Homework 4 Hardcopy

Christopher Chan
chan328

Encrypted Text:

3ba1ab4b7fe412ca26c7a25cff913d1b748da805c97c83554d9e9cf5b12243ff03a8c6b6dc
bc520750a14df9b646fa480d1e64cc2e9174a23dbed6aad77144350ff768093cf7571852a
26ffa36fe47652a546acf9d4bc1ad395a92553b4b7e0a5a7811d7b95d95cacc117e344ac0
93da247168cd4bbbda5bc2866fd044c8ca18ecd2b6a78bfe19520f22b7fa12862132e32e
e78c5e4200166c40f1a93f9b08c5f67b9bde38d34ed34bd03183a529a5a62d81b1cf0848
32fcb9139a51100a04c7c631d3fbfa5bb9b8cbe970f02213ab07d3e179313142865fb8b02
2241552567964250cfa2aa97c59223d30a2a7da8974d0f6c34f4f46ed6cab53e483f95d4e
d157bb78ce078a88397c9d656830fadd080d729ac7428a6ca3c17ad67d0cf16d35a8ecb
35cd818a380309332c4cc29d00b6fe542b67724295b49804b2122b5b24e6f09e22451bb
77c6876d51b7294b405dcff0cdc83754538442fcc766bfe4fac839e932f757aebbe7f43c87
d08249c6ef50d9adefa8eca175785ba0dbc31e2e61ba32a75f596894ea736bcea8f351d3
c4574539e7ad760c4a0c4b252e2dbc859c4b0a6b44fbf29b3fa7fddeace3855c675130ef6
5d4fa7f8125d4575f329cc93d75d14fdcb1419678cae4d686d4b72f56ac4d7974e3b1f1bb
b3776dda5db94b7d2ef1f73f96f7b24378a1e299271006cd478bd84fe7a24c67794e6636
68c918bdb65097099351e1ebf6e7d1148754f1051d33156e4fb7e96cce8f976f6a0ad71d1
2b10d1b43458c02002bf1fc14c9c63e9033dfdcbc9baae76efc8e12a850fdd21ead4e9b14
fb359a27fc4943b0d76714

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.

Code Explanation:

To start, I integrated the starter code for the round key generation and the substitution bytes tables as well as conferred with TAs on a good structure for my solution. Within my encrypt, the steps are as follows.

1. Create the round keys
2. Create the sub bytes tables
3. Make sure that 128 bit blocks are being read in
4. For the first round, XOR the round key in before going into a loop.

5. In the second loop, the block is first changed into the state array before being sent to the subBytes function which finds the appropriate substitution for a specific byte in the block from the generated table earlier.
6. Then the state array is sent to the shiftRows function which circularly shifts to the left the 2nd-4th rows by 1,2 and 3 bytes respectively.
7. The state array is then sent to the mixColumns function which uses GF multiplication between each column and a predefined matrix and is then XORed together.
8. The last step of each round is to convert the state array back into a bitvector and XOR the next round key to it.
9. This repeats until round 14, in which it's a special case where mixColumns is not called.
10. The data is then added to the encrypted file as a hex string.

For my decrypt function, the order for steps per round are different. In addition the round keys are read in reverse order. The steps per round are as follows:

1. InverseShiftRows is the reverse of the shift rows function that circularly shifts to the right the 2nd-4th rows by 1,2 and 3 bytes respectively.
2. InverseSubBytes is the reverse of the sub bytes function where it uses the inverse sub bytes generated table and finds an appropriate replacement per byte in the block
3. The round keys as said earlier are XORed in reverse order.
4. Lastly the inverseMixColumns uses GF multiplication between each column and a predefined matrix for the inverse function which is then XORed together.

Round 14 is again a special case in which the inverseMixColumns is not called. After each block is subject to all 14 rounds, then the block is written directly to the output file.