Encrypted text: 

Decrypted text:

Newly re-signed McLaren driver Lando Norris is confident that the team will be in the mix for race victories in 2024, but the Briton feels he may have to wait a little longer for a championship challenge. McLaren caught the eye last season by going from struggling to score points to regularly fighting for podiums, with highly effective upgrades being implemented following a technical reshuffle. Norris came close to scoring McLaren's first Grand Prix win since 2021 on several occasions, taking six P2 finishes, while team mate Oscar Piastri managed to triumph in the Qatar Sprint Race.

Explanation:

I first wrote the encryption function which first generate the key according to the given function of get\_key\_from\_user and gen\_key\_schedule\_256. Then I open the file and read the plaintext and convert it to bitvector, and then padding the bitvector as needed if it is not exactly 128 bits. Then I proceed with four steps for encryption, which first xor the first word in keywords, and then begin the 14 rounds of byte substitution, shift rows, mixcolumns, and add round key, then update the state array every time at the end of loop. Not doing the mix column at the last round. Then write to the file at the end.

For the decryption function, I basically changed the way of reading the file by slicing the file into bitvector, xor the last four words of the keywords. I then do inverse shift rows, inverse byte substitute, add round keys, and inverse mix columns. I am not doing the inverse mixing column at the last round. Then write to the file of the plaintext by converting bit vector into ascii.