MNM
TEAM
Munich Network Management Team

Ludwig-Maximilians-Universität München

Prof. Dr. D. Kranzlmüller, Dr. N. gentschen Felde

Data Science & Ethics

– interim exercise –

Exercise 1: *CrypTool*

Take a closer look at the CrypTool project at `https://www.cryptool.org/` and try to recap / exercise on the cryptographical functions seen during the lecture.

Exercise 2: *AES*

Given the values below, derive the value of the first byte (1^{st} row, 1^{st} column) after the 1^{st} round of the Rijndael algorithm (AES, 128 bit block und key length). Please note that multiplications have to be carried out in GF(2^8). Let the irreducible polynom be $x^8 + x^4 + x^3 + x + 1$.

clear text:	first round key (round 0):	coulumn mix matrix:
$\begin{pmatrix} 23 & 12 & 19 & 27 \\ 08 & 34 & 42 & 10 \\ 37 & 21 & 14 & 32 \\ 15 & 53 & 11 & 45 \end{pmatrix}$	$\begin{pmatrix} 12 & 07 & 1A & 33 \\ 30 & 01 & 16 & 54 \\ 14 & 63 & 27 & 11 \\ 44 & 23 & 55 & 10 \end{pmatrix}$	$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$

S-BOX (fictitious):

	0	1	2	3	4	5	6	7	8
0	0x00	0x10	0x20	0x01	0x18	0x19	0xB4	0x45	0x2C
1	0x01	0x25	0xE1	0xCB	0x10	0x13	0xA7	0x3B	0x1A
2	0x2D	0xA1	0x40	0x89	0x9D	0x34	0x12	0x5E	0x2D
3	0x38	0xB4	0x2C	0x29	0x02	0xA6	0xF1	0x01	0x89
4	0x43	0xF2	0x20	0x30	0x40	0x02	0xD8	0x7B	0x6A
5	0xC4	0xA1	0x28	0x34	0xA2	0x09	0x7F	0x4D	0xC2
6	0x32	0x27	0x98	0x45	0x51	0x02	0xE4	0x89	0x2E
7	0xA6	0x2A	0x16	0x46	0x18	0x27	0xB3	0x1D	0xC8

The following round key has been calculated during the first key expansion:

$$\begin{pmatrix} 1A & 5A & EE & 18 \\ B7 & 87 & 26 & B4 \\ 41 & 51 & 43 & 45 \\ 19 & 39 & CA & 18 \end{pmatrix}$$