Homework Number: 1

Name: Andrew Wu

ECN Login: wu1795

Due Date: 1/18/24

Recovered Plaintext Quote:

Charles Marc Herve Perceval Leclerc born 16 October 1997 is a Monegasque racing driver, currently racing in Formula One for Scuderia Ferrari. He won the GP3 Series championship in 2016 and the FIA Formula 2 Championship in 2017. Leclerc made his Formula One debut in 2018 for Sauber, a team affiliated with Ferrari, for which he was part of the Ferrari Driver Academy.

Recovered Encryption Key:

Binary: 0000011001010000, Decimal: 1616, Hex: 650

In my file cryptBreak.py, I was given an encrypted file to decrypt via a brute force attack. Given the ciphertext, a passphrase, and importing the BitVector class, the code runs through keys from $0 – 2^{16}$ and decrypts the ciphertext by taking a block size of 16 and using differential XORing of the current and previous blocks as well as the key. This will happen until the entire ciphertext has been run through and returns the decrypted message. Most of my code was based off DecryptForFun.py, with some different variable names used, though there were some parts of DecryptForFun.py that was not used since it pertained to writing the decrypted plaintext to a file as well as getting an encryption key from the user. Since the function in cryptBreak.py returns a string, I added a return statement at the bottom to return the decrypted plaintext.