ECE 404 Homework 1

Recovered plaintext quote: Sir Lewis Carl Davidson Hamilton (born 7 January 1985) is a British racing driver currently competing in Formula One, driving for Mercedes-AMG Petronas Formula One Team. In Formula One, Hamilton has won a joint-record seven World Drivers' Championship titles (tied with Michael Schumacher), and holds the records for the most wins (103), pole positions (103), and podium finishes (191), among many others. Statistically considered as the most successful driver in Formula One history.

Recovered encryption key: 4040

Brief Explanation of code: The function 'cryptBreak' is very similar in functionality to 'DecryptForFun' provided in the lecture slides by Professor Kak. It describes a medium strength decryption algorithm for secure message exchange. My code is essentially based on what is known as differential XORing of bit blocks. Differential XORing can be defined as the process of destroying any repetitive patterns in the message to be encrypted making it more difficult to break encryption by a statistical attack.

The implementation begins with the function definition that takes in two parameters: the ciphertext file which contains the encrypted message and a 16-bit Bit Vector for the decryption key. The code decrypts the ciphertext within the file given using this key and returns the original plaintext as a string.

Primarily the passphrase, and block size (16) were initialized. Then the number of bytes was calculated by floor dividing the block size by 8. The first task would be to reduce the passphrase to a bit array of size block size so we could perform the differential XORing. Therefore, a Bit Vector was initialized of size block size and a for loop runs from 'i' to the length of the passphrase divided by the number of bytes wherein a string variable stores the passphrase in the format of a Bit Vector. The code takes block size iterations at decrypting the ciphertext. This Bit Vector is then XORed with the initialized Bit Vector created in the first step.

Next, a Bit Vector from the ciphertext hex string is created by opening the file and reading each bit and storing it in a variable as a Bit Vector like 'encrypted_bv' for example. Furthermore, a Bit Vector for storing the decrypted plaintext bit array is created.

After initializing the vectors we can now perform the differential XORing in order to decrypt the message. When performing differential XORing, we XOR the Bit Vector (ciphertext block) with the previous block of the ciphertext. Then a for loop runs till the end of the encrypted Bit Vector after which the decrypted message is stored in the Bit Vector variable.

Then we update the previous decrypted block with the current bit block so it can be used on the next iteration. Finally we XOR the Bit Vector with the key and append the now decrypted bit vector to the decrypted message variable.

Credit : The cryptBreak.py file contains code provided in the lecture slides. The link is pasted here: https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture2.pdf