Homework Number: 01
Name: Samitha Ranasinghe
ECN Login: sranasi
Due Date: 01/19/2023

The 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.

The recovered encryption key:

4040

A brief explanation of your code:

The cryptBreak function was written by burrowing the main code from the DecryptForFun.py file provided which contains an example code for decryption. The passphrase is kept the same of "Hopes and dreams of a million years" and the Block size is set to 16 based on the encryption instruction. Bitvector objects are made from the passphrase which is used for as the initial decrypted block and the cyphertext string which is first read from the file. The decryption is then carried out by differential XORing of bit blocks until all the blocks are decrypted and then returned as a extracted plaintext.

The brute force analysis is run under main so that the cryptBreak function can be used independently by importing. The brute force attack is executed using a for loop where the key is iterated from 0 to the maximum number in the key space provided in the hint which is 2^16 – 1 (Since the effective key size is 16 bits). The cryptBreak function is called each time the for loop iterates and then checked whether the returned plaintext contains the words “Sir Lewis” provided by a hint.