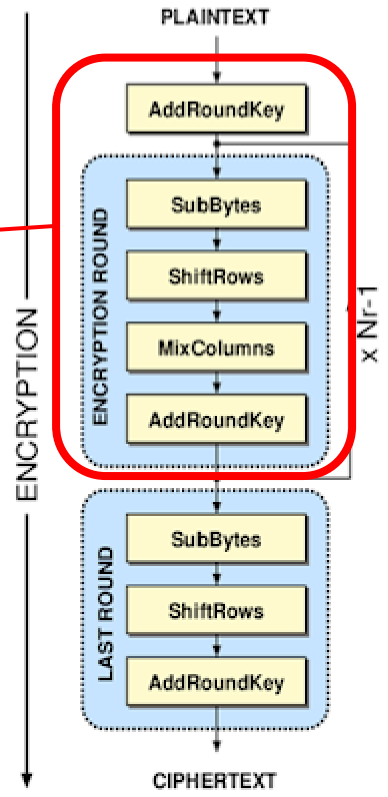
Project #1 (15%) : **ITC 370 (Introduction to Cryptography and Data Security)**

Course:	Introduction to Cryptography and Data Security
Term:	Fall 2023
Instructor:	Dr. Abdalrahman Alfagi
For Inquiries:	You can chat or email me using asaalfagi@auaf.edu.af
Group Assignment:	Group Project (each group made of 3 or 4 students)
Submission Type:	Online document submission & Presentation
File upload:	File upload is required
Restrict Upload File Types:	PDF, DOCX for documentation Part Video for Presentation (Max length 5-7 minutes)
Due date:	

Details

You have studied the AES. The overall structure of AES encryption process shown in figure. The number of rounds is 10, for the case when the encryption key is 128 bit long.

Create a software and explain in details each step to perform the following AES steps: (just for single round)



1- Add round key
2- Substitute bytes
3- Shift rows
4- Mix columns
5- Add round key

The plaintext is: **This is first project**
The key is: **AES is used for Encr**
Ignore the space for both

Please note that:

In the **documentation** part you have to:

1- Provide full explanation for each step.
2- The flowchart of the code is required
3- Use your own words and you are required to define, explain, show figures, tables or examples when it is needed for each step
4- You are required to show the part of the code (***e.g. screenshot***) for each step

In the **presentation** part you have to:

1- Explain How AES work
2- Explain how you create the software.
3- You may ask individually to show how any steps are performed.
4- Each member in the group have to play a part in presentation