Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 6
- Proposed Solution -

Friday, June 2, 2017

Solution of Problem 1

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 C_i is affected
CBC	$E_K^{-1}(C_i) \oplus C_{i-1}$	BS+1	C_i and one bit in C_{i+1}
OFB	$C_i \oplus Z_i$	1	one bit in C_i, as $Z_0 = C_0, Z_i = E_K(Z_{i-1})$
CFB	$C_i \oplus E_k(C_{i-1})$	BS+1	C_i and one bit in C_{i+1}
CTR	$C_i \oplus E_K(Z_i)$	1	one bit in C_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 blocks C_i, C_{i+1} may be corrupt.
In OFB, CFB, CTR, all bits beginning at position j of block C_i may be corrupt.

Solution of Problem 2

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 $i \leftarrow 4$. We have $r = 1$ for K_1.
  tmp $\leftarrow W_{i-1}$
  tmp $\leftarrow W_3 = (65\ 65\ 66\ 66)$
  if $(i \mod 4 = 0)$ **then**
    result is *true* as $i = 4$.
    tmp $\leftarrow$ `SubBytes`(`RotByte`(tmp)) $\oplus$ `Rcon`$(i/4)$
    Evaluate this operation step by step:
    `RotByte`(tmp) $= (65\ 66\ 66\ 65)$, i.e., a cyclic left shift of one byte
    To compute `SubBytes`$(65\ 66\ 66\ 65)$ evaluate Table 5.8 for each byte:
    (row 6, col 5) provides $77_{10} = 4D_{16}$
    (row 6, col 6) provides $51_{10} = 33_{16}$
    Note that the indexation of rows and columns starts with zero.
    `SubBytes`$(65\ 66\ 66\ 65) = (4D\ 33\ 33\ 4D)$
    $i/4 = 1$
    `Rcon`$(1) = ($`RC`$(1)\ 00\ 00\ 00)$, with `RC`$(1) = x^{1-1} = x^0 = 1 \in \mathbb{F}_{2^8}$.
    tmp $\leftarrow (4D\ 33\ 33\ 4D) \oplus (01\ 00\ 00\ 00) = (4C\ 33\ 33\ 4D)$
  end if
  $W_i \leftarrow W_{i-4} \oplus$ tmp $W_4 \leftarrow W_0 \oplus$ 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 3

Message $\boldsymbol{m} = (m_1 m_2, ... m_l)$, with $m_i \in \mathbb{F}_2$.
Key $\boldsymbol{k} = (k_1 k_2, ... k_n)$, with $k_i \in \mathbb{F}_2$ and $n < l$. $\Rightarrow$ Keystream $\boldsymbol{z} = (z_1, z_2, ..., z_l)$

$$\begin{aligned} z_i &= k_i, \quad 1 \leq i \leq n \\ z_i &= \sum\nolimits_{j=1}^{n} s_j z_{ij} \mod 2, \quad n < i \leq l \\ c_i &= z_i \oplus m_i, \quad 1 \leq i \leq l \end{aligned}$$

a) Decryption: $m_i = c_i \oplus z_i$

b) If $\boldsymbol{k} = \boldsymbol{0} = (00...0)$, it follows $z_i = 0, \quad 1 \leq i \leq n$, and $z_i = 0, \quad n < i \leq l$ and $c_i = m_i, \quad 1 \leq i \leq l$. In this case, the plaintext is not encrypted at all.

c) key length $n = 4$, key $\boldsymbol{k} = (0110)$,
addition paths $s_1 = s_4 = 1$, $s_2 = s_3 = 0 \Rightarrow \boldsymbol{s} = (1001)$,
stream length $l = 20$

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}
0	1	1	0	0	1	0	0	0	1
z_{11}	z_{12}	z_{13}	z_{14}	z_{15}	z_{16}	z_{17}	z_{18}	z_{19}	z_{20}
1	1	1	0	1	0	1	1	0	0

The summation simplifies to $z_i = \sum_{j=1}^{n} s_j z_{ij} = z_{i-1} \oplus z_{i-4}$, $4 < i \leq 20$

- n provide registers 2^n states
- Maximal period: $p_{\max} = 2^n - 1 = 15$ (Minor remark: fulfilled if z_i is a *primitive polynomial*)
- The keystream repeats itself at z_{16}

encryption:

$\boldsymbol{m}$	1011	0001	0100	1101	0100
$\boldsymbol{z}$	0110	0100	0111	1010	1100
$\boldsymbol{m} \oplus \boldsymbol{z}$	1101	0101	0011	0111	1000