Anish Laddha
ECE404, Professor Avinash Kak
13 February 2024

HW 04: AES Encryption

Encrypted:
3ba1ab4b7fe412ca26c7a25cff913d1b748da805c97c83554d9e9cf5b12243ff03a8c6b6dcbc52075
0a14df9b646fa480d1e64cc2e9174a23dbed6aad77144350ff768093cf7571852a26ffa36fe47652a5
46acf9d4bc1ad395a92553b4b7e0a5a7811d7b95d95cacc117e344ac093da247168cd4bbbda5bc28
66fd044c8ca18ecd2b6a78bfe19520f22b7fa12862132e32ee78c5e4200166c40f1a93f9b08c5f67b9
bde38d34ed34bd03183a529a5a62d81b1cf084832fcb9139a51100a04c7c631d3fbfa5bb9b8cbe97
0f02213ab07d3e179313142865fb8b022241552567964250cfa2aa97c59223d30a2a7da8974d0f6c
34f4f46ed6cab53e483f95d4ed157bb78ce078a88397c9d656830fadd080d729ac7428a6ca3c17ad6
7d0cf16d35a8ecb35cd818a380309332c4cc29d00b6fe542b67724295b49804b2122b5b24e6f09e2
2451bb77c6876d51b7294b405dcff0cdc83754538442fcc766bfe4fac839e932f757aebbe7f43c87d
08249c6ef50d9adefa8eca175785ba0dbc31e2e61ba32a75f596894ea736bcea8f351d3c4574539e7
ad760c4a0c4b252e2dbc859c4b0a6b44fbf29b3fa7fddeace3855c675130ef65d4fa7f8125d4575f32
9cc93d75d14fdcb1419678cae4d686d4b72f56ac4d7974e3b1f1bbb3776dda5db94b7d2ef1f73f96f
7b24378a1e299271006cd478bd84fe7a24c67794e663668c918bdb65097099351e1ebf6e7d11487
54f1051d33156e4fb7e96cce8f976f6a0ad71d12b10d1b43458c02002bf1fc14c9c63e9033dfdcbc9
baae76efc8e12a850fdd21ead4e9b14fb359a27fc4943b0d76714

Decrypted:
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 on next page:

Explanation:
My code is structured so that on the creation of the cipher object (of class AES) we generate the keys using the AES key schedule method and the provided 256 bit key, to create 60 “words”. These words are joined together in sets of 4 to form 128 bit round keys to be used for encryption at each round. Additionally, I generate the tables for the substitution byte step as well as the inverse.

AES is a block cipher, so after loading the plaintext bitvector, I pad it to make sure we have 128-bit blocks, then i iterate through each 128 bit chunk. First I xor it with the first 4 round keys, then it goes through 14 rounds of processing (each using 4 words). In each round, I first substitute the bytes, then shift the rows, then mix the columns (except for the final round), and finally I xor the round keys. Then I take this encrypted block, append it to me ciphertext bitvector, and when done i dump it into the specified file.

Decryption works similarly, except in reverse. You load in the ciphered bitvector, then iterate through 128 bit chunks. Using the keys at the end first, you run through 14 rounds again. This time, the order is to shift rows, substitute the bytes, xor with the corresponding round keys, and finally mix cols (except for the last round). Finally, you append this block to the deciphered plaintext BitVector, and dump it into a file.