Text

Description automatically generated

Plaintext: 000102030405060708090A0B0C0D0E0F

Key: 01010101010101010101010101010101

a.

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

W0 = 01010101 W1 = 01010101 W2 = 01010101 W3 = 01010101

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| i | temp | After  RotWord() | After  SubWord() | Rcon  [i/Nk] | AfterXOR  withRcon | w[i-Nk] | w[i] |
| 4 | 01010101 | 01010101 | 7c7c7c7c | 01000000 | 7d7c7c7c | 01010101 | 7c7d7d7d |
| 5 | 7c7d7d7d |  |  |  |  | 01010101 | 7d7c7c7c |
| 6 | 7d7c7c7c |  |  |  |  | 01010101 | 7c7d7d7d |
| 7 | 7c7d7d7d |  |  |  |  | 01010101 | 7d7c7c7c |
| 8 | 7d7c7c7c | 7c7c7c7d | 101010ff | 02000000 | 121010ff | 7c7d7d7d | 6e6d6d82 |
| 9 | 6e6d6d82 |  |  |  |  | 7d7c7c7c | 131111fe |
| 10 | 131111fe |  |  |  |  | 7c7d7d7d | 6f6c6c83 |
| 11 | 6f6c6c83 |  |  |  |  | 7d7c7c7c | 121010ff |
| 12 | 121010ff | 1010ff12 | caca16c9 | 04000000 | ceca16c9 | 6e6d6d82 | a0a77b4b |
| 13 | a0a77b4b |  |  |  |  | 131111fe | b3b66ab5 |
| 14 | b3b66ab5 |  |  |  |  | 6f6c6c83 | dcda0636 |
| 15 | dcda0636 |  |  |  |  | 121010ff | ceca16c9 |
| 16 | ceca16c9 | ca16c9ce | 7447dd8b | 08000000 | 7c47dd8b | a0a77b4b | dce0a6c0 |
| 17 | dce0a6c0 |  |  |  |  | b3b66ab5 | 6f56cc75 |
| 18 | 6f56cc75 |  |  |  |  | dcda0636 | b38cca43 |
| 19 | b38cca43 |  |  |  |  | ceca16c9 | 7d46dc8a |
| 20 | 7d46dc8a | 46dc8a7d | 5a867eff | 10000000 | 4a867eff | dce0a6c0 | 9666d83f |
| 21 | 9666d83f |  |  |  |  | 6f56cc75 | f930144a |
| 22 | f930144a |  |  |  |  | b38cca43 | 4abcde09 |
| 23 | 4abcde09 |  |  |  |  | 7d46dc8a | 37fa0283 |
| 24 | 37fa0283 | fa028337 | 2d77ec9a | 20000000 | 0d77ec9a | 9666d83f | 9b1134a5 |
| 25 | 9b1134a5 |  |  |  |  | f930144a | 622120ef |
| 26 | 622120ef |  |  |  |  | 4abcde09 | 289dfee6 |
| 27 | 289dfee6 |  |  |  |  | 37fa0283 | 1f67fc65 |
| 28 | 1f67fc65 | 67fc651f | 85b04dc0 | 40000000 | c5b04dc0 | 9b1134a5 | 5ea17965 |
| 29 | 5ea17965 |  |  |  |  | 622120ef | 3c80598a |
| 30 | 3c80598a |  |  |  |  | 289dfee6 | 141da76c |
| 31 | 141da76c |  |  |  |  | 1f67fc65 | 0b7a5b09 |
| 32 | 0b7a5b09 | 7a5b090b | da39012b | 80000000 | 5a39012b | 5ea17965 | 0498784e |
| 33 | 0498784e |  |  |  |  | 3c80598a | 381821c4 |
| 34 | 381821c4 |  |  |  |  | 141da76c | 2c0586a8 |
| 35 | 2c0586a8 |  |  |  |  | 0b7a5b09 | 277fdda1 |
| 36 | 277fdda1 | 7fdda127 | d2c132cc | 1B000000 | c9c132cc | 0498784e | cd594a82 |
| 37 | cd594a82 |  |  |  |  | 381821c4 | f5416b46 |
| 38 | f5416b46 |  |  |  |  | 2c0586a8 | d944edee |
| 39 | d944edee |  |  |  |  | 277fdda1 | fe3b304f |
| 40 | fe3b304f | 3b304ffe | e20484bb | 36000000 | d40484bb | cd594a82 | 195dce39 |
| 41 | 195dce39 |  |  |  |  | f5416b46 | ec1ca57f |
| 42 | ec1ca57f |  |  |  |  | d944edee | 35584891 |
| 43 | 35584891 |  |  |  |  | fe3b304f | cb6378de |

**Lặp lần 1:**

b. AddRoundKey

- state = input = 000102030405060708090A0B0C0D0E0F

AddRoundKey: state = state  K

=> state W[0,3]

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

=

=> state = 010003020504070609080B0A0D0C0F0E

c. SubBytes

State = ShiftRows(State)

-VD: SubBytes({8A}) = {7E}

Dự vào bảng dưới để SubBytes.

Table

Description automatically generated

Ta có ma trận vừa tìm được là => Ma trận sau khi SubBytes

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

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

d. ShiftRows

State = ShiftRow(State)

Hàng i dịch vòng trái (i-1) byte

Ta có ma trận vừa tìm được là => Ma trận sau khi ShiftRows

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

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

e. MixColumns: Nhân ma trận



Ma trận vừa thu được đem nhân với ma trận

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

Ta có ma trận vừa tìm được là => Ma trận sau khi MixColumns

|  |  |  |  |
| --- | --- | --- | --- |
| 75 | 87 | 0F | B2 |
| 55 | E6 | 04 | 22 |
| 3E | 2E | B8 | 8C |
| 10 | 15 | 58 | 0A |

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

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

x =

**Các lần lặp tiếp theo:** Tương tự như trên và ta sẽ thu được bảng sau:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Round Number | State of Round | | | |  | After SubBytes | | | |  | After ShiftRows | | | |  | After MixColumns | | | |  | Round key value | | | |  | |
|  | |
| input | 00 | 04 | 08 | 0C |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | XOR | 01 | 01 | 01 | 01 | = |
| 01 | 05 | 09 | 0D |  |  |  |  |  |  |  |  |  |  |  |  | 01 | 01 | 01 | 01 |
| 02 | 06 | 0A | 0E |  |  |  |  |  |  |  |  |  |  |  |  | 01 | 01 | 01 | 01 |
| 03 | 07 | 0B | 0F |  |  |  |  |  |  |  |  |  |  |  |  | 01 | 01 | 01 | 01 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 | 05 | 09 | 0D |  | 7C | 6B | 01 | D7 |  | 7C | 6B | 01 | D7 |  | 75 | 87 | 0F | B2 | XOR | 7C | 7D | 7C | 7D | = |
| 00 | 04 | 08 | 0C | 63 | F2 | 30 | FE | F2 | 30 | FE | 63 | 55 | E6 | 04 | 22 | 7D | 7C | 7D | 7C |
| 03 | 07 | 0B | 0F | 7B | C5 | 2B | 76 | 2B | 76 | 7B | C5 | 3E | 3E | B8 | 8C | 7D | 7C | 7D | 7C |
| 02 | 06 | 0A | 0E | 77 | 6F | 67 | AB | AB | 77 | 6F | 67 | 10 | 15 | 58 | 0A | 7D | 7C | 7D | 7C |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 09 | FA | 73 | CF |  | 01 | 2D | 8F | 8A |  | 01 | 2D | 8F | 8A |  | 4F | 2B | 0E | 6C | XOR | 6E | 13 | 6F | 12 | = |
| 28 | 9A | 79 | 5E | 34 | B8 | B6 | 58 | B8 | B6 | 58 | 34 | A3 | E9 | E8 | DD | 6D | 11 | 6C | 10 |
| 43 | 52 | C5 | F0 | 1A | 00 | A6 | 8C | A6 | 8C | 1A | 00 | A6 | DC | F3 | FF | 6D | 11 | 6C | 10 |
| 6D | 69 | 25 | 76 | 3C | F9 | 3F | 38 | 38 | 3C | F9 | 3F | 6D | 35 | 21 | CF | 82 | FE | 83 | FF |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3 | 21 | 38 | 61 | 7E |  | FD | 07 | EF | F3 |  | FD | 07 | EF | F3 |  | FD | EF | 19 | FC | XOR | A0 | B3 | DC | CE | = |
| CE | F8 | 84 | CD | 8B | 41 | 5F | BD | 41 | 5F | BD | 8B | 0D | 1C | B0 | 18 | A7 | B6 | DA | CA |
| CB | CD | 9F | EF | 1F | BD | DB | DF | DB | DF | 1F | BD | 1D | 87 | 4D | 57 | 7B | 6A | 06 | 16 |
| EF | CB | A2 | 30 | DF | 1F | 3A | 04 | 04 | DF | 1F | 3A | 8E | 2C | B6 | 4C | 4B | B5 | 36 | C9 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 5D | 5C | C5 | 32 |  | 4C | 4A | A6 | 23 |  | 4C | 4A | A6 | 23 |  | 53 | B7 | 4E | 31 | XOR | DC | 6F | B3 | 7B | = |
| AA | AA | 6A | D2 | AC | AC | 02 | B5 | AC | 02 | B5 | AC | 56 | 76 | 6C | 52 | E0 | 56 | 8C | 46 |
| 66 | ED | 4B | 41 | 33 | 55 | B3 | 83 | B3 | 83 | 33 | 55 | 3F | A4 | 5C | 69 | A6 | CC | CA | DC |
| C5 | 99 | 80 | 85 | A6 | EE | CD | 97 | 97 | A6 | EE | CD | FE | 08 | B0 | 1D | C0 | 75 | 43 | 8A |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | 8F | D8 | FD | 4C |  | 73 | 61 | 54 | 29 |  | 73 | 61 | 54 | 29 |  | 3C | 9D | AC | C8 | XOR | 96 | F9 | 4A | 37 | = |
| B6 | 20 | E0 | 14 | 4E | B7 | E1 | FA | B7 | E1 | FA | 4E | 25 | 6E | 6D | 77 | 66 | 30 | BC | FA |
| 99 | 68 | 96 | B5 | EE | 45 | 90 | D5 | 90 | D5 | EE | 45 | 7C | FC | 73 | FA | D8 | 14 | DE | 02 |
| 3E | 7D | F3 | 97 | B2 | FF | 0D | 88 | 88 | B2 | FF | 0D | B9 | E8 | 0D | 6A | 3F | 4A | 09 | 83 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | AA | 64 | E6 | FF |  | AC | 43 | 8E | 16 |  | AC | 43 | 8E | 16 |  | 20 | C1 | 93 | 6B | XOR | 9b | 62 | 28 | 1f | = |
| 43 | 5E | D1 | 8D | 1A | 58 | 3E | 5D | 58 | 3E | 5D | 1A | A6 | B8 | D5 | 66 | 11 | 21 | 9d | 67 |
| A4 | E8 | AD | F8 | 49 | 9B | 95 | 41 | 95 | 41 | 49 | 9B | E7 | 33 | 0F | 2C | 34 | 20 | fe | fc |
| 86 | A2 | 04 | E9 | 44 | 3A | F2 | 1E | 1E | 44 | 3A | F2 | 1E | 32 | E9 | 44 | a5 | ef | e6 | 65 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | BB | A3 | BB | 74 |  | EA | 0A | EA | 92 |  | EA | 0A | EA | 92 |  | BA | 78 | EC | D4 | XOR | 5e | 3c | 14 | 0b | = |
| B7 | 99 | 48 | 01 | A9 | Ê | 52 | 7C | EE | 52 | 7C | A9 | 28 | D4 | 79 | 2A | a1 | 80 | 1d | 7a |
| D3 | 13 | F1 | D0 | 66 | 7D | A1 | 70 | A1 | 70 | 66 | 7D | 41 | 9D | 02 | 5B | 79 | 59 | a7 | 5b |
| BB | DD | 0F | 21 | EA | C1 | 76 | FD | FD | EA | C1 | 76 | 8B | F3 | A6 | 95 | 65 | 8a | 6c | 09 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | E4 | 44 | F8 | DF |  | 69 | 1B | 41 | 9E |  | 69 | 1B | 41 | 9E |  | 6A | B8 | C6 | BD | XOR | 04 | 38 | 2c | 27 | = |
| 89 | 54 | 64 | 50 | 7A | 20 | 43 | 53 | 20 | 43 | 53 | A7 | FD | 10 | 58 | 9B | 98 | 18 | 05 | 7f |
| 38 | C4 | A5 | 00 | 07 | 1C | 06 | 63 | 06 | 63 | 07 | 1C | 3C | E6 | DD | 9D | 78 | 21 | 86 | dd |
| EE | 79 | CA | 9C | 28 | B6 | 74 | DE | DE | 28 | B6 | 74 | 3A | 5D | E0 | EA | 4e | c4 | a8 | a1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9 | 6E | 80 | EA | 9A |  | 9F | CD | 87 | B8 |  | 9F | CD | 87 | B8 |  | FF | CE | 5B | 28 | XOR | cd | f5 | d9 | fe | = |
| 65 | 08 | 5D | E4 | 4D | 30 | 4C | 69 | 30 | 4C | 69 | 4D | 07 | DC | 96 | 21 | 59 | 41 | 44 | 3b |
| 44 | C7 | 5B | 40 | 1B | C6 | 39 | 09 | 39 | 09 | 1B | C6 | 13 | 3E | F1 | 94 | 4a | 6b | ed | 30 |
| 74 | 99 | 48 | 4B | 92 | EE | 52 | B3 | B3 | 92 | EE | 52 | CE | 36 | 27 | FC | 82 | 46 | ee | 4f |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 32 | 3B | 82 | D6 |  | 23 | E2 | 13 | F6 |  | 23 | E2 | 13 | F6 |  |  |  |  |  | XOR | 19 | ec | 35 | cb | = |
| 5E | 9D | D2 | 1A | 58 | 5E | B5 | A2 | 5E | B5 | A2 | 58 |  |  |  |  | 5d | 1c | 58 | 63 |
| 59 | 55 | 1C | A4 | CB | FC | 9C | 49 | 9C | 49 | CB | FC |  |  |  |  | ce | a5 | 48 | 78 |
| 4C | 70 | C9 | B3 | 29 | 51 | DD | 6D | 6D | 29 | 51 | DD |  |  |  |  | 39 | 7f | 91 | de |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11 | 3A | 0E | 26 | 3D |
| 03 | A9 | FA | 3B |
| 52 | EC | 83 | 84 |
| 54 | 56 | C0 | 03 |