Assignment No.2

Submission Deadline: 11:59 PM Wednesday 23th October on Google Class Room

Total Marks: 100

NOTE: you can implement it any programming tool but code should be 100% original and this is an individual assignment

Implementation of AES

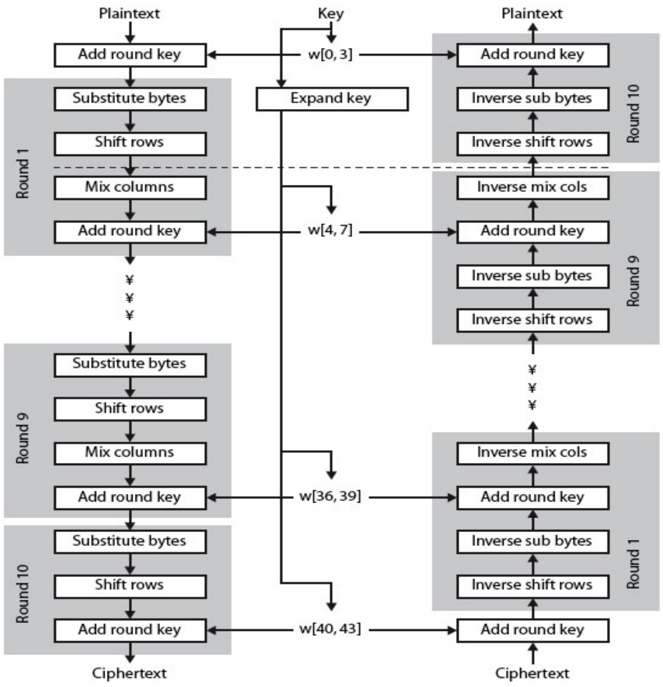
Your assignment is to implement AES-128, meaning the AES algorithm with 128-bit keys.

Several former students described this exercise as the "most useful programming assignment" they had in their undergraduate careers, and one they mention in resumes and interviews with prospective employers. I hope that you find it useful as well.

The Advanced Encryption Standard (AES) is a very important commercial block cipher algorithm, designed to replace the earlier DES.

AES uses repeat cycles or ``rounds." There are 10, 12, or 14 rounds for keys of 128, 192, and 256 bits, respectively. The input text is represented as a 4 x 4 array of bytes. The key is represented as a 4 x 4 array of bytes, where n depends on the key size.

For AES 128 following flowchart is used for encryption and decryption.



(a) Encryption

(b) Decryption

Each round of the algorithm consists of four steps:

1. **subBytes:** for each byte in the array, use its value as an index into a fixed 256-element lookup table, and replace its value in the state by the byte value stored at that location in the table. You can find the table and the inverse table on the web.
2. **shiftRows:** Let Ri denote the ith row in state. Shift R0 in the state left 0 bytes (i.e., no change); shift R1 left 1 byte; shift R2 left 2 bytes; shift R3 left 3 bytes. These are circular shifts. They do not affect the individual byte values themselves.
3. **mixColumns:** for each column of the state, replace the column by its value multiplied by a fixed 4 x 4 matrix of integers (in a particular Galois Field). This is the most complex step. Find details at any of several websites. Note that the inverse operation multiplies by a different matrix.
4. **addRoundkey:** XOR the state with a 128-bit round key derived from the original key K by a recursive process.

For encryption, the final round is slightly different from the others and there is an additional addRoundKey. For decryption, the initial round is slightly different and there is an additional addRoundKey.

There is a tremendous amount of information on the web about the AES algorithm. You can find it by searching for "Rijndael" or "Advanced Encryption Standard" on the web. The AES standard is here:

AES standard (https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf) .

Any questions about the algorithm can be resolved by looking there. There is also a book, The Design of Rijndael by Joan Daemen and Vincent Rijmen that describes the algorithm in detail.

Another student found the following two sites helpful: A HREF="http://www.samiam.org/key-schedule.html">info on Key Schedule and info on mixColumns (http://www.samiam.org/mix-column.html).

Implement AES and perform encryption and decryption using it. Your Task is to implement AES by using appropriate functions and data sets (and structures) by using any programming language. Your work should be original.

Requirements:

1. Calculate keys for AES [keys for all 10-rounds]. And show all of them.
2. Perform Encryption (by using appropriate data)
3. Perform Decryption
4. All types of checks/conditions must be applied on keys, Plain-Text and Cipher-Text.
5. Do not use any built in Library for AES.

Important:

- For any help or confusion you people can email at jawad.hassan@nu.edu.pk.
- This is an individual Assignment. Main Aim of this assignment is understanding of AES and improving your programming skill. So do not plagiarize. You are free to visit my office if you have any problem.
- I am very happy on giving bonus marks on good GUI and efficient implementation skills.

Best of Luck ☺