I-CHIP

PROBLEM STATEMENT

ROUND 2

Task:

Congratulations and welcome to second round. You have proved your eligibility for this task.

Design Encryption and Decryption scheme for following modes of operation on Advanced Encryption Standard (AES-128):

1) Electronic Code Book Mode
2) Cipher Block Chaining Mode
3) Cipher Feedback Mode
4) Output Feedback Mode

Constraints:

Input is in form of 1024*1024 gray scale image with each image pixel value between 0 and 255 Both Encryption and Decryption scheme should be synchronous with base clock of frequency 100 MHz Output should be encrypted image and then

obtained decrypted image

Judging Criteria:

1) Correctness of the encrypted and decrypted images.
2) Time taken to Encrypt and Decrypt the image for each mode i.e. the total simulation time.

Resources:

https://drive.google.com/drive/folders/1L3WVKOIy8eTBOBCHQe7JkbWz5CCpYBPy?usp=sharing

Submission:

Final date for submissions: **17th April 2021**.

Submit **text files** of design module and testbench module of all codes.

Submit an Image (screenshot) of the timing diagram, obtained after executing the behavioural simulation as well as encrypted and decrypted images for each mode.

Also, submit a text file explaining how much time is used for each encryption and decryption for all modes and a brief description about the function of all the files submitted.

All the above mentioned files must be mailed to ichipudyam@gmail.com along with team name and details of the team members.

Contacts:

Anant Kumar Sharma: 73898 40022

Kunal Agarwal: 90573 71637