Homework Number: 1

Name: Dylan Huynh

ECN Login: huynh38

Due Date: 1/19/2023

Recovered Key: in ASCII: È, in decimal: 4040, in hexadecimal: 0fc8, in binary: 0000111111001000

Recovered: 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.

In this code, given a piece of cipher text to decrypt, I ran through keys from $0 - 2^{16}$ in cryptBreak.py, which initializes a BitVector for the ciphertext and the given key, and then decrypts the text by taking a block of size 16 and using differential XOR between the current block, the previous block, and the key. It will loop through the text until the text has been completely iterated over and returns the decrypted message. I took a good amount of code from DecryptForFun.py from lecture 2, importing BitVector and sys the same way. However, I got rid of parts #(B), #(J), #(L), #(M), #(N), #(O), #(d), #(e), and #(f), as all of these parts of the code pertained to formatting the input and output of the code, which were different in my code. The cryptBreak function returns a string instead of nothing so I added a return statement, and I changed the initialization of the ciphertext bitvector to be initialized without a file read.