Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 6
- Proposed Solution -

Friday, May 24, 2019

Solution of Problem 1

The given AES-128 key is denoted in hexadecimal representation:

$$K = (2D\ 61\ 72\ 69 \mid 65\ 00\ 76\ 61 \mid 6E\ 00\ 43\ 6C \mid 65\ 65\ 66\ 66)$$

(a) The round key is $K_0 = K = (W_0\ W_1\ W_2\ W_3)$ with $W_0 = (2D\ 61\ 72\ 69)$, $W_1 = (65\ 00\ 76\ 61)$, $W_2 = (6E\ 00\ 43\ 6C)$, $W_3 = (65\ 65\ 66\ 66)$.

(b) To calculate the first 4 bytes of round key K_1 recall that $K_1 = (W_4\ W_5\ W_6\ W_7)$. Follow Alg. 1 as given in the lecture notes to calculate W_4:

Algorithm 1 AES key expansion (applied)

for $i \leftarrow 4;\ i < 4 \cdot (r+1);\ i++$ **do**
  Initialize *for*-loop with $i \leftarrow 4$.
  $\text{tmp} \leftarrow W_{i-1}$
  $\text{tmp} \leftarrow W_3 = (65\ 65\ 66\ 66)$
  if $(i \mod 4 = 0)$ **then**
    result is *true* as $i = 4$.
    $\text{tmp} \leftarrow \texttt{SubBytes}(\texttt{RotByte}(\text{tmp})) \oplus \texttt{Rcon}(i/4)$
    Evaluate this operation step by step:
    $\texttt{RotByte}(\text{tmp}) = (65\ 66\ 66\ 65)$, i.e., a cyclic left shift of one byte
    To compute $\texttt{SubBytes}(65\ 66\ 66\ 65)$ evaluate Table 5.8 for each byte:
    $(\text{row } 6, \text{col } 5)$ provides $77_{10} = 4D_{16}$
    $(\text{row } 6, \text{col } 6)$ provides $51_{10} = 33_{16}$
    Note that the indexation of rows and columns starts with zero.
    $\texttt{SubBytes}(65\ 66\ 66\ 65) = (4D\ 33\ 33\ 4D)$
    $i/4 = 1$
    $\texttt{Rcon}(1) = (\texttt{RC}(1)\ 00\ 00\ 00)$, with $\texttt{RC}(1) = x^{1-1} = x^0 = 1 \in \mathbb{F}_{2^8}$.
    $\text{tmp} \leftarrow (4D\ 33\ 33\ 4D) \oplus (01\ 00\ 00\ 00) = (4C\ 33\ 33\ 4D)$
  end if
  $W_i \leftarrow W_{i-4} \oplus \text{tmp}$ $W_4 \leftarrow W_0 \oplus \text{tmp}$. Then, next iteration, $i \leftarrow 5$...
end for

	W_0	2	D	6	1	7	2	6	9
$\oplus$	tmp	4	C	3	3	3	3	4	D
	W_0	0010	1101	0110	0001	0111	0010	0110	1001
$\oplus$	tmp	0100	1100	0011	0011	0011	0011	0100	1101
	W_4	0110	0001	0101	0010	0100	0001	0010	0100
	W_4	6	1	5	2	4	1	2	4

Solution of Problem 2

Given: Alphabet $\mathcal{A}$, blocklength $n \in \mathbb{N}$ and $\mathcal{M} = \mathcal{A}^n = \mathcal{C}$.
$\mathcal{A}^n$ describes all possible streams of n bits.

a) An encryption is an injective function $e_K : \mathcal{M} \to \mathcal{C}$, with $K \in \mathcal{K}$.
Fix key $K \in \mathcal{K}$. As $e_K(\cdot)$ is injective, it holds:

- $\{e_K(M) \mid M \in \mathcal{M}\} \subseteq \mathcal{C}$
- $\{e_K(M) \mid M \in \mathcal{M}\} = \mathcal{M}$
- Since $\mathcal{M} = \mathcal{C} \Rightarrow e_K(\mathcal{M}) = \mathcal{C}$ also surjective
- $\Rightarrow e(\mathcal{M}, K)$ is a bijective function.

A permutation π is a bijective (one-to-one) function $\pi : \mathcal{X} \to \mathcal{X}$.
$\Rightarrow$ For each K, the encryption $e_K(\cdot)$ is a permutation with $\mathcal{X} = \mathcal{A}^n$.

b) With $\mathcal{A} = \{0, 1\} \Rightarrow |\mathcal{A}| = |\{0, 1\}| = 2$, and $n = 6$ there are $N = 2^6 = 64$ elements.
It follows that there are $64! \approx 1.2689 \cdot 10^{89}$ different block ciphers.

Solution of Problem 3

a) The bit error occurs in block C_i, $i > 0$, with block size BS.

mode	M_i	max #err	remark
ECB	$E_K^{-1}(C_i)$	BS	Only block M_i is affected
CBC	$E_K^{-1}(C_i) \oplus C_{i-1}$	BS+1	M_i and one bit in M_{i+1}
OFB	$C_i \oplus Z_i$	1	One bit in M_i, as $Z_0 = C_0, Z_i = E_K(Z_{i-1})$
CFB	$C_i \oplus E_k(C_{i-1})$	BS+1	M_{i+1} and one bit in M_i
CTR	$C_i \oplus E_K(Z_i)$	1	One bit in M_i, $Z_0 = C_0, Z_i = Z_{i-1} + 1$

b) If one bit of the ciphertext is lost or an additional one is inserted in block C_i at position j, all bits beginning with the following positions may be corrupt:

mode	block	position
ECB	i	1
CBC	i	1
OFB	i	j
CFB	i	j
CTR	i	j

In ECB and CBC, all bits of all blocks C_{i+k}, $k \in \mathbb{N}_0$ may be corrupt.
In OFB, CFB, CTR, all bits beginning at position j of block C_i may be corrupt.