KRIPTOGRAFIJA, VJEŽBE

(AES operacija)

1. Izračunajte:

$$(\texttt{0x21}, \texttt{0x31}, \texttt{0x01}, \texttt{0x00}) \otimes (\texttt{0x01}, \texttt{0x21}, \texttt{0x01}, \texttt{0x00}).$$

"⊗" označava 32-bitnu AES binarnu operaciju.

Rješenje. Uz oznake

$$(a_3, a_2, a_1, a_0) = (\texttt{0x21}, \texttt{0x31}, \texttt{0x01}, \texttt{0x00})$$
$$(b_3, b_2, b_1, b_0) = (\texttt{0x01}, \texttt{0x21}, \texttt{0x01}, \texttt{0x00}),$$

rezultat (d_3, d_2, d_1, d_0) možemo dobiti matričnim množenjem prema sljedećoj shemi

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

Elemente ove matrice interpretiramo kao polinome na sljedeći način

$$\texttt{0x31} = \texttt{0011 0001}_2 \mapsto x^5 + x^4 + x^0 = x^5 + x^4 + 1$$
$$\texttt{0x21} = \texttt{0010 0001}_2 \mapsto x^5 + x^0 = x^5 + 1$$
$$\texttt{0x01} = \texttt{0000 0001}_2 \mapsto 1$$

Operacije "+" i "·" koje se koriste u ovom matričnom množenju su operacije u polju $GF(2^8)$:

- zbrajanje polinoma (modulo 2) koje možemo gledati kao XOR numeričkih reprezentacija ovih polinoma
- množenje polinoma s koeficijentima iz $\mathbb{Z}_2$ i reduciranje na ostatak modulo polinom $x^8 + x^4 + x^3 + x + 1$.

Prema shemi matričnog množenja

$$\begin{aligned} d_0 &= a_0 \cdot b_0 + a_3 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot b_3 \\ &= \texttt{0x00} \cdot \texttt{0x00} + \texttt{0x21} \cdot \texttt{0x01} + \texttt{0x31} \cdot \texttt{0x21} + \texttt{0x01} \cdot \texttt{0x01} \\ &= \texttt{0x21} + \texttt{0x01} + \texttt{0x31} \cdot \texttt{0x21} \\ &= \texttt{0x20} + \texttt{0x31} \cdot \texttt{0x21} \end{aligned}$$

Izračunajmo $\texttt{0x31} \cdot \texttt{0x21}$:

$$(x^5 + x^4 + 1)(x^5 + 1) = x^{10} + x^9 + 2x^5 + x^4 + 1 \equiv x^{10} + x^9 + x^4 + 1$$

Rezultat množenja trebamo reducirati modulo $g(x) = x^8 + x^4 + x^3 + x + 1$. Treba naći ostatak pri dijeljenju s $g(x)$.

$$\begin{aligned} &(x^{10} + x^9 + x^4 + 1) : (x^8 + x^4 + x^3 + x + 1) = x^2 + x \\ &x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \\ &x^6 + x^3 + x + 1 \end{aligned}$$

Ostatak je $x^6 + x^3 + x + 1$, u heksadecimalnom zapisu $\texttt{0100 1011} = \texttt{0x4b}$. Prema tome je

$$\texttt{0x31} \cdot \texttt{0x21} = \texttt{0x4b}\,.$$

Odavde je

$$d_0 = \texttt{0x20} + \texttt{0x4b} = \texttt{0x6b}\,.$$

Uz isti postupak za d_1, d_2 i d_3 dobije se

$$(d_3, d_2, d_1, d_0) = (\texttt{0x10}, \texttt{0x20}, \texttt{0x5c}, \texttt{0x6b})\,.$$

□