

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 integer value:

1616

Description of Code:

To decrypt this message, I used a lot of the implementation shown in DecryptForFun.py. First, I initiated all the variables for decryption and converted the passphrase variable into a bit array. Next, I created an encrypted bit vector out of the cipher text file given for the assignment. With this encrypted bit vector and a key that was passed through the cryptBreak function, I used differential XORing to decrypt it and store that decryption into a different bit vector. Once decrypted, I returned an ascii version of said bitvector. To test my cryptBreak function I made a test file that went through all the possible keys for the decryption. The correct key was found if the decrypted message contained the string 'Ferrari' and the search would end while writing the correct message and key to an output file.