VE475 Intro to Cryptography Homework 3

Taoyue Xia, 518370910087

2021/06/02

1 Ex1

1. Take X's value as 0, 1, 2 in $\mathbb{F}_3[X]$:

$$0^2 + 1 = 1 \ mod \ 3 \quad 1^2 + 1 = 2 \ mod \ 3 \quad 2^2 + 1 = 2 \ mod \ 3$$

   We can see that for $X \in \mathbb{F}_3[X]$, there doesn't exists an X which makes $X^2 + 1 = 0 \ mod \ 3$
   Thus $X^2 + 1$ is irreducible in $\mathbb{F}_3[X]$.

2. In question 1, we proved that $X^2 + 1$ is irreducible in $\mathbb{F}_3[X]$, and the polynomial $1 + 2X$'s degree is less than 2, according to the proof on page 39, c2, Let $P(X) = X^2 + 1$, $A(X) = 1 + 2X$, then there always exists a $B(X)$, such that $A(X)\,B(X) = 1 \ mod \ P(X)$, which means $B(x)$ is the multiplication inverse of $1 + 2X \ mod \ X^2 + 1$. Proof done.

3. Apply the extended Euclidean algorithm, let a and b be such that $a(1 + 2X) + b(X^2 + 1) = 1 \ mod \ 3$. Then calculate in matrix form(a's value in the first column, b's value in the second):

$$\begin{pmatrix} 1 & 0 & 1+2X \\ 0 & 1 & X^2+1 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 1 & X^2+1 \\ 1 & 0 & 1+2X \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1+2X \\ X & 1 & X+1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} X & 1 & X+1 \\ X+1 & 1 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} X+1 & 1 & 2 \\ X^2+2X & X+1 & 1 \end{pmatrix}$$

Thus we can find that the multiplication inverse of $1+2X$ mod X^2+1 is X^2+2X.

2 Ex2

1. The *InvShiftRows* function cyclicly shift each row i's elements right for $i = 0,\ 1,\ 2\,3$.

   For example, if the 4×4 matrix is $\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{bmatrix}$, then the matrix after the operation *InvShiftRow* would be: $\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$.