Lecture 4: Irreducible Polynomials in AES

LEARNING OUTCOME
By the end of the lesson the student will be able to:

a) understand a concept of irreducible polynomial in AES
b) to multiply two polynomials
c) compute a matrix multiplication in AES.
d) Compute one round of AES

A ring over an irreducible polynomial has been used in modern cryptosystem, namely, ECC, AES and NTRU. In AES algorithm, this irreducible polynomial is

$m(x) = x^8 + x^4 + x^3 + x + 1 = 100011011_2$ = or {01}{1B} in hexadecimal notation.

In the S-box of AES, take the multiplicative inverse in the finite field GF(2^8) first where element {00} is mapped to itself {00}.

Let us take $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ from the top left corner of the S-box and then

$$\begin{bmatrix} b_0^{'} \\ b_1^{'} \\ b_2^{'} \\ b_3^{'} \\ b_4^{'} \\ b_5^{'} \\ b_6^{'} \\ b_7^{'} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 63_{16}$$

One more time, Let us take $\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ from the bottom right corner of the S-box and then we need to take multiplicative inverse first modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1 = 100011011_2$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Let us give an overview of multiplication between two bytes.

{57} • {83} = {C1}

$= (0101\ \ 0111) \cdot (1000\ \ 0011)$ written little endian

```
   10000011
     10000011
        10000011
         10000011
          10000011
=  101001121101221 mod 2 = 10101101101001
```

The convolution will result in

$(0101\ \ 0111) \cdot (1000\ \ 0011) = 10101101101001$

In polynomial, it is written as

$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^3 + 1 \bmod x^8 + x^4 + x^3 + x + 1$

```
=10101101101001
 100011011
```

```
=   100000011001
    100011011
=       11000001=C1.
```

Let us review the mix-column operation in AES encryption. At a certain round, let the state $S=\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix}$ and the mix-column matrix $M=\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$.

It might be a good idea to write the matrix side by side.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

The whole mix-column operation is a matrix multiplication

$$S' = MS$$

$$\begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix}$$

And now, we can see the inverse mix column during the decryption process,

$$S = M^{-1}S'$$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}\begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

Let take an example from the top left corner,

$$s_{00} = \{0E\} \cdot \{s'_{00}\} + \{0B\} \cdot \{s'_{10}\} + \{0D\} \cdot \{s'_{20}\} + \{09\} \cdot \{s'_{30}\}$$

Round	Start of Round	After SubBytes	After ShiftRows	After Mix Columns		Round Key Value
	00 44 88 CC					00 04 08 0C
0 input	11 55 99 DD				⊕	01 05 09 0D
	22 66 AA EE					02 06 0A 0E
	33 77 BB FF					03 07 0B 0F
	00 40 80 C0	63 09 CD BA	63 09 CD BA	5F 57 F7 1D		D6 D2 DA D6
1	10 50 90 D0	CA 53 60 70	53 60 70 CA	72 F5 BE B9	⊕	AA AF A6 AB
	20 60 A0 E0	B7 D0 E0 E1	E0 E1 B7 D0	64 BC 3B F9		74 72 78 76
	30 70 B0 F0	04 51 E7 8C	8C 04 51 E7	15 92 29 1A		FD FA F1 FE

From the above standard sample,
The whole mix-column operation is a matrix multiplication

$$S' = MS$$

$$\begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 63 & 09 & CD & BA \\ 53 & 60 & 70 & CA \\ E0 & E1 & B7 & D0 \\ 8C & 04 & 51 & E7 \end{bmatrix}$$

And now, we can see the inverse mix column during the decryption process,

$$S = M^{-1}S'$$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 5F & 57 & F7 & 1D \\ 72 & F5 & BE & B9 \\ 64 & BC & 3B & F9 \\ 15 & 92 & 29 & 1A \end{bmatrix}$$

Let take an example from the top left corner,

$$s_{00} = \{0E\} \cdot \{5F\} + \{0B\} \cdot \{72\} + \{0D\} \cdot \{64\} + \{09\} \cdot \{15\}$$

Lab Test 4: One round of AES~LT (10%) –C3 PO2

Do the initial and first round of AES Encryption on the string plaintext M using a given symmetric key K. Take the plaintext M as the first 16 character of your name instead. You are also given symmetric key K written in hexadecimals. Compute for full Round 1 until Initial Round 2 State Array.