∗ The recovered plaintext quote:
Time is an illusion. Lunchtime doubly so.
- Douglas Adams

∗ The recovered encryption key:
29556

∗ A brief explanation of the code:
First set the block size to 16 which leads to 2 bytes in each block (16//8=2), and then derive the initialization vector from the PassPhrase(this is done by transfer the passphrase into a 16-bit array). After open the ciphertext and turn it into bit vector, an empty bit vector is prepared to store the decrypted message. Finally, 16-bit of the ciphertext bit vector is being scanned each time and XORing, the initialization vector and decrypted message bit vector are being updated using the key (the process of differential XORing). Once all the bit in the ciphertext bit vector is scanned, decrypted message bit vector will be transfer into plaintext. Those process are what performed in the cryptBreak function, the brute-force attack is basically tried all the key from 1 to 2^16 for the cryptBreak function in a for loop until the decrypted message contains the string “Douglas Adams” and exits the loop.