	0_{16}	1_{16}	2_{16}	3_{16}	4_{16}	5_{16}	6_{16}	7_{16}	8_{16}	9_{16}	a_{16}	b_{16}	c_{16}	d_{16}	e_{16}	f_{16}
0_{16}	0_{16}	1_{16}	2_{16}	3_{16}	4_{16}	5_{16}	6_{16}	7_{16}	8_{16}	9_{16}	a_{16}	b_{16}	c_{16}	d_{16}	e_{16}	f_{16}
1_{16}	1_{16}	0_{16}	3_{16}	2_{16}	5_{16}	4_{16}	7_{16}	6_{16}	9_{16}	8_{16}	b_{16}	a_{16}	d_{16}	c_{16}	f_{16}	e_{16}
2_{16}	2_{16}	3_{16}	0_{16}	1_{16}	6_{16}	7_{16}	4_{16}	5_{16}	a_{16}	b_{16}	8_{16}	9_{16}	e_{16}	f_{16}	c_{16}	d_{16}
3_{16}	3_{16}	2_{16}	1_{16}	0_{16}	7_{16}	6_{16}	5_{16}	4_{16}	b_{16}	a_{16}	9_{16}	8_{16}	f_{16}	e_{16}	d_{16}	c_{16}
4_{16}	4_{16}	5_{16}	6_{16}	7_{16}	0_{16}	1_{16}	2_{16}	3_{16}	c_{16}	d_{16}	e_{16}	f_{16}	8_{16}	9_{16}	a_{16}	b_{16}
5_{16}	5_{16}	4_{16}	7_{16}	6_{16}	1_{16}	0_{16}	3_{16}	2_{16}	d_{16}	c_{16}	f_{16}	e_{16}	9_{16}	8_{16}	b_{16}	a_{16}
6_{16}	6_{16}	7_{16}	4_{16}	5_{16}	2_{16}	3_{16}	0_{16}	1_{16}	e_{16}	f_{16}	c_{16}	d_{16}	a_{16}	b_{16}	8_{16}	9_{16}
7_{16}	7_{16}	6_{16}	5_{16}	4_{16}	3_{16}	2_{16}	1_{16}	0_{16}	f_{16}	e_{16}	d_{16}	c_{16}	b_{16}	a_{16}	9_{16}	8_{16}
8_{16}	8_{16}	9_{16}	a_{16}	b_{16}	c_{16}	d_{16}	e_{16}	f_{16}	0_{16}	1_{16}	2_{16}	3_{16}	4_{16}	5_{16}	6_{16}	7_{16}
9_{16}	9_{16}	8_{16}	b_{16}	a_{16}	d_{16}	c_{16}	f_{16}	e_{16}	1_{16}	0_{16}	3_{16}	2_{16}	5_{16}	4_{16}	7_{16}	6_{16}
a_{16}	a_{16}	b_{16}	8_{16}	9_{16}	e_{16}	f_{16}	c_{16}	d_{16}	2_{16}	3_{16}	0_{16}	1_{16}	6_{16}	7_{16}	4_{16}	5_{16}
b_{16}	b_{16}	a_{16}	9_{16}	8_{16}	f_{16}	e_{16}	d_{16}	c_{16}	3_{16}	2_{16}	1_{16}	0_{16}	7_{16}	6_{16}	5_{16}	4_{16}
c_{16}	c_{16}	d_{16}	e_{16}	f_{16}	8_{16}	9_{16}	a_{16}	b_{16}	4_{16}	5_{16}	6_{16}	7_{16}	0_{16}	1_{16}	2_{16}	3_{16}
d_{16}	d_{16}	c_{16}	f_{16}	e_{16}	9_{16}	8_{16}	b_{16}	a_{16}	5_{16}	4_{16}	7_{16}	6_{16}	1_{16}	0_{16}	3_{16}	2_{16}
e_{16}	e_{16}	f_{16}	c_{16}	d_{16}	a_{16}	b_{16}	8_{16}	9_{16}	6_{16}	7_{16}	4_{16}	5_{16}	2_{16}	3_{16}	0_{16}	1_{16}
f_{16}	f_{16}	e_{16}	d_{16}	c_{16}	b_{16}	a_{16}	9_{16}	8_{16}	7_{16}	6_{16}	5_{16}	4_{16}	3_{16}	2_{16}	1_{16}	0_{16}

Tabelle 1: Ergebnis der XOR-Verknüpfung hexadezimal.

Beispiele für die grundlegenden Rechenoperationen im AES

a) Verknüpfung von Bytes:

$a(x) = x^6 + x^4 + x^2 + x + 1 = 0101\,0111 = 57,$

$b(x) = x^7 + x + 1 = 1000\,0011 = 83$

$c(x) = a(x) \oplus b(x) = x^7 + x^6 + x^4 + x^2 = 1101\,0100 = \mathrm{D4}.$

$$\begin{aligned} d(x) = a(x) \odot b(x) &= (x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) \\ &= x^{13}+x^7+x^6+x^{11}+x^5+x^4+x^9+x^3+x^2+x^8+x^2+x+x^7+x+1 \\ &= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

$d(x)$ muss noch modulo $m(x)$ reduziert werden; dazu wird der Rest von $d(x)$ bei Division durch das Polynom $m(x) = x^8 + x^4 + x^3 + x + 1$ bestimmt:

$$\begin{array}{l}
(x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1) : (x^8+x^4+x^3+x+1) = x^5+x^3 \\
\underline{x^{13} \qquad + x^9 + x^8 + x^6 + x^5} \\
\qquad x^{11} \qquad\qquad\qquad\qquad + x^4 + x^3 + 1 \\
\qquad \underline{x^{11} \;\; + x^7 + x^6 \qquad\quad + x^4 + x^3} \\
\qquad\qquad\quad x^7 + x^6 \qquad\qquad\qquad\qquad + 1 = r(x)
\end{array}$$

$d(x) = x^7 + x^6 + 1 = 1100\,0001 = \mathrm{C1}.$

b) Verknüpfung von Polynomen mit Koeffizienten aus GF(2^8):

$$\begin{aligned} a(x) &= 01 \cdot x^3 + 03 \cdot x^2 + \mathrm{A1} \cdot x + 02, \\ b(x) &= 02 \cdot x^3 + 01 \cdot x + \mathrm{FF} \end{aligned}$$

$$\begin{aligned} c(x) &= a(x) + b(x) \\ &= (01 \oplus 02) \cdot x^3 + (03 \oplus 00) \cdot x^2 + (\mathrm{A1} \oplus 01) \cdot x + (02 \oplus \mathrm{FF}) \\ &= 03 \cdot x^3 + 03 \cdot x^2 + \mathrm{A0} \cdot x + \mathrm{FD} \end{aligned}$$