

IT-Security Cryptography and Secure Communications

Exercise: AES

Lecturer: Prof. Dr. Michael Eichberg

Version: 2023-10-19

For this exercise let's assume that we have a 128 bit key.

1. RoundKey computation:

Given the following RoundKey:

$$rc_1 = w[4] || w[5] || w[6] || w[7] =$$

-w[4]-----	-w[5]-----	-w[6]-----	-w[7]-----
E2 32 FC F1	91 12 91 88	B1 59 E4 E6	D6 79 A2 93

Calculate rc_2 ; i.e. the Roundkey for the second round.

1. Before performing the concrete computation, first write down the formulae:

$$w[8] = \dots \in \dots$$

$$w[9] = \dots \in \dots$$

$$w[10] = \dots \in \dots$$

$$w[11] = \dots \in \dots$$

Solution

$$w[8] = w[4] \in g(w[7])$$

$$w[9] = w[5] \in w[8]$$

$$w[10] = w[6] \in w[9]$$

$$w[11] = w[7] \in w[10]$$

2. Calculate $w[8]$ and $w[9]$.

Solution

$g(w[7])$:

- | | |
|---------------------------------|-------------|
| 1. after left shift of $w[7]$: | 79 A2 93 D6 |
| 2. after s-box substitution: | B6 3A DC F6 |

3. after add RoundConstant (02 00 00 00): B4 3A DC F6

w[8] = E2 32 FC F1 xor B4 3A DC F6 = 56 08 20 07

w[9] = w[8] xor 91 12 91 88 = C7 1A B1 8F

2. Let's assume that the current State matrix is:

00 3C 6E 47

1F 4E 22 74

0E 08 1B 31

54 59 0B 1A

Perform the step *substitute bytes*; i.e., apply the s-box transformation.

Solution

63 EB 9F A0

C0 2F 93 92

AB 30 AF C7

20 CB 2B A2

3. Perform the *shift rows transformation* on your previous result.

Solution

63 EB 9F A0

2F 93 92 C0

AF C7 AB 30

A2 20 CB 2B

4. Given the following State matrix:

6A 59 CB BD

4E 48 12 A0

98 9E 30 9B

8B 3D F4 9B

Perform the mix columns transformation for the missing field ($S'_{0,0}$):

?? C9 7F 9D

CE 4D 4B C2

89 71 BE 88

65 47 97 CD

Solution

$0x02 \cdot 0x6A = (\text{simple left shift of } 6A) : 1101\ 0100_b$

$0x03 \cdot 0x4E = 0x4E \in (0x02 \cdot 0x4E) = 0100\ 1110_b \in 1001\ 1100_b = 11010010_b$

$S^0_{0,0} = 1101\ 0100_b \in 1101\ 0010_b \in 0x98 \in 0x8B = 0x15$

5. Apply the RoundKey:

$-w[x]$ -----	$-w[x+1]$ -----	$-w[x+2]$ -----	$-w[x+3]$ -----
D2 60 0D E7	15 7A BC 68	63 39 E9 01	C3 03 1E FB

to the State:

AA 65 FA 88
16 0C 05 3A
3D C1 DE 2A
B3 4B 5A 0A

Solution

Recall that the round key applies to the column!

78 70 99 4B
76 76 3C 39
30 7D 37 34
54 23 5B F1

6. Ask yourself what happens if you encrypt a block just consisting of 0x00s with a key also consisting only of 0x00s?

Solution

- First substitution will map all values to the same value: 0x63,.
- Shift row will have no effect.
- Mix columns (because the values are no longer 0x00 will lead to some diffusion $0x02 \times 0x63$ and $0x03 \times 0x63$ is not 0x63.)
- AddRoundKey will also effect and lead (already during the first round) to some confusion.