Cryptography Algorithms and Verilog Implementation
130330
Implementing and Testing a Whole Algorithm (Assignment 7)
Date: Sunday, May 21, 2023

Submission:	**Team Work**
Deadline:	**In coordination between the lecturer and the team – in class (See instructions below)**
According to JCT's policy, if you violate any submission or deadline criteria you disqualify your assignment	

A. About this Exercise

This is a whole class exercise, on implementing the **DES encryption algorithm**, as specified in FIPS-46-3. Implementing an algorithm by the whole team is a project, similar the how things are going in "real life". It is important to note that DES encryption is taken as an example and as an exercise… We could take any other algorithm as well!

Each person in class must take part in this assignment and must explicitly write his name at the top of the report and in the report (writing what his role was).

In addition, the results will be presented in class by the team.

אופן הגשת התרגיל	מצגת והדגמה במפגש על ידי הסטודנטים, בהובלת נציגי הקבוצה המצגת והדו"ח יכללו טבלה הכוללת את תפקידי כל אחד מהסטודנטים בתכנון (סטודנט שאינו משתתף לא יכול לקבל ציון על המטלה) משקל מטלה זו – 50% מסך ציון המטלות לאחר ההצגה בכתה – משלוח מייל למרצה ובו קישור **דרופבוקס** לתיקיה הכוללת את כל הקבצים והמסמכים (ללא הקבצים לא ניתן לקבוע ציון!)	
ציון על המטלה	**הישג**	**הציון לכל אחד**
	אם לא מוגש כלום	0
	אם הוצגה רק מצגת	עד 70
	כנ"ל – וסימולציה עובדת ומפיקה תוצאות נכונות	עד 80
	כנ"ל – והוצגו תוצאות סינטזה ו- Place & Route	עד 90
	כנ"ל – וסימולציית Post Place & Route עובדת ונותנת תוצאות	עד 100
נוכחות חובה	בעת הצגת המטלה הקבוצתית	

1. על המצגת לשקף עבודה של ממש בתכנון, בניית קוד, סימולציה, סינטזה ותוצאות.
2. ראה בהמשך מסמך זה מה חייב להיות כלול במצגת.
3. גם אם סימולציה איננה מפיקה תוצאות נכונות, עדיין יש לכלול תוצאות סינטזה ו-Place & Route. במקרה זה הציון שיינתן על ביצוע הסינטזה וה-Place & Route עלול שלא להיות מלא, אך יינתן לפי איכות הקוד ואיכות הביצוע של המשימה.

B. The DES Encription Algorithm

The DES encryption algorithm, is illustrated in the block diagram below:

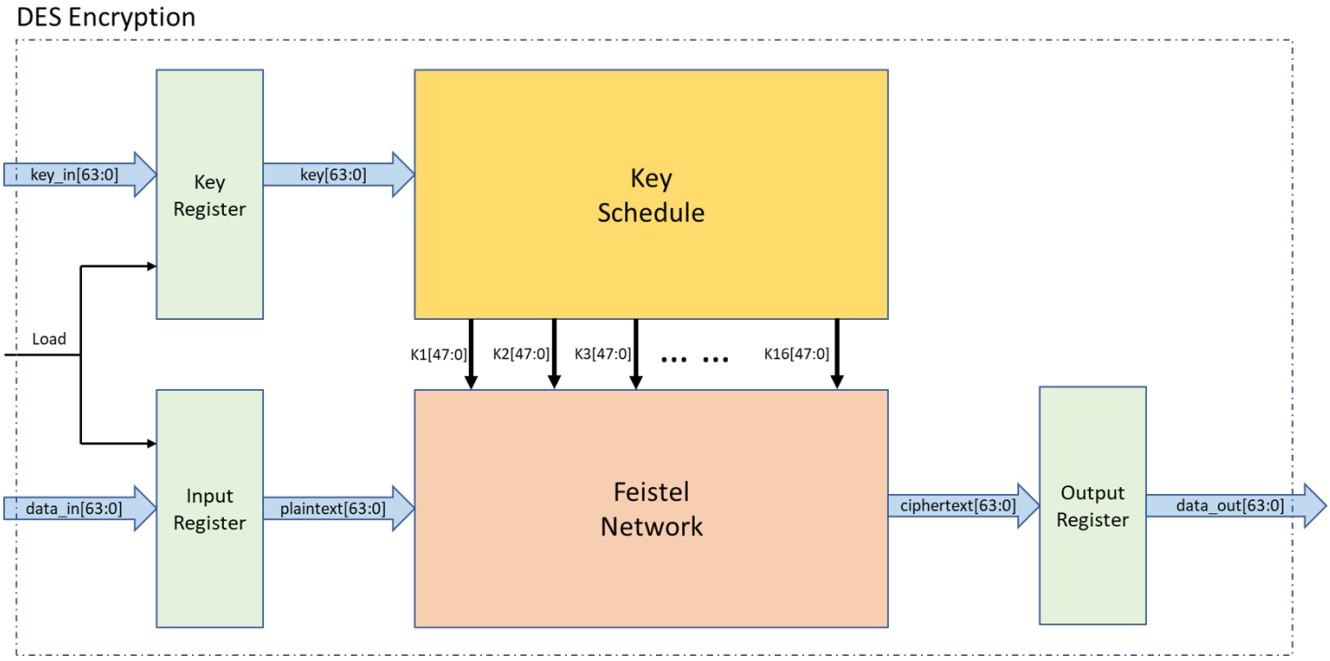

Figure 1: DES Encryption, Block Diagram

DES Feistel network is specified in FIPS-46-3 as follows:

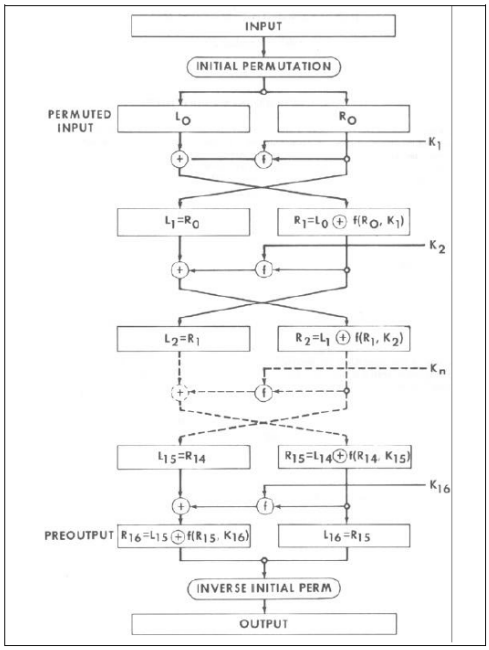

Figure 2: DES Feistel Network

DES key schedule is specified in FIPS-46-3 as follows:

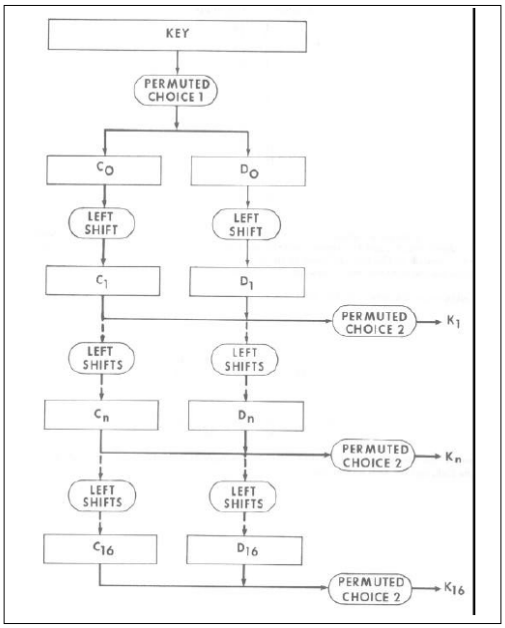

Figure 3: DES Key Schedule

C. The Mission

So, it is a task of the team to design the DES encryption algorithm. Each couple will design a different portion of algorithm or testbench, and when we put it altogether it is going to be a product of the whole team!

The development steps are as follows:

1. Coding (design and and testbench)
2. Simulation
3. Synthesis
4. Place & route
5. Post place & route simulation

To simplify the project, the design shall be implemented in a "loop unrolling" architecture. For synthesis and place & route you may take whatever Artix-7 device to implement (and if it doesn't go well, take a Kintex-7 device), and determine whatever suitable target frequency (1 MHz? 10MHz?)

Each couple (or individuals) will be the owners of a design or verification task, based on the block diagram. Here is a table (if something is forgotten, someone will have to deal with it… if someone finishes and his friends are having problems, then he must help his friends… after all, it's a teamwork):

Identification	Type of work	Task	Owner
0	Result	DES Encryption Algorithm	***Everyone***
0.1	Design and coding	Top level testbench preparation	
0.2	Design and coding	Top level structural design	
1	Design and coding	Top level Feistel network design	
1.1	Design and coding	F function top level structural design	
1.1.1	Design and coding	E function design	
1.1.2	Design and coding	S-boxes (S1, S2, S3… S8) design	
1.1.3	Design and coding	P function design	

Take a decision who will be the owner

Identification	Type of work	Task	Owner
2	Design and coding	Key schedule module, top level structural design	
2.1	Design and coding	PC1 function design	
2.2	Design and coding	PC2 function design	
2.3	Design and coding	Key schedule's left shifts	
3	Design and coding	Input and Output Registers	
...	...	**Any other tasks not listed above...**	...

But there are more tasks and obviously, more tasks than people, so some people will have to do more than one task…

The following tasks shall be owned by the whole team, and lead by the owners of the top level testbench and top level structural design's (it is possible that another person of the team will be delegated to actually do this task):

1. Source simulation
2. Synthesis
3. Place & route
4. Post Place & route simulation

The moto is that ***each one of us is doing a small portion, but together we do the whole task***

כָּל אֶחָד הוּא אוֹר קָטָן
וְכֻלָּנוּ – אוֹר אֵיתָן

D. The Lab Report Must Include

Remember, this is a whole class task. In order to register the submission correctly, each one should submit the (same) ZIP file containing the lab report document and the relevant files.

1. Owners table, specifying explicitly who was the owner of each task (if any task is missing from the original table, fill it in!)
2. The Verilog code for the design and testbench
3. Source level simulation results
   (a) Print of a sample of the regression (an output of the "$display"/"$monitor" of the testbench)
   (b) Sample waveforms
4. Gate level simulation results
   (a) Print of a sample of the regression (an output of the "$display"/"$monitor" of the testbench)
   (b) Sample waveforms
5. Synthesis: Area and timing report
6. Place & route: Area and timing report, I/O report, Screenshot of the chip view
7. Results
   (a) What was the final chip and it's utilization?
   (b) What was the final frequency reported by Vivado?
   (c) What is the possible throughput?

The above 7 points shall be presented in class, in a PowerPoint presentation, by the whole team