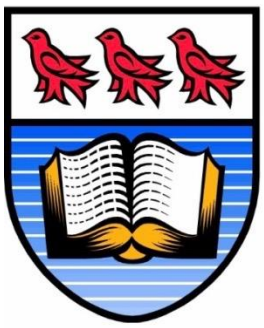

# University of Victoria

## DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

## Elec 572 Project

## Pre-Image

**Harimran Kaur**
**V00879358**

**Maninder Singh**
**V00879900**

**Mansi Lamba**
**V00876307**

# 1. θ FUNCTION:

*The pre-image mapping for data set is as follows:*

**Step 1:** *Convert the input Hexadecimal string to Binary and reverse the binary as shown.*

| For z=1 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 0 | 0 | 0 | 0 |
| 3 | 0 | 1 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 2 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 1 | 0 | 1 |
| 4 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 0 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 3 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 1 | 0 | 1 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 4 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 |
| 4 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 5 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 1 | 0 | 0 | 1 | 0 |
| 3 | 0 | 1 | 0 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 6 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 0 | 0 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 7 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 1 |
| 3 | 0 | 0 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for z = 8 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

***Step 2:*** *Expand inverted data into plane*

| y = 0 | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 0 | 0 | 1 | 1 |
| 6 | 0 | 0 | 0 | 1 | 1 |
| 5 | 1 | 1 | 1 | 1 | 0 |
| 4 | 0 | 0 | 1 | 1 | 0 |
| 3 | 0 | 1 | 1 | 0 | 1 |
| 2 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| | 4 | 3 | 0 | 1 | 2 |

| y = 1 | | | | | |
|---|---|---|---|---|---|
| 7 | 0 | 1 | 0 | 1 | 1 |
| 6 | 0 | 0 | 0 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 1 |
| 4 | 0 | 0 | 1 | 1 | 1 |
| 3 | 0 | 0 | 0 | 1 | 0 |
| 2 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 |
| | 4 | 3 | 0 | 1 | 2 |

| y = 2 | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 0 | 1 | 0 | 0 |
| 6 | 1 | 1 | 0 | 0 | 0 |
| 5 | 0 | 0 | 1 | 1 | 1 |
| 4 | 0 | 0 | 1 | 1 | 1 |
| 3 | 0 | 1 | 1 | 1 | 1 |
| 2 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 1 |
| | 4 | 3 | 0 | 1 | 2 |

| y = 3 | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 1 | 1 | 1 | 1 |
| 6 | 0 | 0 | 1 | 1 | 1 |
| 5 | 1 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 0 | 1 | 1 |
| 3 | 0 | 0 | 1 | 1 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 |
| | 4 | 3 | 0 | 1 | 2 |

| y = 4 | | | | | |
|---|---|---|---|---|---|
| 7 | 0 | 1 | 1 | 1 | 1 |
| 6 | 0 | 1 | 1 | 1 | 1 |
| 5 | 0 | 1 | 1 | 1 | 0 |
| 4 | 1 | 0 | 0 | 1 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 |
| 2 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| | 4 | 3 | 0 | 1 | 2 |

***Step 3:*** *after equation 1 of theta function*

| | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 1 | 1 | 0 | 0 |
| 6 | 1 | 0 | 0 | 1 | 1 |
| 5 | 1 | 1 | 1 | 0 | 1 |
| 4 | 1 | 1 | 1 | 1 | 1 |
| 3 | 0 | 0 | 1 | 1 | 0 |
| 2 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 0 |

***Step 3:*** *after equation 2 of theta function*

| | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 0 | 0 | 0 | 1 |
| 6 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 1 |
| 4 | 0 | 1 | 0 | 0 | 0 |
| 3 | 1 | 1 | 1 | 1 | 1 |
| 2 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 |
| | 4 | 3 | 0 | 1 | 2 |

***Step 4:*** *after equation 3 of theta function*

| | | | | | |
|---|---|---|---|---|---|
| 7 | 0 | 1 | 1 | 1 | 0 |
| 6 | 0 | 0 | 1 | 1 | 1 |
| 5 | 1 | 0 | 0 | 1 | 0 |
| 4 | 0 | 0 | 0 | 1 | 1 |
| 3 | 1 | 1 | 0 | 0 | 1 |
| 2 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 1 | 1 | 1 | 0 |
| 6 | 0 | 1 | 1 | 1 | 1 |
| 5 | 0 | 1 | 1 | 1 | 1 |
| 4 | 1 | 1 | 0 | 1 | 0 |
| 3 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 7 | 0 | 0 | 0 | 1 | 0 |
| 6 | 0 | 0 | 0 | 1 | 1 |
| 5 | 1 | 1 | 1 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 0 | 0 | 1 | 0 |
| 2 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 7 | 1 | 1 | 0 | 1 | 1 |
| 6 | 0 | 0 | 0 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 0 |
| 4 | 0 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 0 | 1 |
| 2 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| 7 | 0 | 0 | 1 | 0 | 1 |
| 6 | 1 | 1 | 0 | 0 | 0 |
| 5 | 0 | 0 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 | 1 | 1 |
| 3 | 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 1 | 0 | 0 |

***Step 5:*** *converted into slices*

| for Z=0 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 1 | 0 | 1 | 0 | 0 |
| 3 | 0 | 1 | 0 | 0 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=1 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 0 | 0 | 0 |
| 3 | 1 | 1 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=2 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 4 | 1 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=3 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 4 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 0 | 0 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=4 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 |
| 4 | 1 | 1 | 0 | 1 | 0 |
| 3 | 0 | 0 | 0 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=5 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 1 |
| 3 | 1 | 0 | 0 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=6 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 1 |
| 3 | 0 | 0 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=7 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 |
| 4 | 1 | 1 | 1 | 1 | 0 |
| 3 | 0 | 1 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

# 2.Rho (ρ) function:

*As an example, we took the following dataset and performed preimage process for the verification of the Pre-image function by mapping technique.*

**Input Bit:** 62509a9dc54838ebc9f5887fea809585eba566f47e17baf474

**Step 1:** *Convert the input Hexadecimal string to Binary and reverse the binary as shown.*

| Input (Hex) | Converted to Binary | Inverted Binary |
|---|---|---|
| dc | 11011100 | 00111011 |
| 72 | 01110010 | 01001110 |
| 62 | 01100010 | 01000110 |
| e5 | 11100101 | 10100111 |
| fc | 11111100 | 00111111 |
| 01 | 00000001 | 10000000 |
| 57 | 01010111 | 11101010 |
| 2d | 00101101 | 10110100 |
| e5 | 11100101 | 10100111 |
| 7a | 01111010 | 01011110 |
| 1f | 00011111 | 11111000 |
| ff | 11111111 | 11111111 |
| 9c | 10011100 | 00111001 |
| 8a | 10001010 | 01010001 |
| 37 | 00110111 | 11101100 |
| df | 11011111 | 11111011 |
| 56 | 01010110 | 01101010 |
| 3b | 00111011 | 11011100 |
| 4d | 01001101 | 10110010 |
| 89 | 10001001 | 10010001 |
| 41 | 01000001 | 10000010 |
| b9 | 10111001 | 10011101 |
| 62 | 01100010 | 01000110 |
| 4f | 01001111 | 11110010 |
| bc | 10111100 | 00111101 |

**Step 2:** Mapped the inverted Hex strings into slices

| for Z=0 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 4 | 1 | 0 | 1 | 1 | 0 |
| 3 | 1 | 1 | 1 | 0 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=1 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 1 | 0 | 0 | 0 | 1 |
| 3 | 0 | 0 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=2 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 4 | 1 | 1 | 0 | 0 | 0 |
| 3 | 1 | 0 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=3 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 |
| 4 | 1 | 1 | 0 | 1 | 0 |
| 3 | 1 | 1 | 1 | 0 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=4 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 |
| 4 | 0 | 1 | 0 | 1 | 0 |
| 3 | 0 | 0 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=5 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 4 | 0 | 1 | 0 | 1 | 1 |
| 3 | 0 | 0 | 0 | 0 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=6 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 4 | 1 | 0 | 1 | 0 | 1 |
| 3 | 1 | 0 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=7 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 4 | 0 | 1 | 0 | 1 | 0 |
| 3 | 0 | 1 | 1 | 0 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

**Step 3:** *Expand each slice into sheet*

| for X=3 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| 4 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 3 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=4 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 4 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 3 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=0 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 4 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=1 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 4 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 3 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=2 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

*Perform Rho operation by shifting the bits into the sheet*

| for X=3 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 4 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 3 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=4 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| 4 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 3 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=0 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| 4 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 3 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=1 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 4 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 3 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| for X=2 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 4 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**<u>Step 4</u>:** *After performing the Rho operation, we again take the bits and arrange them into their respective slices:*

| for Z=0 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 |
| 4 | 1 | 0 | 0 | 0 | 1 |
| 3 | 0 | 1 | 1 | 0 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z= 1 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 |
| 4 | 1 | 1 | 0 | 1 | 1 |
| 3 | 1 | 0 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=2 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 4 | 1 | 0 | 0 | 1 | 0 |
| 3 | 0 | 0 | 1 | 0 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=3 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 4 | 1 | 0 | 0 | 1 | 0 |
| 3 | 1 | 1 | 1 | 0 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=4 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 4 | 0 | 1 | 1 | 0 | 1 |
| 3 | 0 | 0 | 0 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z = 5 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 |
| 4 | 0 | 1 | 0 | 1 | 0 |
| 3 | 1 | 0 | 1 | 1 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=6 | | | | | |
|---|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 |
| 4 | 1 | 1 | 1 | 1 | 0 |
| 3 | 1 | 0 | 1 | 0 | 1 |
| | 3 | 4 | 0 | 1 | 2 |

| for Z=7 | | | | | |
|---|---|---|---|---|---|
| 2 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 |
| 4 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 1 | 1 | 1 | 0 |
| | 3 | 4 | 0 | 1 | 2 |

**Step 4:**

| Binary Data | Inverted Binary | Output (Hex) |
|---|---|---|
| 00111011 | 11011100 | dc |
| 10011100 | 00111001 | 39 |
| 10010001 | 10001001 | 89 |
| 01111010 | 01011110 | 5e |
| 11111001 | 10011111 | 9f |
| 00001000 | 00010000 | 10 |
| 10101110 | 01110101 | 75 |
| 00101101 | 10110100 | b4 |
| 11010011 | 11001011 | cb |
| 11100101 | 10100111 | a7 |
| 11000111 | 11100011 | e3 |
| 11111111 | 11111111 | ff |
| 11001001 | 10010011 | 93 |
| 10100010 | 01000101 | 45 |

| | | |
|---|---|---|
| 01110110 | 01101110 | 6e |
| 11111111 | 11101111 | ef |
| 01001101 | 10110010 | b2 |
| 01101110 | 01110110 | 76 |
| 01010110 | 01101010 | 6a |
| 10010001 | 10001001 | 89 |
| 00001010 | 01010000 | 50 |
| 01110110 | 01101110 | 6e |
| 11001000 | 00010011 | 13 |
| 11110010 | 01001111 | 4f |
| 01001111 | 11110010 | f2 |

# 3. Pi (π) FUNCTION:

*Let the Input state array be **A** and Output state array be **A'**.*

*Following are the steps for calculation of pi function*:

1. For all triples ($x$, $y$, $z$) such that $0 \le x < 5$, $0 \le y < 5$, and $0 \le z < w$, let **A'** [$x$, $y$, $z$]= **A**[($x + 3y$) mod 5, $x$, $z$]. **(1)**

2. Return **A'**.

The movement of bits by substituting the X and Y values from the above equation is shown as follows:

| S:No | Input | Output |
|---|---|---|
| | A | A' |
| 1 | 00 | 00 |
| 2 | 10 | 11 |
| 3 | 20 | 22 |
| 4 | 30 | 33 |
| 5 | 40 | 44 |
| 6 | 01 | 30 |
| 7 | 11 | 41 |
| 8 | 21 | 02 |
| 9 | 31 | 13 |
| 10 | 41 | 24 |
| 11 | 02 | 10 |
| 12 | 12 | 21 |
| 13 | 22 | 32 |
| 14 | 32 | 43 |
| 15 | 42 | 04 |
| 16 | 03 | 40 |
| 17 | 13 | 01 |
| 18 | 23 | 12 |
| 19 | 33 | 23 |
| 20 | 43 | 34 |
| 21 | 04 | 21 |
| 22 | 14 | 31 |
| 23 | 24 | 42 |
| 24 | 34 | 03 |

| | | |
|---|---|---|
| 25 | 44 | 14 |

*Consider the equation (1), to find the pre-image function*

Compare the similarities,

X’ = (X+3y) mod5 **(2)**
Y’ = X **(3)**
Z’ = Z **(4)**

Now, take equation **(2)**

X’= X+3Y

$Y = \frac{X' - X}{3}$

$Y= (X' - X)3\text{mod}^{-1} 5$

Value of $3\text{mod}^{-1}5$ yields 2

Y = 2(X’-X) mod 5

And X = Y’

Y = 2 (X’-Y’)mod 5

To make the mod 5 value return +ve , add +5

Y = 2(X’-Y ‘+ 5) mod 5

Convert it into equation, to get the final pre-image equation as

**A’[*x*, *y*, *z*]= A[Y , 2 (X -Y + 5) mod 5, *z*]**

# 4. chi FUNCTION:

*Function : XoR ing the bits in the entire row*

**A'= A** $\oplus$ **(**$\overline{B}$**. C)**

The forward function for chi is given by the below equation

*Input be state array **A** and Output state be array **A'**.*

*Now*,
1. For all triples (*x*, *y*, *z*) such that 0 ≤ *x* < 5, 0 ≤ *y* < 5, and 0 ≤ *z* < *w*, let

**A'** [*x*, *y*, *z*] = **A**[*x*, *y*, *z*] $\oplus$ ((**A**[(*x*+1) mod 5, *y*, *z*] $\oplus$ 1) · **A**[(*x*+2) mod 5, *y*, *z*]). **(1)**

2. Return **A'**.

*Using equation 1, we will convert the output bits into the input for the purpose of pre-image.*

| **Input** | **Output** |
|---|---|
| ABCDE | A'B'C'D'E' |
| 00000 | 0 0 0 0 0 |
| 10101 | 0 0 0 0 1 |
| 01011 | 0 0 0 1 0 |
| 01010 | 0 0 0 1 1 |
| 10110 | 0 0 1 0 0 |
| 00001 | 0 0 1 0 1 |
| 10100 | 0 0 1 1 0 |
| 10111 | 0 0 1 1 1 |
| 01101 | 0 1 0 0 0 |
| 01000 | 0 1 0 0 1 |
| 00010 | 0 1 0 1 0 |
| 00011 | 0 1 0 1 1 |
| 01001 | 0 1 1 0 0 |
| 01100 | 0 1 1 0 1 |
| 01111 | 0 1 1 1 0 |
| 01110 | 0 1 1 1 1 |
| 11010 | 1 0 0 0 0 |
| 00101 | 1 0 0 0 1 |
| 10000 | 1 0 0 1 0 |
| 11011 | 1 0 0 1 1 |

| | |
|---|---|
| 00100 | 1 0 1 0 0 |
| 10001 | 1 0 1 0 1 |
| 00110 | 1 0 1 1 0 |
| 00111 | 1 0 1 1 1 |
| 10010 | 1 1 0 0 0 |
| 11101 | 1 1 0 0 1 |
| 11000 | 1 1 0 1 0 |
| 10011 | 1 1 0 1 1 |
| 11110 | 1 1 1 0 0 |
| 11001 | 1 1 1 0 1 |
| 11100 | 1 1 1 1 0 |
| 11111 | 1 1 1 1 1 |

*Present the output to input for the purpose of deriving the equation,*

| **ABC/DE** | **00** | **01** | **10** | **11** |
|---|---|---|---|---|
| 000 | 0 | 1 | 0 | 0 |
| 001 | 1 | 0 | 1 | 1 |
| 010 | 0 | 0 | 0 | 0 |
| 011 | 0 | 0 | 0 | 0 |
| 100 | 1 | 0 | 1 | 1 |
| 101 | 0 | 1 | 0 | 0 |
| 110 | 1 | 1 | 1 | 1 |
| 111 | 1 | 1 | 1 | 1 |

*Derive the k map from above.*

K map when A=0

| DE/ABC | 000 | 001 | 011 | 010 |
|---|---|---|---|---|
| 00 | 0 | 1 | 0 | 0 |
| 01 | 1 | 0 | 0 | 0 |
| 11 | 0 | 1 | 0 | 0 |
| 10 | 0 | 1 | 0 | 0 |

K map when A=1
K map when A=0

| DE/ABC | 000 | 001 | 011 | 010 |
|---|---|---|---|---|
| 00 | 1 | 0 | 1 | 1 |
| 01 | 0 | 1 | 1 | 1 |
| 11 | 1 | 0 | 1 | 1 |

| | | | | |
|---|---|---|---|---|
| 10 | 1 | 0 | 1 | 1 |

*Group 1's together to form equation from the kmap*

AB + A$\overline{BC}$D + A$\overline{BCE}$ + A$\bar{B}$C$\bar{D}$E +$\overline{AB}$CD + $\overline{AB}$C$\bar{E}$ + $\overline{ABCD}$E
Simplifying above equation we get,
AB + $\bar{B}$(A $\oplus$ C) (D + $\bar{E}$) +$\overline{BD}$E(A$\otimes C$) **(2)**

Following is the equation for pre-image function,
**Y = AB + $\bar{B}$(A $\oplus$ C) (D + $\bar{E}$) +$\overline{BD}$E(A$\otimes C$)**

# 5. IOTA FUNCTION:

The forward mapping function of iota is based on the *two algorithms*. These algorithms are as follows:

**Algorithm 1: find *rc*(*t*)**

*Input be* integer *t* and *Output* be bit *rc*(*t*).
Following are the steps in algorithm.
1. If *t* mod 255 = 0, return 1.
2. Let *R* = 10000000.
3. For *i* from 1 to *t* mod 255, let:
a. *R* = 0 || *R*;
b. *R*[0] = *R*[0] ⊕ *R*[8];
c. *R*[4] = *R*[4] ⊕ *R*[8];
d. *R*[5] = *R*[5] ⊕ *R*[8];
e. *R*[6] = *R*[6] ⊕ *R*[8];
f. *R* =Trunc8[*R*].
4. Return *R*[0]

**Algorithm 2: ι(A, *ir*)**

Input is state array **A**; round index ir. And output is state array **A'**.

1. For all triples (*x*, *y*, *z*) such that 0 ≤ *x* < 5, 0 ≤ *y* < 5, and 0 ≤ *z* < *w*, let **A'**[*x*, *y*, *z*] = **A**[*x*, *y*, *z*].
2. Let *RC* = 0*w*.
3. For *j* from 0 to l, let *RC* [2*j* – 1] = *rc*(*j* + 7$i_r$). **(1)**
4. For all *z* such that 0 ≤ *z* < *w*, let **A'** [0, 0, *z*] = **A'** [0, 0, *z*] ⊕ *RC*[*z*]. **(2)**
5. Return **A'.**

*The effect of ι is to modify bits of Lane (0, 0) such that it depends on the round index ir with other 24 lanes not affected by ι.*

We know that, $2^l$ =8, So l = 3 Whereas, l in the equation 1 Varies from 0 to 3
the number of rounds here, $i_r$ = 2

*calculate values for RC (based on equation 1, for Round 1)*

When j =0, RC[0] = rc[7]
When j =1, RC[1] = rc[8]
When j =2, RC[3] = rc[9]
When j =3, RC[7] = rc[10]

*calculate the values for RC (based on equation 1, for Round 2)*

When j =0, RC[0] = rc[14]
When j =1, RC[1] = rc[15]
When j =2, RC[3] = rc[16]
When j =3, RC[7] = rc[17]

*By performing the operations based on the algorithm 1 and Substituting the values of t, we get value of rc.*

As we need value for rc[17], we need t only till 17 where, t ranges from 0 to 255.

Now t=0, R= 10000000 rc[0] = 1
t=1, R= 01000000 rc[1] = 0
t=2, R= 00100000 rc[2] = 0
t=3, R= 00010000 rc[3] = 0
t=4, R= 00001000 rc[4] = 0
t=5, R= 00000100 rc[5] = 0
t=6, R= 00000010 rc[6] = 0
t=7, R= 00000001 rc[7] = 0
t=8, R= 10001110 rc[8] = 1
t=9, R= 01000111 rc[9] = 0
t=10, R= 10101101 rc[10] = 1
t=11, R= 11011000 rc[11] = 1
t=12, R= 01101100 rc[12] = 0
t=13, R= 00110110 rc[13] = 0
t=14, R= 00011011 rc[14] = 0
t=15, R= 10000011 rc[15] = 1
t=16, R= 11001111 rc[16] = 1
t=17, R= 11101001 rc[17] = 1

*For Round 1 RC values are as follows:*

When j =0, RC[0] = rc[7] = 0
When j =1, RC[1] = rc[8] = 1
When j =2, RC[3] = rc[9] = 0
When j =3, RC[7] = rc[10]=1

*we can get the equation for Round 1 based on these observations*:
For j = 0 to 3,
$RC[2^j - 1] \oplus [j \bmod 2]$ **(3)**

*For Round 2 RC values are as follows*:

When j =0, RC[0] = rc[14] = 0

When j =1, RC[1] = rc[15] = 1
When j =2, RC[3] = rc[16] = 1
When j =3, RC[7] = rc[17] = 1

*we can get the equation for Round 2 based on these observations*:
For j = 0 to 3,
$RC[2^j - 1] \oplus [2^j - 1] \bmod 2$ **(4)**

*As seen that the Round 2 is derived from Round 1 i.e. the equation 4 is derived from equation 3, it is sufficient for proposed evaluation.*