MATH 178 Homework #8

Tamir Enkhjargal

May 2019

AES

K_0=1011 1101 0010 0101
K_1=0010 0111 0000 0010
K_2=1011 1110 1011 1100
K =1011 1101 0010 0101 0010 0111 0000 0010 1011 1110 1011 1100

$b_3 \oplus b_5$	$b_0 \oplus b_6$	$b_1 \oplus b_4 \oplus b_7$	$b_2 \oplus b_3 \oplus b_4$
$b_1 \oplus b_7$	$b_2 \oplus b_4$	$b_0 \oplus b_3 \oplus b_5$	$b_0 \oplus b_6 \oplus b_7$

Table 1: Mix Column Inverse Table

4

ii) Using the Mix Column Inverse Table on K_1, we get:

1011 1101 0010 0101→ 1111 1110 0100 0001

iii) We know that we're using the same key that we expanded. The string we want to decrypt is 0111 0001 0011 1001

$$A_{K0} \circ SR^{-1} \circ NS^{-1} \circ A_{c(z)^{-1}K1} \circ MC^{-1} \circ SR^{-1} \circ NS^{-1} \circ A_{K2} \quad (1)$$

$$CT_0 \oplus A_{K2} = 0111000100111001 \oplus 1011111010111100 \quad (2)$$

$$= 1100\ 1111\ 1000\ 0101 = CT_1 \quad (3)$$

$$NS^{-1}(CT_1) = 1100\ 1110\ 0110\ 0111 = CT_2 \quad (4)$$

$$SR^{-1}(CT_2) = 1100\ 0111\ 0110\ 1110 = CT_3 \quad (5)$$

$$MC^{-1}(CT_3) = \quad (6)$$

$$[(0+1)(1+1)(1+0+1)(0+0+0)] \quad (7)$$

$$[(1+1)(0+0)(1+0+1)(1+1+1)] \quad (8)$$

$$[(0+1)(0+1)(1+1+0)(1+0+1)] \quad (9)$$

$$[(1+0)(1+1)(0+0+1)(0+1+0)] \quad (10)$$

$$= 1000\ 0001\ 1100\ 1011 = CT_4 \quad (11)$$

$$CT_4 \oplus A_{c(z)^{-1}K1} = 1000000111001011 \oplus 1111111001000001 \quad (12)$$

$$= 0111\ 1111\ 1000\ 1010 = CT_5 \quad (13)$$

$$NS^{-1}(CT_5) = 1111\ 1110\ 0110\ 0010 = CT_6 \quad (14)$$

$$SR^{-1}(CT_6) = 1111\ 0010\ 0110\ 1110 = CT_7 \quad (15)$$

$$CT_7 \oplus A_{K0} = 1111001001101110 \oplus 1011110100100101 \quad (16)$$

$$= 0100\ 1111\ 0100\ 1011 = PT \quad (17)$$

After decoding from binary to ASCII, we get the plaintext message OK