ECE 40400: Introduction to Computer Security

Spring 2024

Prateek Yashwant Jannu

Purdue University, West Lafayette

Professor: Dr. Avinash C Kak

Encrypted Hex String:

```
3ba1ab4b7fe412ca26c7a25cff913d1b748da805c97c83554d9e9cf5b12243ff03a8c6b6dcbc52
0750a14df9b646fa480d1e64cc2e9174a23dbed6aad77144350ff768093cf7571852a26ffa36fe
47652a546acf9d4bc1ad395a92553b4b7e0a5a7811d7b95d95cacc117e344ac093da247168c
d4bbbda5bc2866fd044c8ca18ecd2b6a78bfe19520f22b7fa12862132e32ee78c5e4200166c4
0f1a93f9b08c5f67b9bde38d34ed34bd03183a529a5a62d81b1cf084832fcb9139a51100a04c
7c631d3fbfa5bb9b8cbe970f02213ab07d3e179313142865fb8b022241552567964250cfa2aa
97c59223d30a2a7da8974d0f6c34f4f46ed6cab53e483f95d4ed157bb78ce078a88397c9d656
830fadd080d729ac7428a6ca3c17ad67d0cf16d35a8ecb35cd818a380309332c4cc29d00b6fe
542b67724295b49804b2122b5b24e6f09e22451bb77c6876d51b7294b405dcff0cdc8375453
8442fcc766bfe4fac839e932f757aebbe7f43c87d08249c6ef50d9adefa8eca175785ba0dbc31e
2e61ba32a75f596894ea736bcea8f351d3c4574539e7ad760c4a0c4b252e2dbc859c4b0a6b44
fbf29b3fa7fddeace3855c675130ef65d4fa7f8125d4575f329cc93d75d14fdcb1419678cae4d6
86d4b72f56ac4d7974e3b1f1bbb3776dda5db94b7d2ef1f73f96f7b24378a1e299271006cd47
8bd84fe7a24c67794e663668c918bdb65097099351e1ebf6e7d1148754f1051d33156e4fb7e9
6cce8f976f6a0ad71d12b10d1b43458c02002bf1fc14c9c63e9033dfdcbc9baae76efc8e12a850
fdd21ead4e9b14fb359a27fc4943b0d76714
```

Decrypted Hex String:

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:

Encryption Process:

1. SubBytes (Substitution) Step:
   - Code Step: step_one function performs byte substitution on the input block.
   - Explanation: Substitutes each byte of the block with a corresponding value from the S-Box (subBytesTable).

2. ShiftRows (Permutation) Step:
   - Code Step: step_four_four function shifts rows of the state array.
   - Explanation: Rearranges the bytes in each row of the block according to the row number accordingly.

3. MixColumns (Permutation) Step:
   - Code Step: step_five function mixes the columns of the state array.
   - Explanation: Transforms each column of the block using a fixed matrix multiplication.

4. AddRoundKey (XOR) Step:

- Code Step: step_two_two function XORs the state array with the round key.
- Explanation: Combines each byte of the block with a corresponding byte from the round key using bitwise XOR operation.

5. Key Schedule:
   - Code Logic: The constructor generates round keys (key_words) from the original key using various operations including byte substitution, permutation, and XOR with round constants.
   - Explanation: Expands the original key into a set of round keys for each round of encryption.

Last round does not include mix columns!

Decryption Process:

1. InverseShiftRows (Permutation) Step:
   - Code Step: inv_step_four_four function undoes the row shifts.
   - Explanation: Reverts the rearrangement of bytes in each row performed during encryption.

2. InverseSubBytes (Substitution) Step:
   - Code Step: inv_step_three_three function performs byte substitution in reverse.
   - Explanation: Reverts the byte substitution performed during encryption using the inverse S-Box (invSubBytesTable).

3. InverseMixColumns (Permutation) Step:
   - Code Step: inv_step_five function undoes the column mixing.
   - Explanation: Reverts the column transformation performed during encryption by multiplying each column with the inverse of the mixing matrix.

4. AddRoundKey (XOR) Step (Final):
   - Code Step: step_two_two function XORs the state array with the final round key.
   - Explanation: Applies the final XOR operation with the round key to obtain the plaintext.

Substitution Boxes:

- Code Logic: The gen_subbytes_table function generates substitution boxes (subBytesTable and invSubBytesTable) used for byte substitution during encryption and decryption.
- Explanation: Provides fixed mappings of input bytes to output bytes, which are used in the SubBytes and InverseSubBytes steps.

Last round does not include mix columns!
Reversed round keys!