Eder Mazariegos

10/16/2017

CIS3362

Assignment 5

1. C(x) = B(A(x)). Column and Row matrices multiplication applied and the answer is given below.

|  |  |  |  |
| --- | --- | --- | --- |
| 3 | 7 | 12 | 9 |
| 11 | 14 | 6 | 1 |
| 15 | 16 | 10 | 13 |
| 2 | 4 | 5 | 8 |

\*

|  |  |  |  |
| --- | --- | --- | --- |
| 16 | 13 | 10 | 5 |
| 7 | 4 | 1 | 12 |
| 2 | 11 | 14 | 9 |
| 15 | 8 | 6 | 3 |

=

|  |  |  |  |
| --- | --- | --- | --- |
| 256 | 271 | 259 | 234 |
| 301 | 273 | 214 | 280 |
| 567 | 473 | 384 | 396 |
| 190 | 161 | 142 | 127 |

1. IP and IP ^-1

|  |  |  |  |
| --- | --- | --- | --- |
| 6 | 13 | 7 | 5 |
| 11 | 15 | 9 | 16 |
| 2 | 14 | 3 | 12 |
| 8 | 1 | 4 | 10 |

In order to do the IP^-1 I simply applied the appropriate Left and Right shifts needed. In the middle of doing this however, I started to notice the pattern which started with the largest number ending in the second to last column and smallest in the bottom of the second column. With this the numbers increased and moved throughout the grid in a snake fashion.

IP^-1 =

|  |  |  |  |
| --- | --- | --- | --- |
| 12 | 4 | 16 | 8 |
| 11 | 3 | 15 | 7 |
| 10 | 2 | 14 | 6 |
| 9 | 1 | 13 | 5 |

1. 8df63098e724 = Input… Output?

100011|011111|011000|110000|100110|001110|011100|100100

S1 S2 S3 S4 S5 S6 S7 S8

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11=3 | 01=1 | 00=0 | 10=2 | 10=2 | 00=0 | 00=0 | 10=2 | : Row |
| 0001=1 | 1111=15 | 1100=12 | 1000=8 | 0011=3 | 0111=7 | 1110=14 | 0010=2 | : Col |
| = C | = 5 | = B | = F | = B | = 8 | = 6 | = 4 |  |

This was calculated using the S-Box found within the excerpts from the book posted on the class website…

1. BF8293E6 = Input… Output?

1011|1111|1000|0010|1001|0011|1110|0110

* Split into individual sections or boxes of four, then crossing the last and first bits into two new boxes within the middle of each section, we get…

010111|111111|110000|000101|010010|100111|111100|001101

* Then by splitting binary into groups of 4 or HEX,

0101|1111|1111|1100|0000|0101|0100|1010|0111|1111|0000|1101

5 F F C 0 5 4 B 7 F 0 D : HEX

1. We have 48 bits left from the k1-16 which is already known to process. Therefore, with the possible combinations of 2.81475e14… We divide 2^20 (Our processing time for one sec) by the combinations and then proceed to divide accordingly to get minutes, hours, days and years. We don’t need years for this answer, but I just did it because I was intrigued.

Answer: 3107 days (8.51 yrs.)

1. MixCols…

|  |  |  |  |
| --- | --- | --- | --- |
| A0 | 74 | 65 | 96 |
| 2B | 8D | 2E | E3 |
| 99 | 1F | C8 | 37 |
| C5 | E5 | F7 | BB |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 02 | 03 | 01 | 01 | 04 |
| 01 | 02 | 03 | 01 | 66 |
| 01 | 01 | 02 | 03 | 81 |
| 03 | 01 | 01 | 02 | E5 |

Row 4 Col 1:

(A0\*02) ⊕ (74\*01) ⊕ (65\*01) ⊕ (96\*03)

(2B\*03) ⊕ (8B\*02) ⊕ (2E\*01) ⊕ (E3\*01)

(99\*01) ⊕ (1F\*03) ⊕ (C8\*02) ⊕ (37\*01)

(C5\*01) ⊕ (E5\*01) ⊕ (F7\*03) ⊕ (BB\*02) = 11000101

11100101 = 00100000

10111001

101110110=000000100 ⊕

🡪001000100 = 24

1. W[26] = 8EFA5329

W[23] = 7EE826D3

W[27] = ?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1000 | 1110 | 1111 | 1010 | 0101 | 0011 | 0010 | 1001 |
| 0111 | 1110 | 1110 | 1000 | 0010 | 0110 | 1101 | 0011 |

⊕

= 1111|0000|0001|0010|0111|0101|1111|1010

F 0 1 2 7 5 F A : HEX

1. W[36] = 3A|74|E5|8D

W[39] = 8F|17|60|C2

1000|1111|0001|0111|0110|0000|1100|0010

0011|1010|0111|0100|1110|0101|1000|1101

=

1011|0101|0110|0011|1000|0101|0100|1111

B 5 6 3 8 5 4 F

RotWord: B5|63|85|4F 🡪[63|85|4F|B5]

SubWord: [39|05|6A|BF] (Calculated by using chart…)

RCON:

|  |  |  |
| --- | --- | --- |
| 39 | ⊕ | 01 |
| 05 | ⊕ | 00 |
| 6A | ⊕ | 00 |
| BF | ⊕ | 00 |

=

|  |
| --- |
| 38 |
| 05 |
| 6A |
| BF |

1. The numbers do not appear the same number of times. There are 16x48 Values (56 possible) and it has an avg. of about 0.0729 percent and since the integer doesn’t exist, there is no way every value could appear exactly that many times.
2. The shift rows would be in the order of 0,1,2,3 which would yield a matrix of…

|  |  |  |  |
| --- | --- | --- | --- |
| 01 | 89 | FE | 76 |
| AB | DC | 54 | 23 |
| BA | 32 | 45 | CD |
| 10 | 67 | EF | 98 |

🡪0

🡪1

🡪2

🡪3