Bài tập

P =

K = 0F1571C9 47D9E859 0CB7ADD6 AF7F6798

W3 = AF 7F 67 98

Rotword = 7F 67 98 AF

SubByte = D2 85 46 79

RC1/4 = RC4/4 = 1 = 01 00 00 00

W0 = 0F 15 71 C9 + T4 = D3 85 46 79

W4 = DC 90 37 B0

W5 = W1 + W4

W1 = 47 D9 E8 59 + W4 = DC 90 37 B0

W5 = 9B 49 DF E9

W6 = W2 + W5

W2 = 0C B7 AD D6 + W5 = 9B 49 DF E9

W6 = 97 FE 72 3F

W7 = W3 + W6

W3 = AF 7F 67 98 + W6 = 97 FE 72 3F

W7  = 38 81 15 A7