Name: Nazran Farook

Purdue email: nfarook@purdue.edu

Homework #1

Decrypted plaintext quote:

Time is an illusion. Lunchtime doubly so.

- Douglas Adams

Recovered Encryption Key:

29556

decryptBreak method description:

Line 20: Set the passphrase, to be used to create initial bitvector

Lines 23-24: Set the required blocksize, and calculate number of bytes required to store bitvector equal to this blocksize

Line 28: initialize initial bitvector

Lines 29-31: break the passphrase into equal sized chunks, create bitvectors using these individual chunks of BLOCKSIZE, and perform bitwise xor on them, to obtain a single bitvector (to be used as initial bitvector in the process of encryption). Effectively, we reduce the passphrase into a single bitvector of size BLOCKSIZE.

Lines 34-35: open the ciphertext file, and convert the contained ciphertext to a bitvector

Line 38: initialize the bitvector for decrypted text

Line 41: initialize a bitvector, to keep track of previous decrypted block

Lines 42-48: break the encrypted bitvector into equal sized chunks of BLOCKSIZE. For i'th such chunk perform xor with previous decrypted block and then key, to obtain i'th part of decrypted bitvector. Hence, append this part to current decrypted vector.

Lines 51-53: Finally, convert the decrypted bitvector to normal string and return the string

The test code (lines 55-74) calls the decryptBreak method for each possible value of key (integer value ranging from 0 to 2^16-1), and checks if the decrypted text contains the expected text.