Homework4

Jun Rao

jr2339@nau.edu

**Find , the inverse of with GF, and after affine mapping.**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 0101 1000 | 0001 1000 | 0110 1010 |
| 1101 0001 | 0000 0111 | 0011 1110 |
| 1011 1010 | 0111 0110 | 1111 0100 |
| 1110 0011 | 1110 1011 | 0001 0001 |
| 0110 1000 | 1111 0100 | 0100 0101 |

= 0101 1000 = 5 8 ---------> = 1 8 = 0001 1000 ---------> = 6 A = 0110 1010

= + = = 0110 1010 = 6A

= 1101 0001= D 1 ---------> = 0 7 = 0000 0111 ---------> = 3 E = 0011 1110

= + = = 0011 1110 = 3 E

= 1011 1010= B A ---------> = 7 6 = 0111 0110 ---------> = 3 E = 0011 1110

= + = = 1111 0100 = F 4

= 1110 0011= E 3 ---------> = E B = 1110 1011 ---------> = 1 1 = 0001 0001

= + = = 0001 0001 = 1 1

= 0110 1000= 6 8 ---------> = F 4 = 1111 0100 ---------> = 4 5 = 0100 0101

= + = = 0100 0101 = 45

**Find , ,, from , ,, with mix column transform**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| 0101 1000 | 1101 0001 | 1011 1010 | 1110 0011 |
|  |  |  |  |
|  |  |  |  |

= 0101 1000 = + +

= 1101 0001 =  + + + 1

= 1011 1010 =  + + +

= 1110 0011 = + + + + 1

01 = 1

02 =

03 = + 1

P () = + + + 1

=

=

=

mod P () =

=