Title of the mini project:

Basic Encryption Decryption Model using Asymmetric Key

Name : Shushant Kumar, Anmol Horo

Reg. No.: 16CO143, 16CO206

Abstract: This model demonstrates the basic working of encryption of data using various keys and methods and then finally decrypting the encrypted data back to get back the original data

Functionalities:

1. Initially we take a hexadecimal input and convert it into binary format using 16:4 encoder

2. Then this input is negated by passing through not gates (implemented using XOR gates)

3. This input is passed through binary to grey converter

4. This input is further passed to a private key generator which generates a private key using inputs

5. The previous input is XOR with private key , this is first level of encryption

(Private key is always generated by applying a function on each bits as shown in Logisim file)

6. Then this input is XOR with public key, second level of encryption

7. Final encrypted input is now generated and further passed to decryption model with private key

8. On decryption side the input is XOR with public key

9. Then this input is XOR with private key

10. The previous output generated is passed to grey to binary converter

11. Then this is negated by passing through not gates(implemented using XOR)

12. This data is passed through 4:16 decoder to get back the final hexadecimal decoded value

Note: All the modules are given brief description in the Logisim file

The main modules in this Logisim are :-

a) **4 bit Main(MAIN MODULE):** This module takes 4 hexadecimal inputs which are then encrypted using public and private keys and finally they are decrypted to get back original hexadecimal inputs

b) **1 bit main:** This module is a 1 bit model of previous 4 bit main model

c) **encoding :** In encoding model functionalities 1-6 are carried out.

***encoder:** This model is illustrates 16:4 encoder

***negation :** This model takes 4 bit input and returns negation of each bits

***binary to grey :** This model takes 4 bit binary code and converts it into grey code

***private key generator :** This model generates private key by certain combinations as shown in Logisim model

***4bit reg :** This model is a basic 4 bit register that stores private key

***public XOR :** This model performs XOR operation of input 4 bits with public key

***justxor:** This model is used to XOR two 4bits inputs

d) **decoding :** In decoding model functionalities 7-12 are carried out.

***public xor :** This model performs XOR operation of inputs with the public key and private key

***grey to binary:** This model takes 4 bit grey code input and converts it into binary code

***negate :** This model takes 4 bit input and gives the negation of each bits as output

***decoder :** This model illustrates 4:16 decoder

e) **4bit Encryption:** In this model 4-hexadecimal inputs are taken and they are encrypted, output of this module is the 4 8bits encrypted data.

f) **encryption:** This is single hexadecimal model of 4-bit encryption.

g) **4bit Decryption :** In this model 4-8bit encrypted data is taken and they are decrypted to give 4 hexadecimal numbers

h) **decryption:** This model is a single 8bit model of 4bit Decryption model.