Ethan James
33378430
epjames

HW04

Encryption:

The AES encryption code works like the lecture notes. I first created the empty state array. It is then Xored with the initial 4 words. We then start the actual rounds of encryption which constitute subbing the bytes and the process contained within that. This is given to us. Then we shift the rows by shifting how the lecture notes states. We shift the second row by one byte, third row by two bytes, and the last row by three bytes. We then mix the columns again with how the lecture notes stated. I use the gf modular function to do this. We are given a formula that does this. Finally, we add the round key with the four words corresponding to the round. I do this by xoring the round key when we say add. We continuously do this until every block is encrypted along with its padding if it is required.

Output:

3ba1ab4b7fe412ca26c7a25cff913d1b748da805c97c83554d9e9cf5b12243ff03a8c6b6dcbc520750a14df9
b646fa480d1e64cc2e9174a23dbed6aad77144350ff768093cf7571852a26ffa36fe47652a546acf9d4bc1ad
395a92553b4b7e0a5a7811d7b95d95cacc117e344ac093da247168cd4bbbda5bc2866fd044c8ca18ecd2b
6a78bfe19520f22b7fa12862132e32ee78c5e4200166c40f1a93f9b08c5f67b9bde38d34ed34bd03183a52
9a5a62d81b1cf084832fcb9139a51100a04c7c631d3fbfa5bb9b8cbe970f02213ab07d3e179313142865fb8
b022241552567964250cfa2aa97c59223d30a2a7da8974d0f6c34f4f46ed6cab53e483f95d4ed157bb78ce
078a88397c9d656830fadd080d729ac7428a6ca3c17ad67d0cf16d35a8ecb35cd818a380309332c4cc29d0
0b6fe542b67724295b49804b2122b5b24e6f09e22451bb77c6876d51b7294b405dcff0cdc83754538442fc
c766bfe4fac839e932f757aebbe7f43c87d08249c6ef50d9adefa8eca175785ba0dbc31e2e61ba32a75f5968
94ea736bcea8f351d3c4574539e7ad760c4a0c4b252e2dbc859c4b0a6b44fbf29b3fa7fddeace3855c67513
0ef65d4fa7f8125d4575f329cc93d75d14fdcb1419678cae4d686d4b72f56ac4d7974e3b1f1bbb3776dda5d
b94b7d2ef1f73f96f7b24378a1e299271006cd478bd84fe7a24c67794e663668c918bdb65097099351e1eb
f6e7d1148754f1051d33156e4fb7e96cce8f976f6a0ad71d12b10d1b43458c02002bf1fc14c9c63e9033dfdc
bc9baae76efc8e12a850fdd21ead4e9b14fb359a27fc4943b0d76714

Decryption:

In decryption I do the reverse of encryption. Here what I do is first create the state array which is Xored with the last four words. Then I go and do inverse shift rows, inverse sub bytes, inverse round key, and inverse mix columns. Inverse shift rows we are using various hexadecimal representations to create the matrix given in the notes along with the modulus. Inverse sub bytes is given to us. I just use the inverse sub table instead of the regular subtable. Inverse round key is the same as the encryption round key function. Finally mix columns is similar, but we do not use it on the last round again. I use all the steps listed in the lecture notes that are contained within the functions. However, for sub bytes I don't use inverse gen tables as I still use the normal one for which I do not know why. Again, inverse mix columns is not used on the last iteration of the round. I also convert everything to a hex string to read like that and output as plaintext to the file. I also flatten my state array at the end of both encryption and decryption prior to outputting to the output file.

Ouput(What it should be):

```
      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.
```