Created By: Arda Çekiç 2646149

In this page, the summary of the Homework is written. The all source codes, including c language and HDL language given. PRESENT block cipher is implemented using both c language and HDL language CHISEL. CHISEL source code added, also generated verilog code is added. If you want to generate the verilog code, you need to install “sbt” and scala with proper chisel3 libraries.

Verilog code is tested with veripool’s verilator test bench, test bench is written in c++ language. The output waveform also added as waveform.vcd. You can open this waveform using gtkwave application.

You can also check the README.MD file for proper output and how to run implemented c code.Executable is NOT added for security purposes. You can use “run.sh” bash script to generate executable.

1) The c output of the first question:

```
Calculating Question One
------------------------
Given Key : 00 00 00 00 00 00 00 00 00 00
Given Plaintext : 0
Resulting Ciphertext : 5579c1387b228445
------------
```

2) The second question is:

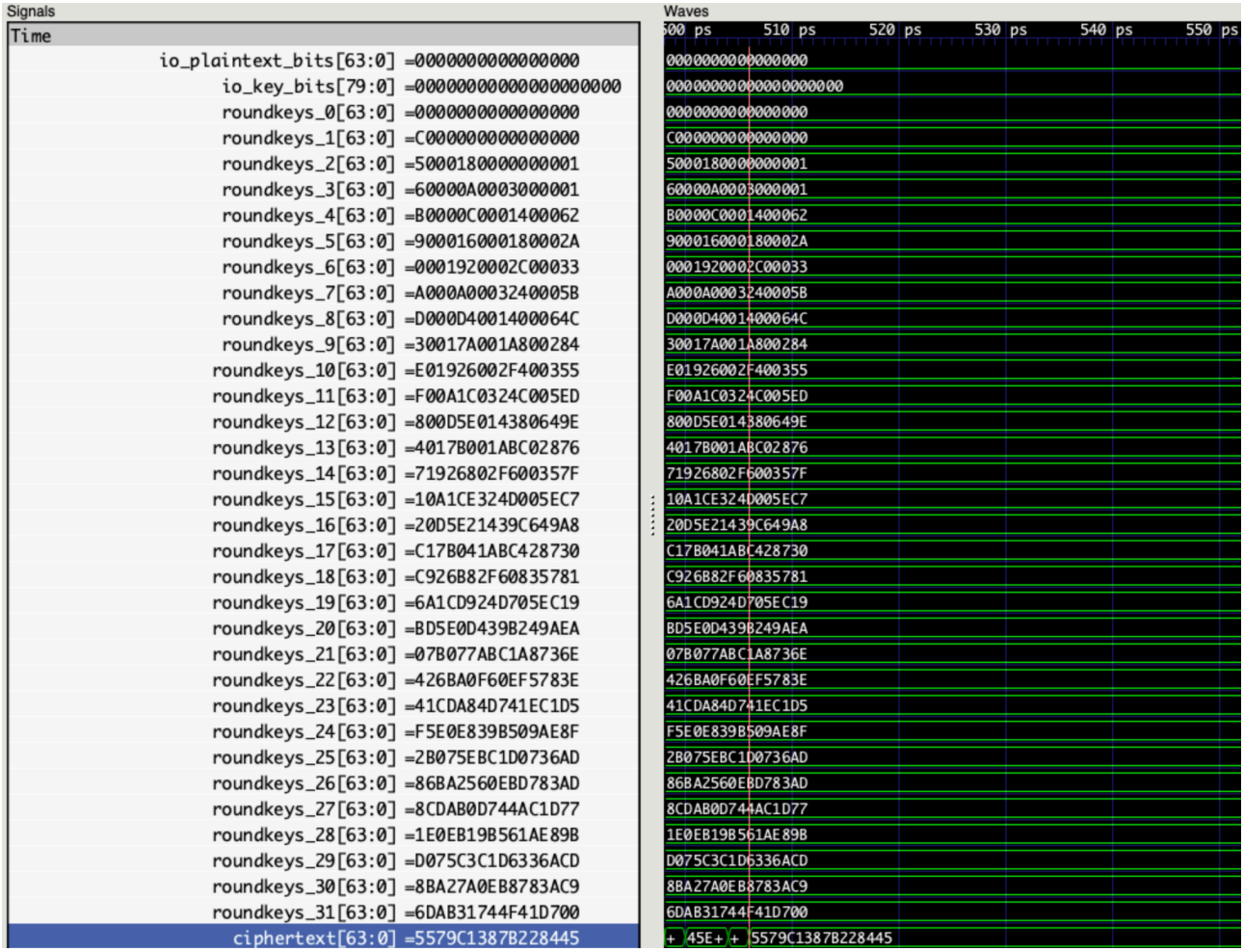
```
Calculating Question Two
------------------------
Given HEX string with Proper Padding 10*
array[0] = 0x417264612043656b
array[1] = 0x6963800000000000
CBC Resulting Ciphertext
ciphertext 0 : 140ba5595b61e12e
ciphertext 1 : f78427afcb351681
------------------------
```

3) The third question is:

```
On MacBook Pro (13-inch, 2022) Apple M2 @ 3.5 GHz (8 cores)
it takes nearly 5 minutes to do encryption of 64MB of data .
(4min43sec)
```

```
The current start time is: Sun Jan 14 01:11:23 +03 2024
Calculating Question Three
------------------------
CBC 64MB Encrypton is started Padding is not issued...
CBC 64MB is done...
------------------------
The current finish time is: Sun Jan 14 01:16:08 +03 2024
```

The waveform of the block cipher:



From the waveform we can see the generated round keys and cipher text.
This verilog implementation MAY NOT be embed to FPGA. Because 19 bit cyclic Right shift operation is not divided and registered. So, 1 or 2 more cycles will take to generate correct results also in FPGA. It is an easy implementation.

Key generation takes : ~250 / 2 cycles

Ciphertext generation takes: 300 / 2 cycles for ready to cipher text

CBC mode is not implemented in CHISEL.