Advanced Encryption Standard (AES)

**Advanced Encryption Standard (AES):** The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details
* Software implementable in C and Java

**Example:**

**Plaintext**  : {A17067B7C7A2B6045766FD827DD8B3B5)

**Key**  : {3F0EBF2BBC1589A33E21B2BDAD71A23C}

**1. Initial contents of the State Array displayed as a 4 x 4 matrix**

Plaintext {A17067B7C7A2B6045766FD827DD8B3B5)

|  |  |  |  |
| --- | --- | --- | --- |
| A1 | C7 | 57 | 7D |
| 70 | A2 | 66 | D8 |
| 67 | B6 | FD | B3 |
| B7 | 04 | 82 | B5 |

Key {3F0EBF2BBC1589A33E21B2BDAD71A23C}

|  |  |  |  |
| --- | --- | --- | --- |
| 3F | BC | 3E | AD |
| 0E | 15 | 21 | 71 |
| BF | 89 | B2 | A2 |
| 2B | A3 | BD | 3C |

**Value of State after initial Add Round Key:**

A1 = 1010 0001

3F = 0011 1111

⊕ = 1010 0010

Hexadecimal equivalent of 1010 0010= A2

|  |  |  |  |
| --- | --- | --- | --- |
| A1 | C7 | 57 | 7D |
| 70 | A2 | 66 | D8 |
| 67 | B6 | FD | B3 |
| B7 | 04 | 82 | B5 |

⊕

|  |  |  |  |
| --- | --- | --- | --- |
| 3F | BC | 3E | AD |
| 0E | 15 | 21 | 71 |
| BF | 89 | B2 | A2 |
| 2B | A3 | BD | 3C |

**=**

|  |  |  |  |
| --- | --- | --- | --- |
| A2 | 7B | 07 | D0 |
| 7E | B7 | 47 | A9 |
| D8 | 3F | 4F | 11 |
| 9C | A7 | 3F | 89 |

**Value of State after Sub Bytes:**

In this step, we use a lookup table called S-box to perform a byte-by-byte substitution of the block. For example,

A2

Row A

Column 2

E

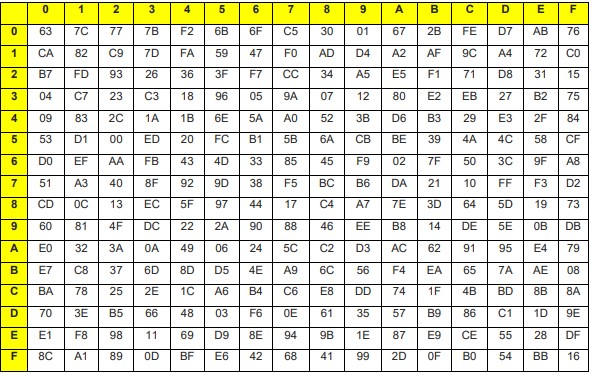
5

So, the value of State after Sub Bytes:

|  |  |  |  |
| --- | --- | --- | --- |
| A2 | 7B | 07 | D0 |
| 7E | B7 | 47 | A9 |
| D8 | 3F | 4F | 11 |
| 9C | A7 | 3F | 89 |

**=>**

|  |  |  |  |
| --- | --- | --- | --- |
| E5 | A9 | 51 | D7 |
| 94 | 21 | 92 | B8 |
| 5D | 0D | BF | 82 |
| DD | DA | 0D | A7 |

 **Table 1**: S-box

**Value of State after Shift Rows:**

|  |  |  |  |
| --- | --- | --- | --- |
| E5 | A9 | 51 | D7 |
| 94 | 21 | 92 | B8 |
| 5D | 0D | BF | 82 |
| DD | DA | 0D | A7 |

**=>**

|  |  |  |  |
| --- | --- | --- | --- |
| E5 | A9 | 51 | D7 |
| 21 | 92 | B8 | 94 |
| BF | 82 | 5D | 0D |
| A7 | DD | DA | 0D |

**5. Value of State after Mix Columns:**

In this step, a forward mix column transformation, called Mix Columns, is performed on each column individually.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 02 03  01 02    01 01    03 01  Here, | 01  03  02  01 | 01  01 x 𝐵𝐹𝐸215    03  02 𝐴7 | 𝐴9  92  82  𝐷𝐷 | 51  𝐵8  5𝐷  𝐷𝐴 |  *r*1 𝐷7 *r*5  94=   0𝐷 *r*9  0𝐷   *r*13 | *r*2 *r*6  *r*10 *r*14 | *r*3 *r*7  *r*11 *r*15 | *r*4 *r*8   *r*12 *r*16 |

Rules of r1 is = (02\*E5) r1.

Rules of r2 is = (02\*A9)\*DD) = r2.

Rules of r3 is = (02\*51)(01\*DA) = r3.

Rules of r4 is = (02\*D7)\*0D) = r4.

Rules of r5 is = (01\*E5)

Rules of r6 is = (01\*A9) (01\*DD) = r6.

Rules of r7 is = (01\*51)(01\*DA) = r7.

Rules of r8 is = (01\*D7) 

Rules of r9 is = (01\*E5)

Rules of r10 is = (01\*A9)(03\*DD) = r10.

Rules of r11 is = (01\*51) (03\*DA) = r11.

Rules of r12 is = (01\*D7) ⊕ (01\*94) ⊕ (02\*0D) ⊕ (03\*0D) = r12.

Rules of r13 is = (01\*E5) ⊕ (01\*21) ⊕ (02\*BF) ⊕ (03\*A7) = r13.

Rules of r14 is = (03\*A9) ⊕ (01\*92) ⊕ (01\*82) ⊕ (02\*DD) = r14.

Rules of r15 is = (03\*51) ⊕ (01\*B8) ⊕ (01\*5D) ⊕ (02\*DA) = r15.

Rules of r16 is = (03\*D7) ⊕ (01\*94) ⊕ (01\*0D) ⊕ (02\*0D) = r16.