

Report Week 4

1. Chứng minh $M \cdot M^{-1} = I$ trong $GF(2^8) \pmod{x^8 + x^4 + x^3 + x + 1}$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 5 & 1 \\ 1 & 1 & 2 & 3 \\ 1 & 6 & 4 & 3 & 2 \end{bmatrix} \quad \begin{bmatrix} 14 & 14 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix}$$

Nhân hai ma trận này ra có được:

$$\begin{bmatrix} 79 & 86 & 82 & 82 \\ 82 & 79 & 86 & 82 \\ 82 & 82 & 79 & 86 \\ 86 & 82 & 82 & 79 \end{bmatrix}$$

Nhân tiếp từng hàng sau sẽ là hàng được shift 1. Nên chỉ cần tính hàng đầu tiên được sẽ tính được các hàng còn lại.

Định nhân hai ma trận trong $GF(2^8) \pmod{x^8 + x^4 + x^3 + x + 1}$

- $S_{0,0} = 2 \cdot 14 \oplus 3 \cdot 9 \oplus 1 \cdot 13 \oplus 1 \cdot 11$
 $= x \cdot (x^3 + x^2 + x) \oplus (x+1)(x^3+1) \oplus (x^3+x^2+1) \oplus (x^3+x+1)$
 $= (x^4+x^3+x^2) \oplus (x^4+x^3+x+1) \oplus (x^3+x^2+1) \oplus (x^3+x+1)$
 $= 1$

- $S_{0,1} = 2 \cdot 11 \oplus 3 \cdot 14 \oplus 1 \cdot 9 \oplus 1 \cdot 13$
 $= x(x^3+x+1) \oplus (x+1)(x^3+x^2+x) \oplus (x^3+1) \oplus (x^3+x^2+1)$
 $= (x^4+x^2+x) \oplus (x^4+x^3+x^2+x^2+x) \oplus (x^3+1) \oplus (x^3+x^2+1)$
 $= 0$

- $S_{0,2} = 2 \cdot 13 \oplus 3 \cdot 11 \oplus 1 \cdot 4 \cdot 1 \oplus 1 \cdot 9$
 $= x(x^3+x^2+1) \oplus (x+1)(x^3+x+1) \oplus (x^3+x^2+x) \oplus (x^3+1)$
 $= (x^4+x^3+x) \oplus (x^4+x^3+x^2+x+x+1) \oplus (x^3+x^2+x) \oplus (x^3+1)$
 $= 0$

- $S_{0,3} = 2 \cdot 9 \oplus 3 \cdot 13 \oplus 1 \cdot 11 \oplus 1 \cdot 14$
 $= (x^4+x) \oplus (x^4+x^3+x^3+x^2+x+1) \oplus (x^3+x+1) \oplus (x^3+x^2+x)$
 $= 0$

Như vậy ta được: $M \cdot M^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I \pmod{x^8+x^4+x^3+x+1}$