Ethan James
33378430

HW01 PDF

Plain Text Code: 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.

Encryption Key: 11001010000 which is 1616 in decimal.

Code Brief: First and foremost, I need to give credit to Prof. Kak as most of the code was taken and adapted from his lecture slides. My code first takes the passphrase and reduces it to a bit Vector array to prepare it for block cipher encryption. Then it opens and reads the file. It then closes, so that it can create the bit vector from the hex string. Then we create a bit vector for storing the decrypted message. Then we do the differential Xoring of the bit blocks. Finally we extract the plaintext from the decrypted bitVector.