**ASSIGNMENT REPORT – WEEK 5**

|  |  |  |
| --- | --- | --- |
| **Instructor** | **PhD. Nguyễn Ngọc Tự** | |
| **Student** | Mai Nguyễn Phúc Minh | 23520930 |

1. Chứng minh M.M(^-1) = I trong GF(2^8) mod (x⁸ + x⁴ + x³ + x + 1)

**Chứng minh tương tự với các phép tính ta dễ dàng thấy M.M(^-1) = I**

**Dựa vào công thức:**

**a’0,j = M (a0,j) ⊕ [M (a1,j) ⊕ a1,j] ⊕ a2,j ⊕ a3,j​**

**a’1,j = a0,j ⊕ M (a1,j) ⊕ [M (a2,j )⊕a2,j] ⊕ a3,j​**

**a’2,j = a0,j ⊕ a1,j ⊕ M (a2,j ) ⊕ [M (a3,j ) ⊕ a3,j]​**

**a’3,j = [M (a0,j )⊕ a0,j ] ⊕ a1,j ⊕ a2,j ⊕ M (a3,j )​**

