

Block Message[1] running... [Two One Nine Two]

Plaintext :

[["54", "4f", "4e", "20"], ["77", "6e", "69", "54"], ["6f", "65", "6e", "77"], ["20", "20", "65", "6f"]]

Key :

[84, 104, 97, 116, 115, 32, 109, 121, 32, 75, 117, 110, 103, 32, 70, 117]

EXPANDED-KEY :

[84, 104, 97, 116], [115, 32, 109, 121], [32, 75, 117, 110], [103, 32, 70, 117], [226, 50, 252, 241], [145, 18, 145, 136], [177, 89, 228, 230], [214, 121, 162, 147], [86, 8, 32, 7], [199, 26, 177, 143], [118, 67, 85, 105], [160, 58, 247, 250], [210, 96, 13, 231], [21, 122, 188, 104], [99, 57, 233, 1], [195, 3, 30, 251], [161, 18, 2, 201], [180, 104, 190, 161], [215, 81, 87, 160], [20, 82, 73, 91], [177, 41, 59, 51], [5, 65, 133, 146], [210, 16, 210, 50], [198, 66, 155, 105], [189, 61, 194, 135], [184, 124, 71, 21], [106, 108, 149, 39], [172, 46, 14, 78], [204, 150, 237, 22], [116, 234, 170, 3], [30, 134, 63, 36], [178, 168, 49, 106], [142, 81, 239, 33], [250, 187, 69, 34], [228, 61, 122, 6], [86, 149, 75, 108], [191, 226, 191, 144], [69, 89, 250, 178], [161, 100, 128, 180], [247, 241, 203, 216], [40, 253, 222, 248], [109, 164, 36, 74], [204, 192, 164, 254], [59, 49, 111, 38]]

#=====#
#=====ROUND-#

KEY=====#

STATE- 0[0][0] : $84 \oplus 84 = 0$ | [0][1] : $79 \oplus 115 = 60$ | [0][2] : $78 \oplus 32 = 110$ | [0][3] : $32 \oplus 103 = 71$ |

STATE- 1[1][0] : $119 \oplus 104 = 31$ | [1][1] : $110 \oplus 32 = 78$ | [1][2] : $105 \oplus 75 = 34$ | [1][3] : $84 \oplus 32 = 116$ |

STATE- 2[2][0] : $111 \oplus 97 = 14$ | [2][1] : $101 \oplus 109 = 8$ | [2][2] : $110 \oplus 117 = 27$ | [2][3] : $119 \oplus 70 = 49$ |

STATE- 3[3][0] : $32 \oplus 116 = 84$ | [3][1] : $32 \oplus 121 = 89$ | [3][2] : $101 \oplus 110 = 11$ | [3][3] : $111 \oplus 117 = 26$ |

S[ADDROUNDKEY] :

[0, 60, 110, 71], [31, 78, 34, 116], [14, 8, 27, 49], [84, 89, 11, 26]]

S[ADDROUNDKEY] :

[["0", "3c", "6e", "47"], ["1f", "4e", "22", "74"], ["e", "8", "1b", "31"], ["54", "59", "b", "1a"]]

#=====#
S[SUB_BYTES]-1 :

[99, 235, 159, 160], [192, 47, 147, 146], [171, 48, 175, 199], [32, 203, 43, 162]]

S[SUB_BYTES]-1 :

[["63", "eb", "9f", "a0"], ["c0", "2f", "93", "92"], ["ab", "30", "af", "c7"], ["20", "cb", "2b", "a2"]]

S[SHIFT_ROWS]-1 :

[99, 235, 159, 160], [47, 147, 146, 192], [175, 199, 171, 48], [162, 32, 203, 43]]

S[SHIFT_ROWS]-1 :

[["63", "eb", "9f", "a0"], ["2f", "93", "92", "c0"], ["af", "c7", "ab", "30"], ["a2", "20", "cb", "2b"]]

S[MIX_COLUMN]-1 :

[186, 132, 232, 27], [117, 164, 141, 64], [244, 141, 6, 125], [122, 50, 14, 93]]

S[MIX_COLUMN]-1 :

[["ba", "84", "e8", "1b"], ["75", "a4", "8d", "40"], ["f4", "8d", "6", "7d"], ["7a", "32", "e", "5d"]]

STATE- 0[0][0] : $186 \oplus 226 = 88$ | [0][1] : $132 \oplus 145 = 21$ | [0][2] : $232 \oplus 177 = 89$ | [0][3] : $27 \oplus 214 = 205$ |

STATE- 1[1][0] : $117 \oplus 50 = 71$ | [1][1] : $164 \oplus 18 = 182$ | [1][2] : $141 \oplus 89 = 212$ | [1][3] : $64 \oplus 121 = 57$ |

STATE- 2[2][0] : $244 \oplus 252 = 8$ | [2][1] : $141 \oplus 145 = 28$ | [2][2] : $6 \oplus 228 = 226$ | [2][3] : $125 \oplus 162 = 223$ |

STATE- 3[3][0] : $122 \oplus 241 = 139$ | [3][1] : $50 \oplus 136 = 186$ | [3][2] : $14 \oplus 230 = 232$ | [3][3] : $93 \oplus 147 = 206$ |

S[ADDROUNDKEY]-1 :

[88, 21, 89, 205], [71, 182, 212, 57], [8, 28, 226, 223], [139, 186, 232, 206]]

S[ADDROUNDKEY]-1 :

[["58", "15", "59", "cd"], ["47", "b6", "d4", "39"], ["8", "1c", "e2", "df"], ["8b", "ba", "e8", "ce"]]

```
#=====#
S[SUB_BYTES]-2 :

[[106,89,203,189],[160,78,72,18],[48,156,152,158],[61,244,155,139]]

S[SUB_BYTES]-2 :

[["6a","59","cb","bd"],["a0","4e","48","12"],["30","9c","98","9e"],["3d","f4","9b","8b"]]

S[SHIFT_ROWS]-2 :

[[106,89,203,189],[78,72,18,160],[152,158,48,156],[139,61,244,155]]

S[SHIFT_ROWS]-2 :

[["6a","59","cb","bd"],["4e","48","12","a0"],["98","9e","30","9c"],["8b","3d","f4","9b"]]

S[MIX_COLUMN]-2 :

[[21,201,127,157],[206,77,75,194],[137,113,190,136],[101,71,151,205]]

S[MIX_COLUMN]-2 :

[["15","c9","7f","9d"],["ce","4d","4b","c2"],["89","71","be","88"],["65","47","97","cd"]]

STATE- 0[0][0]:21⊕86 = 67 | [0][1]:201⊕199 = 14 | [0][2]:127⊕118 = 9 | [0][3]:157⊕160 = 61 |
STATE- 1[1][0]:206⊕8 = 198 | [1][1]:77⊕26 = 87 | [1][2]:75⊕67 = 8 | [1][3]:194⊕58 = 248 |
STATE- 2[2][0]:137⊕32 = 169 | [2][1]:113⊕177 = 192 | [2][2]:190⊕85 = 235 | [2][3]:136⊕247 = 127 |
STATE- 3[3][0]:101⊕7 = 98 | [3][1]:71⊕143 = 200 | [3][2]:151⊕105 = 254 | [3][3]:205⊕250 = 55 |
S[ADDROUNDKEY]-2 :

[[67,14,9,61],[198,87,8,248],[169,192,235,127],[98,200,254,55]]

S[ADDROUNDKEY]-2 :

[["43","e","9","3d"],["c6","57","8","f8"],["a9","c0","eb","7f"],["62","c8","fe","37"]]

#=====#
S[SUB_BYTES]-3 :

[[26,171,1,39],[180,91,48,65],[211,186,233,210],[170,232,187,154]]

S[SUB_BYTES]-3 :

[["1a","ab","1","27"],["b4","5b","30","41"],["d3","ba","e9","d2"],["aa","e8","bb","9a"]]

S[SHIFT_ROWS]-3 :

[[26,171,1,39],[91,48,65,180],[233,210,211,186],[154,170,232,187]]

S[SHIFT_ROWS]-3 :

[["1a","ab","1","27"],["5b","30","41","b4"],["e9","d2","d3","ba"],["9a","aa","e8","bb"]]

S[MIX_COLUMN]-3 :

[[170,101,250,136],[22,12,5,58],[61,193,222,42],[179,75,90,10]]

S[MIX_COLUMN]-3 :

[["aa","65","fa","88"],["16","c","5","3a"],["3d","c1","de","2a"],["b3","4b","5a","a"]]

STATE- 0[0][0]:170⊕210 = 120 | [0][1]:101⊕21 = 112 | [0][2]:250⊕99 = 153 | [0][3]:136⊕195 = 75 |
STATE- 1[1][0]:22⊕96 = 118 | [1][1]:12⊕122 = 118 | [1][2]:5⊕57 = 60 | [1][3]:58⊕3 = 57 |
STATE- 2[2][0]:61⊕13 = 48 | [2][1]:193⊕188 = 125 | [2][2]:222⊕233 = 55 | [2][3]:42⊕30 = 52 |
STATE- 3[3][0]:179⊕231 = 84 | [3][1]:75⊕104 = 35 | [3][2]:90⊕1 = 91 | [3][3]:10⊕251 = 241 |
S[ADDROUNDKEY]-3 :

[[120,112,153,75],[118,118,60,57],[48,125,55,52],[84,35,91,241]]
```

S[ADDDROUNDKEY]-3 :

[["78", "70", "99", "4b"], ["76", "76", "3c", "39"], ["30", "7d", "37", "34"], ["54", "23", "5b", "f1"]]

#=====

S[SUB_BYTES]-4 :

[["188", "81", "238", "179"], ["56", "56", "235", "18"], ["4", "255", "154", "24"], ["32", "38", "57", "161"]]

S[SUB_BYTES]-4 :

[["bc", "51", "ee", "b3"], ["38", "38", "eb", "12"], ["4", "ff", "9a", "18"], ["20", "26", "39", "a1"]]

S[SHIFT_ROWS]-4 :

[["188", "81", "238", "179"], ["56", "235", "18", "56"], ["154", "24", "4", "255"], ["161", "32", "38", "57"]]

S[SHIFT_ROWS]-4 :

[["bc", "51", "ee", "b3"], ["38", "eb", "12", "38"], ["9a", "18", "4", "ff"], ["a1", "20", "26", "39"]]

S[MIX_COLUMN]-4 :

[["16", "188", "211", "243"], ["216", "148", "224", "224"], ["83", "234", "158", "37"], ["36", "64", "115", "123"]]

S[MIX_COLUMN]-4 :

[["10", "bc", "d3", "f3"], ["d8", "94", "e0", "e0"], ["53", "ea", "9e", "25"], ["24", "40", "73", "7b"]]

STATE- 0[0][0] : $16 \oplus 161 = 177$ | 0[0][1] : $188 \oplus 180 = 8$ | 0[0][2] : $211 \oplus 215 = 4$ | 0[0][3] : $243 \oplus 20 = 231$ |
STATE- 1[1][0] : $216 \oplus 18 = 202$ | 1[1][1] : $148 \oplus 104 = 252$ | 1[1][2] : $224 \oplus 81 = 177$ | 1[1][3] : $224 \oplus 82 = 178$ |
STATE- 2[2][0] : $83 \oplus 2 = 81$ | 2[2][1] : $234 \oplus 190 = 84$ | 2[2][2] : $158 \oplus 87 = 201$ | 2[2][3] : $37 \oplus 73 = 108$ |
STATE- 3[3][0] : $36 \oplus 201 = 237$ | 3[3][1] : $64 \oplus 161 = 225$ | 3[3][2] : $115 \oplus 160 = 211$ | 3[3][3] : $123 \oplus 91 = 32$ |
S[ADDDROUNDKEY]-4 :

[["177", "8", "4", "231"], ["202", "252", "177", "178"], ["81", "84", "201", "108"], ["237", "225", "211", "32"]]

S[ADDDROUNDKEY]-4 :

[["b1", "8", "4", "e7"], ["ca", "fc", "b1", "b2"], ["51", "54", "c9", "6c"], ["ed", "e1", "d3", "20"]]

#=====

S[SUB_BYTES]-5 :

[["200", "48", "242", "148"], ["116", "176", "200", "55"], ["209", "32", "221", "80"], ["85", "248", "102", "183"]]

S[SUB_BYTES]-5 :

[["c8", "30", "f2", "94"], ["74", "b0", "c8", "37"], ["d1", "20", "dd", "50"], ["55", "f8", "66", "b7"]]

S[SHIFT_ROWS]-5 :

[["200", "48", "242", "148"], ["176", "200", "55", "116"], ["221", "80", "209", "32"], ["183", "85", "248", "102"]]

S[SHIFT_ROWS]-5 :

[["c8", "30", "f2", "94"], ["b0", "c8", "37", "74"], ["dd", "50", "d1", "20"], ["b7", "55", "f8", "66"]]

S[MIX_COLUMN]-5 :

[["42", "38", "143", "233"], ["120", "30", "12", "122"], ["27", "167", "111", "10"], ["91", "98", "0", "63"]]

S[MIX_COLUMN]-5 :

[["2a", "26", "8f", "e9"], ["78", "1e", "c", "7a"], ["1b", "a7", "6f", "a"], ["5b", "62", "0", "3f"]]

STATE- 0[0][0] : $42 \oplus 177 = 155$ | 0[0][1] : $38 \oplus 5 = 35$ | 0[0][2] : $143 \oplus 210 = 93$ | 0[0][3] : $233 \oplus 198 = 47$ |
STATE- 1[1][0] : $120 \oplus 41 = 81$ | 1[1][1] : $30 \oplus 65 = 95$ | 1[1][2] : $12 \oplus 16 = 28$ | 1[1][3] : $122 \oplus 66 = 56$ |

```
5/13/2021                                localhost:8000/coba

STATE- 2[2][0]:27⊕59 = 32 | [2][1]:167⊕133 = 34 | [2][2]:111⊕210 = 189 | [2][3]:10⊕155 = 145 |
STATE- 3[3][0]:91⊕51 = 104 | [3][1]:98⊕146 = 240 | [3][2]:0⊕50 = 50 | [3][3]:63⊕105 = 86 |
S[ADDDROUNDKEY]-5 :

[[155,35,93,47],[81,95,28,56],[32,34,189,145],[104,240,50,86]]

S[ADDDROUNDKEY]-5 :

[["9b","23","5d","2f"],["51","5f","1c","38"],["20","22","bd","91"],["68","f0","32","56"]]

#=====#
S[SUB_BYTES]-6 :

[[20,38,76,21],[209,207,156,7],[183,147,122,129],[69,140,35,177]]

S[SUB_BYTES]-6 :

[["14","26","4c","15"],["d1","cf","9c","7"],["b7","93","7a","81"],["45","8c","23","b1"]]

S[SHIFT_ROWS]-6 :

[[20,38,76,21],[207,156,7,209],[122,129,183,147],[177,69,140,35]]

S[SHIFT_ROWS]-6 :

[["14","26","4c","15"],["cf","9c","7","d1"],["7a","81","b7","93"],["b1","45","8c","23"]]

S[MIX_COLUMN]-6 :

[[169,55,170,242],[174,216,12,33],[231,108,177,156],[240,253,103,59]]

S[MIX_COLUMN]-6 :

[["a9","37","aa","f2"],["ae","d8","c","21"],["e7","6c","b1","9c"],["f0","fd","67","3b"]]

STATE- 0[0][0]:169⊕189 = 20 | [0][1]:55⊕184 = 143 | [0][2]:170⊕106 = 192 | [0][3]:242⊕172 = 94 |
STATE- 1[1][0]:174⊕61 = 147 | [1][1]:216⊕124 = 164 | [1][2]:12⊕108 = 96 | [1][3]:33⊕46 = 15 |
STATE- 2[2][0]:231⊕194 = 37 | [2][1]:108⊕71 = 43 | [2][2]:177⊕149 = 36 | [2][3]:156⊕14 = 146 |
STATE- 3[3][0]:240⊕135 = 119 | [3][1]:253⊕21 = 232 | [3][2]:103⊕39 = 64 | [3][3]:59⊕78 = 117 |
S[ADDDROUNDKEY]-6 :

[[20,143,192,94],[147,164,96,15],[37,43,36,146],[119,232,64,117]]

S[ADDDROUNDKEY]-6 :

[["14","8f","c0","5e"],["93","a4","60","f"],["25","2b","24","92"],["77","e8","40","75"]]

#=====#
S[SUB_BYTES]-7 :

[[250,115,186,88],[220,73,208,118],[63,241,54,79],[245,155,9,157]]

S[SUB_BYTES]-7 :

[["fa","73","ba","58"],["dc","49","d0","76"],["3f","f1","36","4f"],["f5","9b","9","9d"]]

S[SHIFT_ROWS]-7 :

[[250,115,186,88],[73,208,118,220],[54,79,63,241],[157,245,155,9]]

S[SHIFT_ROWS]-7 :

[["fa","73","ba","58"],["49","d0","76","dc"],["36","4f","3f","f1"],["9d","f5","9b","9"]]

S[MIX_COLUMN]-7 :

[[159,55,81,55],[175,236,140,250],[99,57,4,102],[75,251,177,215]]

S[MIX_COLUMN]-7 :
```

5/13/2021localhost:8000/coba

[[{"9f","37","51","37"},{"af","ec","8c","fa"},{"63","39","4","66"},{"4b","fb","b1","d7"}]]

STATE- 0[0][0]:159⊕204 = 83 | 0[0][1]:55⊕116 = 67 | 0[0][2]:81⊕30 = 79 | 0[0][3]:55⊕178 = 133 |
STATE- 1[1][0]:175⊕150 = 57 | 1[1][1]:236⊕234 = 6 | 1[1][2]:140⊕134 = 10 | 1[1][3]:250⊕168 = 82 |
STATE- 2[2][0]:99⊕237 = 142 | 2[2][1]:57⊕170 = 147 | 2[2][2]:4⊕63 = 59 | 2[2][3]:102⊕49 = 87 |
STATE- 3[3][0]:75⊕22 = 93 | 3[3][1]:251⊕3 = 248 | 3[3][2]:177⊕36 = 149 | 3[3][3]:215⊕106 = 189 |
S[ADDDROUNDKEY]-7 :

[[83,67,79,133],[57,6,10,82],[142,147,59,87],[93,248,149,189]]

S[ADDDROUNDKEY]-7 :

[[{"53","43","4f","85"},{"39","6","a","52"},{"8e","93","3b","57"},{"5d","f8","95","bd"}]]

#=====

S[SUB_BYTES]-8 :

[[237,26,132,151],[18,111,103,0],[25,220,226,91],[76,65,42,122]]

S[SUB_BYTES]-8 :

[[{"ed","1a","84","97"},{"12","6f","67","0"},{"19","dc","e2","5b"},{"4c","41","2a","7a"}]]

S[SHIFT_ROWS]-8 :

[[237,26,132,151],[111,103,0,18],[226,91,25,220],[122,76,65,42]]

S[SHIFT_ROWS]-8 :

[[{"ed","1a","84","97"},{"6f","67","0","12"},{"e2","5b","19","dc"},{"7a","4c","41","2a"}]]

S[MIX_COLUMN]-8 :

[[232,138,75,245],[116,117,238,230],[211,31,117,88],[85,138,12,56]]

S[MIX_COLUMN]-8 :

[[{"e8","8a","4b","f5"},{"74","75","ee","e6"},{"d3","1f","75","58"},{"55","8a","c","38"}]]

STATE- 0[0][0]:232⊕142 = 102 | 0[0][1]:138⊕250 = 112 | 0[0][2]:75⊕228 = 175 | 0[0][3]:245⊕86 = 163 |
STATE- 1[1][0]:116⊕81 = 37 | 1[1][1]:117⊕187 = 206 | 1[1][2]:238⊕61 = 211 | 1[1][3]:230⊕149 = 115 |
STATE- 2[2][0]:211⊕239 = 60 | 2[2][1]:31⊕69 = 90 | 2[2][2]:117⊕122 = 15 | 2[2][3]:88⊕75 = 19 |
STATE- 3[3][0]:85⊕33 = 116 | 3[3][1]:138⊕34 = 168 | 3[3][2]:12⊕6 = 10 | 3[3][3]:56⊕108 = 84 |
S[ADDDROUNDKEY]-8 :

[[102,112,175,163],[37,206,211,115],[60,90,15,19],[116,168,10,84]]

S[ADDDROUNDKEY]-8 :

[[{"66","70","af","a3"},{"25","ce","d3","73"},{"3c","5a","f","13"},{"74","a8","a","54"}]]

#=====

S[SUB_BYTES]-9 :

[[51,81,121,10],[63,139,102,143],[235,190,118,125],[146,194,103,32]]

S[SUB_BYTES]-9 :

[[{"33","51","79","a"},{"3f","8b","66","8f"},{"eb","be","76","7d"},{"92","c2","67","20"}]]

S[SHIFT_ROWS]-9 :

[[51,81,121,10],[139,102,143,63],[118,125,235,190],[32,146,194,103]]

S[SHIFT_ROWS]-9 :

[[{"33","51","79","a"},{"8b","66","8f","3f"},{"76","7d","eb","be"},{"20","92","c2","67"}]]

S[MIX_COLUMN]-9 :

localhost:8000/coba

5/12

```
5/13/2021                                localhost:8000/coba

[[182,231,81,140],[132,136,152,202],[52,96,102,251],[232,215,112,81]]

S[MIX_COLUMN]-9 :

[["b6","e7","51","8c"],["84","88","98","ca"],["34","60","66","fb"],["e8","d7","70","51"]]

STATE- 0[0][0]:182⊕191 = 9 | [0][1]:231⊕69 = 162 | [0][2]:81⊕161 = 240 | [0][3]:140⊕247 = 123 |
STATE- 1[1][0]:132⊕226 = 102 | [1][1]:136⊕89 = 209 | [1][2]:152⊕100 = 252 | [1][3]:202⊕241 = 59 |
STATE- 2[2][0]:52⊕191 = 139 | [2][1]:96⊕250 = 154 | [2][2]:102⊕128 = 230 | [2][3]:251⊕203 = 48 |
STATE- 3[3][0]:232⊕144 = 120 | [3][1]:215⊕178 = 101 | [3][2]:112⊕180 = 196 | [3][3]:81⊕216 = 137 |
S[ADDROUNDKEY]-9 :

[[9,162,240,123],[102,209,252,59],[139,154,230,48],[120,101,196,137]]

S[ADDROUNDKEY]-9 :

[["9","a2","f0","7b"],["66","d1","fc","3b"],["8b","9a","e6","30"],["78","65","c4","89"]]

#=====#
S[SUB_BYTES]-10 :

[[1,58,140,33],[51,62,176,226],[61,184,142,4],[188,77,28,167]]

S[SUB_BYTES]-10 :

[["1","3a","8c","21"],["33","3e","b0","e2"],["3d","b8","8e","4"],["bc","4d","1c","a7"]]

S[SHIFT_ROWS]-10 :

[[1,58,140,33],[62,176,226,51],[142,4,61,184],[167,188,77,28]]

S[SHIFT_ROWS]-10 :

[["1","3a","8c","21"],["3e","b0","e2","33"],["8e","4","3d","b8"],["a7","bc","4d","1c"]]

STATE- 0[0][0]:1⊕40 = 41 | [0][1]:58⊕109 = 87 | [0][2]:140⊕204 = 64 | [0][3]:33⊕59 = 26 |
STATE- 1[1][0]:62⊕253 = 195 | [1][1]:176⊕164 = 20 | [1][2]:226⊕192 = 34 | [1][3]:51⊕49 = 2 |
STATE- 2[2][0]:142⊕222 = 80 | [2][1]:4⊕36 = 32 | [2][2]:61⊕164 = 153 | [2][3]:184⊕111 = 215 |
STATE- 3[3][0]:167⊕248 = 95 | [3][1]:188⊕74 = 246 | [3][2]:77⊕254 = 179 | [3][3]:28⊕38 = 58 |
S[ADDROUNDKEY]-10 :

[[41,87,64,26],[195,20,34,2],[80,32,153,215],[95,246,179,58]]

S[ADDROUNDKEY]-10 :

[["29","57","40","1a"],["c3","14","22","2"],["50","20","99","d7"],["5f","f6","b3","3a"]]

#=====#
Block Message[2] running... [□□□□□□□□□□□□□□□□]
Plaintext :

[["10","10","10","10"],["10","10","10","10"],["10","10","10","10"],["10","10","10","10"]]

Key :

[84,104,97,116,115,32,109,121,32,75,117,110,103,32,70,117]

EXPANDED-KEY :

[[84,104,97,116],[115,32,109,121],[32,75,117,110],[103,32,70,117],[226,50,252,241],[145,18,145,136],[177,89,228,230],[214,121,162,147],
[86,8,32,7],[199,26,177,143],[118,67,85,105],[160,58,247,250],[210,96,13,231],[21,122,188,104],[99,57,233,1],[195,3,30,251],[161,18,2,201],
[180,104,190,161],[215,81,87,160],[20,82,73,91],[177,41,59,51],[5,65,133,146],[210,16,210,50],[198,66,155,105],[189,61,194,135],
[184,124,71,21],[106,108,149,39],[172,46,14,78],[204,150,237,22],[116,234,170,3],[30,134,63,36],[178,168,49,106],[142,81,239,33],
[250,187,69,34],[228,61,122,6],[86,149,75,108],[191,226,191,144],[69,89,250,178],[161,100,128,180],[247,241,203,216],[40,253,222,248],
[109,164,36,74],[204,192,164,254],[59,49,111,38]]

#=====#
#=====ROUND-#
KEY=====#
STATE- 0[0][0]:16⊕84 = 68 | [0][1]:16⊕115 = 99 | [0][2]:16⊕32 = 48 | [0][3]:16⊕103 = 119 |
```

STATE- 1[1][0]: $16 \oplus 104 = 120$ | [1][1]: $16 \oplus 32 = 48$ | [1][2]: $16 \oplus 75 = 91$ | [1][3]: $16 \oplus 32 = 48$ |
STATE- 2[2][0]: $16 \oplus 97 = 113$ | [2][1]: $16 \oplus 109 = 125$ | [2][2]: $16 \oplus 117 = 101$ | [2][3]: $16 \oplus 70 = 86$ |
STATE- 3[3][0]: $16 \oplus 116 = 100$ | [3][1]: $16 \oplus 121 = 105$ | [3][2]: $16 \oplus 110 = 126$ | [3][3]: $16 \oplus 117 = 101$ |
S[ADDROUNDKEY] :

[[68,99,48,119], [120,48,91,48], [113,125,101,86], [100,105,126,101]]

S[ADDROUNDKEY] :

[["44", "63", "30", "77"], ["78", "30", "5b", "30"], ["71", "7d", "65", "56"], ["64", "69", "7e", "65"]]

#=====

S[SUB_BYTES]-1 :

[[27,251,4,245], [188,4,57,4], [163,255,77,177], [67,249,243,77]]

S[SUB_BYTES]-1 :

[["1b", "fb", "4", "f5"], ["bc", "4", "39", "4"], ["a3", "ff", "4d", "b1"], ["43", "f9", "f3", "4d"]]

S[SHIFT_ROWS]-1 :

[[27,251,4,245], [4,57,4,188], [77,177,163,255], [77,67,249,243]]

S[SHIFT_ROWS]-1 :

[["1b", "fb", "4", "f5"], ["4", "39", "4", "bc"], ["4d", "b1", "a3", "ff"], ["4d", "43", "f9", "f3"]]

S[MIX_COLUMN]-1 :

[[58,84,94,34], [137,2,11,127], [82,126,77,162], [254,24,66,186]]

S[MIX_COLUMN]-1 :

[["3a", "54", "5e", "22"], ["89", "2", "b", "7f"], ["52", "7e", "4d", "a2"], ["fe", "18", "42", "ba"]]

STATE- 0[0][0]: $58 \oplus 226 = 216$ | [0][1]: $84 \oplus 145 = 197$ | [0][2]: $94 \oplus 177 = 239$ | [0][3]: $34 \oplus 214 = 244$ |
STATE- 1[1][0]: $137 \oplus 50 = 187$ | [1][1]: $2 \oplus 18 = 16$ | [1][2]: $11 \oplus 89 = 82$ | [1][3]: $127 \oplus 121 = 6$ |
STATE- 2[2][0]: $82 \oplus 252 = 174$ | [2][1]: $126 \oplus 145 = 239$ | [2][2]: $77 \oplus 228 = 169$ | [2][3]: $162 \oplus 162 = 0$ |
STATE- 3[3][0]: $254 \oplus 241 = 15$ | [3][1]: $24 \oplus 136 = 144$ | [3][2]: $66 \oplus 230 = 164$ | [3][3]: $186 \oplus 147 = 41$ |
S[ADDROUNDKEY]-1 :

[[216,197,239,244], [187,16,82,6], [174,239,169,0], [15,144,164,41]]

S[ADDROUNDKEY]-1 :

[["d8", "c5", "ef", "f4"], ["bb", "10", "52", "6"], ["ae", "ef", "a9", "0"], ["f", "90", "a4", "29"]]

#=====

S[SUB_BYTES]-2 :

[[97,166,223,191], [234,202,0,111], [228,223,211,99], [118,96,73,165]]

S[SUB_BYTES]-2 :

[["61", "a6", "df", "bf"], ["ea", "ca", "0", "6f"], ["e4", "df", "d3", "63"], ["76", "60", "49", "a5"]]

S[SHIFT_ROWS]-2 :

[[97,166,223,191], [202,0,111,234], [211,99,228,223], [165,118,96,73]]

S[SHIFT_ROWS]-2 :

[["61", "a6", "df", "bf"], ["ca", "0", "6f", "ea"], ["d3", "63", "e4", "df"], ["a5", "76", "60", "49"]]

S[MIX_COLUMN]-2 :

[[241,66,144,214], [37,117,86,67], [226,250,195,43], [235,126,49,125]]

S[MIX_COLUMN]-2 :

[["f1", "42", "90", "d6"], ["25", "75", "56", "43"], ["e2", "fa", "c3", "2b"], ["eb", "7e", "31", "7d"]]

STATE- 0[0][0]: $241 \oplus 86 = 167$ | 0[0][1]: $66 \oplus 199 = 133$ | 0[0][2]: $144 \oplus 118 = 230$ | 0[0][3]: $214 \oplus 160 = 118$ |
STATE- 1[1][0]: $37 \oplus 8 = 45$ | 1[1][1]: $117 \oplus 26 = 111$ | 1[1][2]: $86 \oplus 67 = 21$ | 1[1][3]: $67 \oplus 58 = 121$ |
STATE- 2[2][0]: $226 \oplus 32 = 194$ | 2[2][1]: $250 \oplus 177 = 75$ | 2[2][2]: $195 \oplus 85 = 150$ | 2[2][3]: $43 \oplus 247 = 220$ |
STATE- 3[3][0]: $235 \oplus 7 = 236$ | 3[3][1]: $126 \oplus 143 = 241$ | 3[3][2]: $49 \oplus 105 = 88$ | 3[3][3]: $125 \oplus 250 = 135$ |
S[ADDDROUNDKEY]-2 :

[167,133,230,118],[45,111,21,121],[194,75,150,220],[236,241,88,135]]

S[ADDDROUNDKEY]-2 :

[["a7", "85", "e6", "76"], ["2d", "6f", "15", "79"], ["c2", "4b", "96", "dc"], ["ec", "f1", "58", "87"]]

#=====

S[SUB_BYTES]-3 :

[92,151,142,56],[216,168,89,182],[37,179,144,134],[206,161,106,23]]

S[SUB_BYTES]-3 :

[["5c", "97", "8e", "38"], ["d8", "a8", "59", "b6"], ["25", "b3", "90", "86"], ["ce", "a1", "6a", "17"]]

S[SHIFT_ROWS]-3 :

[92,151,142,56],[168,89,182,216],[144,134,37,179],[23,206,161,106]]

S[SHIFT_ROWS]-3 :

[["5c", "97", "8e", "38"], ["a8", "59", "b6", "d8"], ["90", "86", "25", "b3"], ["17", "ce", "a1", "6a"]]

S[MIX_COLUMN]-3 :

[220,150,66,218],[171,122,55,55],[246,144,138,35],[242,250,67,247]]

S[MIX_COLUMN]-3 :

[["dc", "96", "42", "da"], ["ab", "7a", "37", "37"], ["f6", "90", "8a", "23"], ["f2", "fa", "43", "f7"]]

STATE- 0[0][0]: $220 \oplus 210 = 14$ | 0[0][1]: $150 \oplus 21 = 131$ | 0[0][2]: $66 \oplus 99 = 33$ | 0[0][3]: $218 \oplus 195 = 25$ |
STATE- 1[1][0]: $171 \oplus 96 = 203$ | 1[1][1]: $122 \oplus 122 = 0$ | 1[1][2]: $55 \oplus 57 = 14$ | 1[1][3]: $55 \oplus 3 = 52$ |
STATE- 2[2][0]: $246 \oplus 13 = 251$ | 2[2][1]: $144 \oplus 188 = 44$ | 2[2][2]: $138 \oplus 233 = 99$ | 2[2][3]: $35 \oplus 30 = 61$ |
STATE- 3[3][0]: $242 \oplus 231 = 21$ | 3[3][1]: $250 \oplus 104 = 146$ | 3[3][2]: $67 \oplus 1 = 66$ | 3[3][3]: $247 \oplus 251 = 12$ |
S[ADDDROUNDKEY]-3 :

[14,131,33,25],[203,0,14,52],[251,44,99,61],[21,146,66,12]]

S[ADDDROUNDKEY]-3 :

[["e", "83", "21", "19"], ["cb", "0", "e", "34"], ["fb", "2c", "63", "3d"], ["15", "92", "42", "c"]]

#=====

S[SUB_BYTES]-4 :

[171,236,253,212],[31,99,171,24],[15,113,251,39],[89,79,44,254]]

S[SUB_BYTES]-4 :

[["ab", "ec", "fd", "d4"], ["1f", "63", "ab", "18"], ["f", "71", "fb", "27"], ["59", "4f", "2c", "fe"]]

S[SHIFT_ROWS]-4 :

[171,236,253,212],[99,171,24,31],[251,39,15,113],[254,89,79,44]]

S[SHIFT_ROWS]-4 :

[["ab", "ec", "fd", "d4"], ["63", "ab", "18", "1f"], ["fb", "27", "f", "71"], ["fe", "59", "4f", "2c"]]

S[MIX_COLUMN]-4 :

[[237,91,137,207], [133,145,147,85], [60,226,42,93], [153,17,149,81]]

S[MIX_COLUMN]-4 :

[["ed", "5b", "89", "cf"], ["85", "91", "93", "55"], ["3c", "e2", "2a", "5d"], ["99", "11", "95", "51"]]

STATE- 0[0][0]: $237 \oplus 161 = 76$ | [0][1]: $91 \oplus 180 = 239$ | [0][2]: $137 \oplus 215 = 94$ | [0][3]: $207 \oplus 20 = 219$ |

STATE- 1[1][0]: $133 \oplus 18 = 151$ | [1][1]: $145 \oplus 104 = 249$ | [1][2]: $147 \oplus 81 = 194$ | [1][3]: $85 \oplus 82 = 7$ |

STATE- 2[2][0]: $60 \oplus 2 = 62$ | [2][1]: $226 \oplus 190 = 92$ | [2][2]: $42 \oplus 87 = 125$ | [2][3]: $93 \oplus 73 = 20$ |

STATE- 3[3][0]: $153 \oplus 201 = 80$ | [3][1]: $17 \oplus 161 = 176$ | [3][2]: $149 \oplus 160 = 53$ | [3][3]: $81 \oplus 91 = 10$ |

S[ADDROUNDKEY]-4 :

[[76,239,94,219], [151,249,194,7], [62,92,125,20], [80,176,53,10]]

S[ADDROUNDKEY]-4 :

[["4c", "ef", "5e", "db"], ["97", "f9", "c2", "7"], ["3e", "5c", "7d", "14"], ["50", "b0", "35", "a"]]

#=====

S[SUB_BYTES]-5 :

[[41,223,88,185], [136,153,37,197], [178,74,255,250], [83,231,150,103]]

S[SUB_BYTES]-5 :

[["29", "df", "58", "b9"], ["88", "99", "25", "c5"], ["b2", "4a", "ff", "fa"], ["53", "e7", "96", "67"]]

S[SHIFT_ROWS]-5 :

[[41,223,88,185], [153,37,197,136], [255,250,178,74], [103,83,231,150]]

S[SHIFT_ROWS]-5 :

[["29", "df", "58", "b9"], ["99", "25", "c5", "88"], ["ff", "fa", "b2", "4a"], ["67", "53", "e7", "96"]]

S[MIX_COLUMN]-5 :

[[122,99,177,54], [125,211,227,250], [252,224,208,4], [211,3,74,37]]

S[MIX_COLUMN]-5 :

[["7a", "63", "b1", "36"], ["7d", "d3", "e3", "fa"], ["fc", "e0", "d0", "4"], ["d3", "3", "4a", "25"]]

STATE- 0[0][0]: $122 \oplus 177 = 203$ | [0][1]: $99 \oplus 5 = 102$ | [0][2]: $177 \oplus 210 = 99$ | [0][3]: $54 \oplus 198 = 240$ |

STATE- 1[1][0]: $125 \oplus 41 = 84$ | [1][1]: $211 \oplus 65 = 146$ | [1][2]: $227 \oplus 16 = 243$ | [1][3]: $250 \oplus 66 = 184$ |

STATE- 2[2][0]: $252 \oplus 59 = 199$ | [2][1]: $224 \oplus 133 = 101$ | [2][2]: $208 \oplus 210 = 2$ | [2][3]: $4 \oplus 155 = 159$ |

STATE- 3[3][0]: $211 \oplus 51 = 224$ | [3][1]: $3 \oplus 146 = 145$ | [3][2]: $74 \oplus 50 = 120$ | [3][3]: $37 \oplus 105 = 76$ |

S[ADDROUNDKEY]-5 :

[[203,102,99,240], [84,146,243,184], [199,101,2,159], [224,145,120,76]]

S[ADDROUNDKEY]-5 :

[["cb", "66", "63", "f0"], ["54", "92", "f3", "b8"], ["c7", "65", "2", "9f"], ["e0", "91", "78", "4c"]]

#=====

S[SUB_BYTES]-6 :

[[31,51,251,140], [32,79,13,108], [198,77,119,219], [225,129,188,41]]

S[SUB_BYTES]-6 :

[["1f", "33", "fb", "8c"], ["20", "4f", "d", "6c"], ["c6", "4d", "77", "db"], ["e1", "81", "bc", "29"]]

S[SHIFT_ROWS]-6 :

[[31,51,251,140], [79,13,108,32], [119,219,198,77], [41,225,129,188]]

S[SHIFT_ROWS]-6 :

[["1f", "33", "fb", "8c"], ["4f", "d", "6c", "20"], ["77", "db", "c6", "4d"], ["29", "e1", "81", "bc"]]

S[MIX_COLUMN]-6 :

[177, 75, 30, 146], [49, 190, 243, 167], [197, 171, 152, 233], [75, 90, 165, 129]]

S[MIX_COLUMN]-6 :

[["b1", "4b", "1e", "92"], ["31", "be", "f3", "a7"], ["c5", "ab", "98", "e9"], ["4b", "5a", "a5", "81"]]

STATE- 0[0][0]: $177 \oplus 189 = 12$ | 0[0][1]: $75 \oplus 184 = 243$ | 0[0][2]: $30 \oplus 106 = 116$ | 0[0][3]: $146 \oplus 172 = 62$ |
STATE- 1[1][0]: $49 \oplus 61 = 12$ | 1[1][1]: $190 \oplus 124 = 194$ | 1[1][2]: $243 \oplus 108 = 159$ | 1[1][3]: $167 \oplus 46 = 137$ |
STATE- 2[2][0]: $197 \oplus 194 = 7$ | 2[2][1]: $171 \oplus 71 = 236$ | 2[2][2]: $152 \oplus 149 = 13$ | 2[2][3]: $233 \oplus 14 = 231$ |
STATE- 3[3][0]: $75 \oplus 135 = 204$ | 3[3][1]: $90 \oplus 21 = 79$ | 3[3][2]: $165 \oplus 39 = 130$ | 3[3][3]: $129 \oplus 78 = 207$ |
S[ADDDROUNDKEY]-6 :

[12, 243, 116, 62], [12, 194, 159, 137], [7, 236, 13, 231], [204, 79, 130, 207]]

S[ADDDROUNDKEY]-6 :

[["c", "f3", "74", "3e"], ["c", "c2", "9f", "89"], ["7", "ec", "d", "e7"], ["cc", "4f", "82", "cf"]]

=====#
S[SUB_BYTES]-7 :

[254, 13, 146, 178], [254, 37, 219, 167], [197, 206, 215, 148], [75, 132, 19, 138]]

S[SUB_BYTES]-7 :

[["fe", "d", "92", "b2"], ["fe", "25", "db", "a7"], ["c5", "ce", "d7", "94"], ["4b", "84", "13", "8a"]]

S[SHIFT_ROWS]-7 :

[254, 13, 146, 178], [37, 219, 167, 254], [215, 148, 197, 206], [138, 75, 132, 19]]

S[SHIFT_ROWS]-7 :

[["fe", "d", "92", "b2"], ["25", "db", "a7", "fe"], ["d7", "94", "c5", "ce"], ["8a", "4b", "84", "13"]]

S[MIX_COLUMN]-7 :

[213, 179, 140, 187], [92, 76, 23, 15], [235, 56, 51, 254], [228, 206, 220, 219]]

S[MIX_COLUMN]-7 :

[["d5", "b3", "8c", "bb"], ["5c", "4c", "17", "f"], ["eb", "38", "33", "fe"], ["e4", "ce", "dc", "db"]]

STATE- 0[0][0]: $213 \oplus 204 = 25$ | 0[0][1]: $179 \oplus 116 = 199$ | 0[0][2]: $140 \oplus 30 = 146$ | 0[0][3]: $187 \oplus 178 = 9$ |
STATE- 1[1][0]: $92 \oplus 150 = 202$ | 1[1][1]: $76 \oplus 234 = 166$ | 1[1][2]: $23 \oplus 134 = 145$ | 1[1][3]: $15 \oplus 168 = 167$ |
STATE- 2[2][0]: $235 \oplus 237 = 6$ | 2[2][1]: $56 \oplus 170 = 146$ | 2[2][2]: $51 \oplus 63 = 12$ | 2[2][3]: $254 \oplus 49 = 207$ |
STATE- 3[3][0]: $228 \oplus 22 = 242$ | 3[3][1]: $206 \oplus 3 = 205$ | 3[3][2]: $220 \oplus 36 = 248$ | 3[3][3]: $219 \oplus 106 = 177$ |
S[ADDDROUNDKEY]-7 :

[25, 199, 146, 9], [202, 166, 145, 167], [6, 146, 12, 207], [242, 205, 248, 177]]

S[ADDDROUNDKEY]-7 :

[["19", "c7", "92", "9"], ["ca", "a6", "91", "a7"], ["6", "92", "c", "cf"], ["f2", "cd", "f8", "b1"]]

=====#
S[SUB_BYTES]-8 :

[212, 198, 79, 1], [116, 36, 129, 92], [111, 79, 254, 138], [137, 189, 65, 200]]

S[SUB_BYTES]-8 :

[["d4", "c6", "4f", "1"], ["74", "24", "81", "5c"], ["6f", "4f", "fe", "8a"], ["89", "bd", "41", "c8"]]

S[SHIFT_ROWS]-8 :

[[212,198,79,1], [36,129,92,116], [254,138,111,79], [200,137,189,65]]

S[SHIFT_ROWS]-8 :

[["d4", "c6", "4f", "1"], ["24", "81", "5c", "74"], ["fe", "8a", "6f", "4f"], ["c8", "89", "bd", "41"]]

S[MIX_COLUMN]-8 :

[[233,12,168,144], [77,211,251,121], [84,200,17,40], [54,83,131,186]]

S[MIX_COLUMN]-8 :

[["e9", "c", "a8", "90"], ["4d", "d3", "fb", "79"], ["54", "c8", "11", "28"], ["36", "53", "83", "ba"]]

STATE- 0[0][0]: $233 \oplus 142 = 103$ | 0[0][1]: $12 \oplus 250 = 246$ | 0[0][2]: $168 \oplus 228 = 76$ | 0[0][3]: $144 \oplus 86 = 198$ |
STATE- 1[1][0]: $77 \oplus 81 = 28$ | 1[1][1]: $211 \oplus 187 = 104$ | 1[1][2]: $251 \oplus 61 = 198$ | 1[1][3]: $121 \oplus 149 = 236$ |
STATE- 2[2][0]: $84 \oplus 239 = 187$ | 2[2][1]: $200 \oplus 69 = 141$ | 2[2][2]: $17 \oplus 122 = 107$ | 2[2][3]: $40 \oplus 75 = 99$ |
STATE- 3[3][0]: $54 \oplus 33 = 23$ | 3[3][1]: $83 \oplus 34 = 113$ | 3[3][2]: $131 \oplus 6 = 133$ | 3[3][3]: $186 \oplus 108 = 214$ |
S[ADDDROUNDKEY]-8 :

[[103,246,76,198], [28,104,198,236], [187,141,107,99], [23,113,133,214]]

S[ADDDROUNDKEY]-8 :

[["67", "f6", "4c", "c6"], ["1c", "68", "c6", "ec"], ["bb", "8d", "6b", "63"], ["17", "71", "85", "d6"]]

#=====

S[SUB_BYTES]-9 :

[[133,66,41,180], [156,69,180,206], [234,93,127,251], [240,163,151,246]]

S[SUB_BYTES]-9 :

[["85", "42", "29", "b4"], ["9c", "45", "b4", "ce"], ["ea", "5d", "7f", "fb"], ["f0", "a3", "97", "f6"]]

S[SHIFT_ROWS]-9 :

[[133,66,41,180], [69,180,206,156], [127,251,234,93], [246,240,163,151]]

S[SHIFT_ROWS]-9 :

[["85", "42", "29", "b4"], ["45", "b4", "ce", "9c"], ["7f", "fb", "ea", "5d"], ["f6", "f0", "a3", "97"]]

S[MIX_COLUMN]-9 :

[[87,72,82,6], [120,215,40,231], [63,16,214,48], [89,114,2,51]]

S[MIX_COLUMN]-9 :

[["57", "48", "52", "6"], ["78", "d7", "28", "e7"], ["3f", "10", "d6", "30"], ["59", "72", "2", "33"]]

STATE- 0[0][0]: $87 \oplus 191 = 232$ | 0[0][1]: $72 \oplus 69 = 13$ | 0[0][2]: $82 \oplus 161 = 243$ | 0[0][3]: $6 \oplus 247 = 241$ |
STATE- 1[1][0]: $120 \oplus 226 = 154$ | 1[1][1]: $215 \oplus 89 = 142$ | 1[1][2]: $40 \oplus 100 = 76$ | 1[1][3]: $231 \oplus 241 = 22$ |
STATE- 2[2][0]: $63 \oplus 191 = 128$ | 2[2][1]: $16 \oplus 250 = 234$ | 2[2][2]: $214 \oplus 128 = 86$ | 2[2][3]: $48 \oplus 203 = 251$ |
STATE- 3[3][0]: $89 \oplus 144 = 201$ | 3[3][1]: $114 \oplus 178 = 192$ | 3[3][2]: $2 \oplus 180 = 182$ | 3[3][3]: $51 \oplus 216 = 235$ |
S[ADDDROUNDKEY]-9 :

[[232,13,243,241], [154,142,76,22], [128,234,86,251], [201,192,182,235]]

S[ADDDROUNDKEY]-9 :

[["e8", "d", "f3", "f1"], ["9a", "8e", "4c", "16"], ["80", "ea", "56", "fb"], ["c9", "c0", "b6", "eb"]]

#=====

S[SUB_BYTES]-10 :

[[155,215,13,161], [184,25,41,71], [205,135,177,15], [221,186,78,233]]

S[SUB_BYTES]-10 :

[["9b","d7","d","a1"],["b8","19","29","47"],["cd","87","b1","f"],["dd","ba","4e","e9"]]

S[SHIFT_ROWS]-10 :

[155,215,13,161],[25,41,71,184],[177,15,205,135],[233,221,186,78]]

S[SHIFT_ROWS]-10 :

[["9b","d7","d","a1"],["19","29","47","b8"],["b1","f","cd","87"],["e9","dd","ba","4e"]]

STATE- 0[0][0]:155⊕40 = 179 | 0[0][1]:215⊕109 = 186 | 0[0][2]:13⊕204 = 193 | 0[0][3]:161⊕59 = 154 |
STATE- 1[1][0]:25⊕253 = 228 | 1[1][1]:41⊕164 = 141 | 1[1][2]:71⊕192 = 135 | 1[1][3]:184⊕49 = 137 |
STATE- 2[2][0]:177⊕222 = 111 | 2[2][1]:15⊕36 = 43 | 2[2][2]:205⊕164 = 105 | 2[2][3]:135⊕111 = 232 |
STATE- 3[3][0]:233⊕248 = 17 | 3[3][1]:221⊕74 = 151 | 3[3][2]:186⊕254 = 68 | 3[3][3]:78⊕38 = 104 |
S[ADDROUNDKEY]-10 :

[179,186,193,154],[228,141,135,137],[111,43,105,232],[17,151,68,104]]

S[ADDROUNDKEY]-10 :

[["b3","ba","c1","9a"],["e4","8d","87","89"],["6f","2b","69","e8"],["11","97","44","68"]]

#=====

"KcNQX1cUIPZAipmzGgLX0rPkbxG6jSuXwYdpRJqJ6Gg="