Lab 6 - Public Crypto

> Igor Mpore
>
> BS19-CS01
>
> i.mpore@innopolis.university

1. Crypto basics 1

In this solution, I have ignored the inital Key Addition of k_0 . We know that all the S-boxes are the same function, and that the input will the same in each case ($FF_{16}FF_{16}$). The array (A_0–A_{15}) is produced by Byte Substitution and it resulted into the array below:

$$\begin{bmatrix} 16_{16} & 16_{16} & 16_{16} & 16_{16} \\ 16_{16} & 16_{16} & 16_{16} & 16_{16} \\ 16_{16} & 16_{16} & 16_{16} & 16_{16} \\ 16_{16} & 16_{16} & 16_{16} & 16_{16} \end{bmatrix}$$

Using the MixColumn matrix multiplication, we can express the above matrix as below since $ax + bx + cx + dx = x(a + b + c + d)$:

$$\begin{bmatrix} (02 + 03 + 01 + 01) \times 16_{16} \\ (01 + 02 + 03 + 01) \times 16_{16} \\ (01 + 01 + 02 + 03) \times 16_{16} \\ (03 + 01 + 01 + 02) \times 16_{16} \end{bmatrix}$$

Now, let's bitwise XOR the round key into the state:

$$\begin{bmatrix} 16_{16} & 16_{16} & 16_{16} & 16_{16} \\ 16_{16} & 16_{16} & 16_{16} & 16_{16} \\ 16_{16} & 16_{16} & 16_{16} & 16_{16} \\ 16_{16} & 16_{16} & 16_{16} & 16_{16} \end{bmatrix} XOR \begin{bmatrix} FF_{16} & FF_{16} & FF_{16} & FF_{16} \\ FF_{16} & FF_{16} & FF_{16} & FF_{16} \\ FF_{16} & FF_{16} & FF_{16} & FF_{16} \\ FF_{16} & FF_{16} & FF_{16} & FF_{16} \end{bmatrix} = \begin{bmatrix} E9_{16} & E9_{16} & E9_{16} & E9_{16} \\ E9_{16} & E9_{16} & E9_{16} & E9_{16} \\ E9_{16} & E9_{16} & E9_{16} & E9_{16} \\ E9_{16} & E9_{16} & E9_{16} & E9_{16} \end{bmatrix}$$

That is the final state after the first round of encryption.

2. Crypto basics 2

> Hint: CBC (Cipher Block Chaining) Cryptography

Since both attacks are based on CBC (Cipher Block Chaining), let's first define it.

CBC Mode cryptography is a cryptography mode of operation for a block cipher which allows encryption of arbitrary length data. Encryption and decryption are defined by:

$$C_i = e_K(P_i \oplus C_{i-1})$$
$$P_i = d_K(C_i) \oplus C_{i-1}$$

1. **Padding Oracle Attack**

In symmetric cryptography, the padding oracle attack can be applied to the CBC mode of operation, where the "oracle" (usually a server) leaks data about whether the padding of an encrypted message is correct or not. Such data can allow attackers to decrypt (and sometimes encrypt) messages through the oracle using the oracle's key, without knowing the encryption key.

2. **CBC Byte Flipping Attack**

   This attack prepends certain values to the plaintext before encryption with the aim to hange the final cipher text even though the attacker has no ability to know what the plaintext was. This attack can be considered as a Denial of Service attack since the intended receiver can't get the correct message from the sender.

3. Crypto basics 3

In this exercise, the ordering of bytes within the array table grid will be column by column (i.e from left to right).

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

1. **First round of AES to the input W and the subkeys W0, . . . ,W7.**

The first state after adding k_0 is as follow:

$2A$	28	AB	09
$7E$	AE	$F7$	CF
15	$D2$	15	$4F$
16	$A6$	88	$3C$

After applying the ByteSubstitution (S-box) layer, the state is as follows:

$E5$	34	62	01
$F3$	$E4$	68	$8A$
59	$B5$	59	84
47	24	$C4$	EB

We then perform ShiftRows layer where the first row remains unchainged and the other rows are rotated right by a number of positions; the second by 3, the third by 2 and the fourth by 1. This gives the following:

$E5$	34	62	01
$E4$	68	$8A$	$F3$
59	84	59	$B5$
EB	47	24	$C4$

The final transformation (other than the k_1 addition) is the MixColumn layer. This involves a Galois Extension Field matrix multiplication with the following description:

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

Where $C = Outputted\ Column$ And
$B = Input\ columns\ which\ were\ the\ output\ of\ the\ ShiftRows\ layer.$

After doing the calculations, the resulted state is as follow :

54	13	$3C$	$7D$
36	34	$A2$	FC
95	86	36	$D4$
44	$3E$	$3D$	$D6$

All that's left to do after this is the KeyAddition layer which results into the following final state:

$F4$	$9B$	$1F$	57
CC	60	01	90
$6B$	AA	$0F$	$A2$
53	$8F$	04	$D3$

$$= F4CC6B539B60AA8F1F010F045790A2D3_{16}$$

2. **<u>First round of AES for the case that all input bits are zero</u>**

For the case that the input is all-zeroes, the state after the k_0 key addition will be:

$2B$	28	AB	09
$7E$	AE	$F7$	CF
15	$D2$	15	$4F$
16	$A6$	88	$3C$

After this, we apply ByteSubstitution (S-box) layer , ShiftRows layer and The MixColumn respectively:

$F1$	34	62	01
$F3$	$E4$	68	$8A$
59	$B5$	59	84
47	24	$C4$	EB

$\rightarrow$

$F1$	34	62	01
$E4$	68	$8A$	$F3$
59	84	59	$B5$
EB	47	24	$C4$

$\rightarrow$

$7C$	13	$3C$	$7D$
22	34	$A2$	FC
81	86	36	$D4$
78	$3E$	$3D$	$D6$

Lastly, we perform KeyAddition for $k_1 = W_4, \ldots, W_7$ and the final state is as follow:

DC	$9B$	$1F$	57
$D8$	60	01	90
$7F$	AA	$0F$	$A2$
$6F$	$8F$	04	$D3$

$$= DCD87F6F9B60AA8F1F010F045790A2D3_{16}$$

3. **<u>How many output bits have changed?</u>**

To be able to view the changes, we can apply XOR on the two output values together. This produces:

$$2814143c00000000000000000000000_{16}$$

From this, we can see that only the first column is altered after the first round:

$$2814143c_{16} = 10100000010100000101000011110 0_2$$

4. Crypto basics 4

Starting from $RC[1] = 01$, $RC[i] = 02 \times RC[i-1] mod P(x)$ where $P(x)$ is the AES polynomial, we get that:

$$\begin{aligned}
RC[1] = 1 = 00000001_2 = 01_{16} \\
RC[2] = x = 00000010_2 = 02_{16} \\
RC[3] = x^2 = 00000100_2 = 04_{16} \\
RC[4] = x^3 = 00001000_2 = 08_{16} \\
RC[5] = x^4 = 00010000_2 = 10_{16} \\
RC[6] = x^5 = 00100000_2 = 20_{16} \\
RC[7] = x^6 = 01000000_2 = 40_{16} \\
RC[8] = x^7 = 10000000_2 = 80_{16} \\
RC[9] = x^4 + x^3 + x + 1 = 00011011_2 = 1B_{16} \\
RC[10] = x^5 + x^4 + x^2 + x = 00110110_2 = 36_{16}
\end{aligned}$$

So, from the above calculation, $RC[8] = 80_{16}$ and $RC[10] = 36_{16}$