

a.

|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 04 | 08 | 0C |
| 01 | 05 | 09 | 0D |
| 02 | 06 | 0A | 0E |
| 03 | 07 | 0B | 0F |

b. AddRoundKey

State = Input

AddRoundKey: state = state K



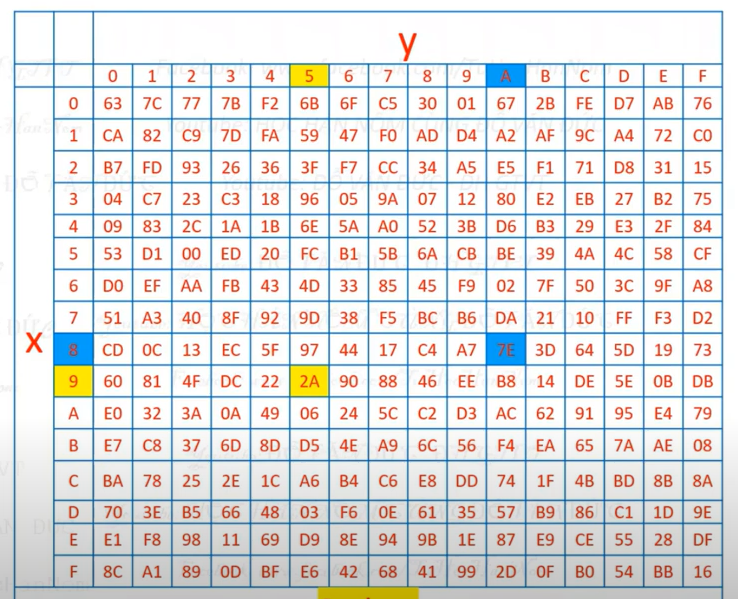
|  |  |  |  |
| --- | --- | --- | --- |
| 00 | 04 | 08 | 0C |
| 01 | 05 | 09 | 0D |
| 02 | 06 | 0A | 0E |
| 03 | 07 | 0B | 0F |

|  |  |  |  |
| --- | --- | --- | --- |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |
| 01 | 01 | 01 | 01 |

|  |  |  |  |
| --- | --- | --- | --- |
| 01 | 05 | 09 | 0D |
| 00 | 04 | 08 | 0C |
| 03 | 07 | 0B | 0F |
| 02 | 06 | 0A | 0E |

c. SubBytes

State = ShiftRows(State)



|  |  |  |  |
| --- | --- | --- | --- |
| 7C | 6B | 01 | D7 |
| 63 | F2 | 30 | FE |
| 7B | C5 | 2B | 76 |
| 77 | 6F | 67 | AB |

|  |  |  |  |
| --- | --- | --- | --- |
| 01 | 05 | 09 | 0D |
| 00 | 04 | 08 | 0C |
| 03 | 07 | 0B | 0F |
| 02 | 06 | 0A | 0E |

d. ShiftRows

State = ShiftRow(State)

|  |  |  |  |
| --- | --- | --- | --- |
| 7C | 6B | 01 | D7 |
| F2 | 30 | FE | 63 |
| 2B | 76 | 7B | C5 |
| AB | 77 | 7F | 67 |

* Hàng i dịch vòng trái (i-1) byte

|  |  |  |  |
| --- | --- | --- | --- |
| 7C | 6B | 01 | D7 |
| 63 | F2 | 30 | FE |
| 7B | C5 | 2B | 76 |
| 77 | 6F | 67 | AB |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

e. MixColumns



|  |  |  |  |
| --- | --- | --- | --- |
| 02 | 03 | 01 | 01 |
| 01 | 02 | 03 | 01 |
| 01 | 01 | 02 | 03 |
| 03 | 01 | 01 | 02 |

|  |  |  |  |
| --- | --- | --- | --- |
| 7C | 6B | 01 | D7 |
| F2 | 30 | FE | 63 |
| 2B | 76 | 7B | C5 |
| AB | 77 | 7F | 67 |