**Tutorial 3a: AES S-box**

**LEARNING OUTCOME**

**By the end of the lesson the student will be able to:**

1. understand a concept of S-box in AES
2. compute an S-box output from AES
3. compute an Affine Transform

Take y = matrix ID mod 100 as the last 2 digit of ID number.

1. Take *a* = 100 + y, convert to hexa, take *a*1 (mod *b*) from an inverse table
2. An irreducible polynomial *b*(*x*) = *x*8+ *x*4+ *x*3+*x*+1 where *b*(2) = 28310.
3. Plug in an inverse into an Affine Transform to get an output for AES S-box.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *a*-1 |  | **0** |  | **1** |  | **2** |  | **3** |  | **4** |  | **5** |  | **6** |  | **7** |  | **8** |  | **9** |  | **A** |  | **B** |  | **C** |  | **D** |  | **E** |  | **F** |
| **0** | 0 | 0 | 0 | 1 | 8 | D | F | 6 | C | B | 5 | 2 | 7 | B | D | 1 | E | 8 | 4 | F | 2 | 9 | C | 0 | B | 0 | E | 1 | E | 5 | C | 7 |
| **1** | 7 | 4 | B | 4 | A | A | 4 | B | 9 | 9 | 2 | B | 6 | 0 | 5 | F | 5 | 8 | 3 | F | F | D | C | C | **F** | **F** | 4 | 0 | E | E | B | 2 |
| **2** | 3 | A | 6 | E | 5 | A | F | 1 | 5 | 5 | 4 | D | A | 8 | C | 9 | C | 1 | 0 | A | 9 | 8 | 1 | 5 | 3 | 0 | 4 | 4 | A | 2 | C | 2 |
| **3** | 2 | C | 4 | 5 | 9 | 2 | 6 | C | F | 3 | 3 | 9 | 6 | 6 | 4 | 2 | F | 2 | 3 | 5 | 2 | 0 | 6 | F | 7 | 7 | B | B | 5 | 9 | 1 | 9 |
| **4** | 1 | D | F | E | 3 | 7 | 6 | 7 | 2 | D | 3 | 1 | F | 5 | 6 | 9 | A | 7 | 6 | 4 | A | B | 1 | 3 | 5 | 4 | 2 | 5 | E | 9 | 0 | 9 |
| **5** | E | D | 5 | C | 0 | 5 | C | A | 4 | C | 2 | 4 | 8 | 7 | B | F | 1 | 8 | 3 | E | 2 | 2 | F | 0 | 5 | 1 | E | C | 6 | 1 | 1 | 7 |
| **6** | 1 | 6 | 5 | E | A | F | D | 3 | 4 | 9 | A | 6 | 3 | 6 | 4 | 3 | F | 4 | 4 | 7 | 9 | 1 | D | F | 3 | 3 | 9 | 3 | 2 | 1 | 3 | B |
| **7** | 7 | 9 | B | 7 | 9 | 7 | 8 | 5 | 1 | 0 | B | 5 | B | A | 3 | C | B | 6 | 7 | 0 | D | 0 | 0 | 6 | A | 1 | F | A | 8 | 1 | 8 | 2 |
| **8** | 8 | 3 | 7 | E | 7 | F | 8 | 0 | 9 | 6 | 7 | 3 | B | E | 5 | 6 | 9 | B | 9 | E | 9 | 5 | D | 9 | F | 7 | 0 | 2 | B | 9 | A | 4 |
| **9** | D | E | 6 | A | 3 | 2 | 6 | D | D | 8 | 8 | A | 8 | 4 | 7 | 2 | 2 | A | 1 | 4 | 9 | F | 8 | 8 | F | 9 | D | C | 8 | 9 | 9 | A |
| **A** | F | B | 7 | C | 2 | E | C | 3 | 8 | F | B | 8 | 6 | 5 | 4 | 8 | 2 | 6 | C | 8 | 1 | 2 | 4 | A | C | E | E | 7 | D | 2 | 6 | 2 |
| **B** | 0 | C | E | 0 | 1 | F | E | F | 1 | 1 | 7 | 5 | 7 | 8 | 7 | 1 | A | 5 | 8 | E | 7 | 6 | 3 | D | B | D | B | C | 8 | 6 | 5 | 7 |
| **C** | 0 | B | 2 | 8 | 2 | F | A | 3 | D | A | D | 4 | E | 4 | 0 | F | A | 9 | 2 | 7 | 5 | 3 | 0 | 4 | 1 | B | F | C | A | C | E | 6 |
| **D** | 7 | A | 0 | 7 | A | E | 6 | 3 | C | 5 | D | B | E | 2 | E | A | 9 | 4 | 8 | B | C | 4 | D | 5 | 9 | D | F | 8 | 9 | 0 | 6 | B |
| **E** | B | 1 | 0 | D | D | 6 | E | B | C | 6 | 0 | E | C | F | A | D | 0 | 8 | 4 | E | D | 7 | E | 3 | 5 | D | 5 | 0 | 1 | E | B | 3 |
| **F** | 5 | B | 2 | 3 | 3 | 8 | 3 | 4 | 6 | 8 | 4 | 6 | 0 | 3 | 8 | C | D | D | 9 | C | 7 | D | A | 0 | C | D | 1 | A | 4 | 1 | 1 | C |

Table 3.2 An inverse table *a*(*x*) mod *m*(*x*) = *x*8+*x*4+*x*3+*x*+1.

An inverse usually gives a good unpredictable spread.

In AES algorithm, this irreducible polynomial is

=1000110112 = 28310 or {01}{1B} in hexadecimal notation.

In the S-box of AES, take the multiplicative inverse in the finite field GF(28) first where

element {00} is mapped to itself {00}.

Let us take  from the top left corner of the S-box and then y =Ax + c= 011000112 = 6316.

Note: A matrix multiplication here is written in big-endian.

One more time, Let us take  from the bottom right corner of the S-box and then we need to take multiplicative inverse first modulo the irreducible polynomial =1000110112

=100111002=9C16.

An S-box used in the **SubBytes()** transformation is presented in hexadecimal index.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | y | | | | | | | | | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| x | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

An Affine Transform in AES is given as



Let *a*(*x*) = *x*5+*x*3+*x* and *m*(*x*) = *x*8+*x*4+*x*3+*x*+1 be the polynomials respectively.

For *a* = 4210 = 32+8+2 = 1010102 = *x*5+*x*3+*x* = 2A16. Trace along row 2 and column A, an answer is 9816.

From the *a* = 4210 = 1010102 = 2A16, then *a*−1 = 15210 =100110002 = 9816. Thus, *a*−1(*x*) = *x*7+*x*4+*x*3.

Let us see again, from an initial input *a* = 4210 = 1010102 = 2A16,

Then *a*−1 = 15210 =100110002 = 9816.

=111001012=E516.

One more time, take *a* = 4310 = 32+8+2+1 = 1010112 = *x*5+*x*3+*x*+1= 2B16. Trace along row 2 and column B, an answer is 1516. From the *a* = 4310 = 1010112 = 2B16, then *a*−1  =101012 = 1516. Thus, in polynomial *a*−1(*x*) = *x*4+*x*2+1.

Let us take another example: Suppose *a*= 200 = 128+64+8= 110010002 = C816.

Then from an inverse table, we will get *a−*1 = A916 = 101010012

==111010002=E816.

An S-box used in the **SubBytes()** transformation is presented in hexadecimal index.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | y | | | | | | | | | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| x | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |