

# System Design with FPGA

Project Report - MT2019528, MT2019016

## Title of Project:

Send the data through UART, encrypt data in the FPGA using any encryption algorithm, and send encrypted data back.

## Brief Explanation:

We have implemented RSA encryption algorithm which encrypts one byte of data (right now input type is numbers) and sends back the encrypted data. The receiver will decrypt the data to see the message sent.

## RSA Algorithm:

- It is asymmetric cryptographic algorithm. It works on 2 different keys, public key and private key.
- Suppose x wants to send information to y so x should know the public key of y to encrypt the message and y will have his own private key to decrypt the message.
- So for that, y will send the public key (n,e) to x. But, private key d is never shared.

○ Message	---	m
○ Encrypted data	---	c
○ Decrypted data	---	m'
○ Public key	---	(n,e)
○ Private key	---	d

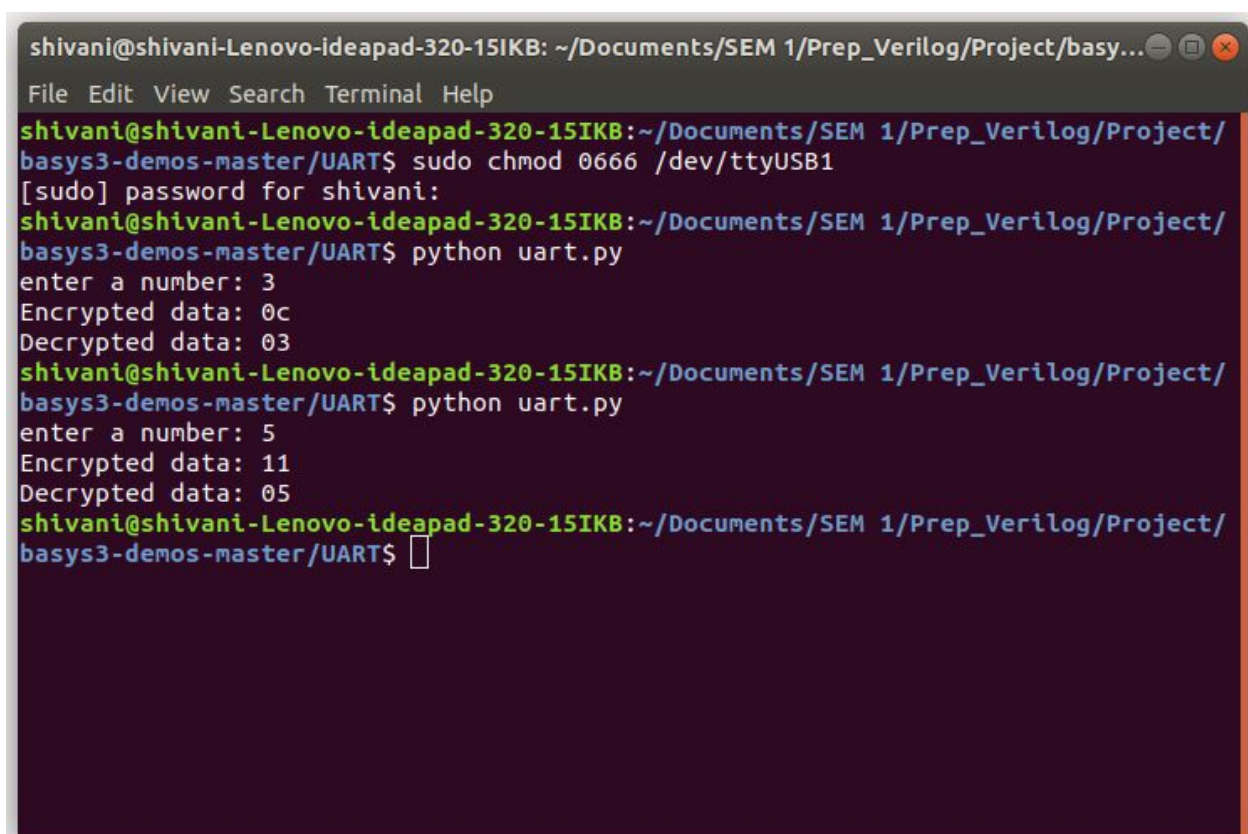
$$c = m^e \bmod n$$

$$m' = c^d \bmod n$$

### Implementation of RSA on FPGA:

- $n = p \cdot q$ , where  $p$  and  $q$  are two random prime numbers. In our code we have parameterized these two numbers so that whenever you change these values automatically it will affect the rest of the code.
- $\text{totient} = (p-1) \cdot (q-1)$  and  $e$  should be generated in such a way that  $\text{gcd}(e, \text{totient})$  is 1, i.e.  $e$  and  $\text{totient}$  should be coprime.
- private key  $d$  is generated in such a way that  $de \equiv 1 \pmod{\text{totient}}$ .

### Snapshot:



```
shivani@shivani-Lenovo-ideapad-320-15IKB: ~/Documents/SEM 1/Prep_Verilog/Project/basy...
File Edit View Search Terminal Help
shivani@shivani-Lenovo-ideapad-320-15IKB:~/Documents/SEM 1/Prep_Verilog/Project/
basy3-demos-master/UART$ sudo chmod 0666 /dev/ttyUSB1
[sudo] password for shivani:
shivani@shivani-Lenovo-ideapad-320-15IKB:~/Documents/SEM 1/Prep_Verilog/Project/
basy3-demos-master/UART$ python uart.py
enter a number: 3
Encrypted data: 0c
Decrypted data: 03
shivani@shivani-Lenovo-ideapad-320-15IKB:~/Documents/SEM 1/Prep_Verilog/Project/
basy3-demos-master/UART$ python uart.py
enter a number: 5
Encrypted data: 11
Decrypted data: 05
shivani@shivani-Lenovo-ideapad-320-15IKB:~/Documents/SEM 1/Prep_Verilog/Project/
basy3-demos-master/UART$
```

Encrypted and Decrypted data are in hex format in above screenshot.

### Acknowledgement:

UART module : <https://github.com/risikesh/basys3-demos>