give or take a few seconds given the use of remote connectivity to ecn.

The purpose of the function cryptBreak() was to decipher the text file with a given encryption key. First the function would take in the passphrase and alter its length to size of BLOCKSIZE in form of a bit array using the BitVector class. Next we would need to create a new (empty) BitVector to hold space for the deciphered string as we will append to it while differential XORing. The first argument in the differential XORing would be the passphrase that is reduced to a BitVector of length BLOCKSIZE previously. Then continuing with the differential XORing we are able to use the previous XOR of size BLOCKSIZE as an input argument to our next block. Finally, as we work our way through the loop, each output of the differential XOR is appended to our empty BitVector. Thus, when the loop is finished, we are able to translate the BitVector into plaintext and return from the function to see if all the appended characters translate into a field of text containing the name ’Yogi Berra.’