Chan Ng Cashin
ECE 404
HW 4

Description:

In my AES.py algorithm I first started by creating function genTables() from lecture 8 to generate the substitution tables used in the first step of each encryption and decryption round. Next, I used the functions in Lecture 8 to generate a key_words list using the subBytes table generated before. This list would be used later for the key expansion step when generating round keys. The subBytes function was then created which substituted each byte in the state array with the byte created in the substitution table. The subBytes function also handled the decryption invSubBytes step using the inverse substitution table also generated in genTables(). Next, the shiftRows function was created which I hardcoded to shift each row for encryption and decryption. The mixCols function was then made which utilized the mixColsTable and invMixColsTable to mix up the columns of the state array. After this I wrote a key expansion algorithm that took the keywords list and generated round keys from it. To implement the last step of the encryption round I needed to XOR a roundkey for any given round with the state array. I did this by creating a function that converted the state array to a bit vector as well as one that did the opposite so the operation would succeed. Finally I created my encrypt and decrypt function by calling all of the functions in the correct order depending on whether it was encryption and decryption.

encrypted.txt:

4a7d5603596bcf81c9e67e806ac442d15e9a8239dcbc57d2ee253263e12b6bfdceb6ec4372ad8fc8d2a953
aaaa03db9ac0246236cb93a7c1e4a4aa175748aa59783f8d671c16f4d688cf41cae5710d9a915119ba3af6e
7ab9a93b74ce5c2596885f26cdf5eb873cc05365b298c07d33bbaa06389a5d3e01c614eaf91a1510f21e18
95db9b6981c3b9e3b0e53c9f4e0c7a3b1cbb1c263eba1cd6ed3ce8a0fc605730062bf9c5bd556123ef33a2
8126fb9bf5f65e3d1b528f0fab690e306bc5b043868076c426b013fa86d9501c96eae26638f9933abbf6347
1aaccd611f6f3e60122034b72c82f15533f7e45998650d062faa1116b92ce9644a8e521d1facd846a0595ba
5f59859cc30a3145931e5eb9424d9b6b4af2b2e01c0618a670df7ad96fb47cd605da85bca866204014a88d
5720af509aa5f67663123410afa406917d1c50a1469587a8efcc5827a1d0953a8b0f20adf03e3bf4aed83fc0
5a54dd0699625e2342eadf199ca8d8bbdf14f46891c12813c338f4e4ecfe1247e39ce10ea19e3ea8de42c92
c3a7844351491065ee0dc7402756047f31bb2cdf8bdaff573a1da8bde0ed3f3ed9f90ddcec50b60e49ad405
9f34a57785ca7a1600a2caf55ed1ef9814392da5b99c27a114e6ad1a90f3a3d549b4cdcdd91bce7fab0063f
32230ec7e872d99ddfe291b93cd19edacb8cb1f9daf90e21f5d36037e4b1e782df69a6af2753ed92ec3f3a2
bc6a9d7eb116531e6576d1a45b8ff33247db4fd95eea3350527936be1b3bf4ce05344547906955002fdbe
b260c3a79dc177256268744dd4e127c4d56bf007e638ce5a7115a704d

decrypted.txt

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.