

TH Brandenburg
Online Studiengang IT Sicherheit
Fachbereich Informatik und Medien
Algorithmen und Datenstrukturen
Prof. Dr. rer. nat. Ulrich Baum

Einsendeaufgabe 2
Sommersemester 2022
Abgabetermin 4. April 2022

Mara Schulke
Matrikel-Nr. 20215853

Einsendeaufgabe 2

2.1 OTP-Verschlüsselung

(a)

$$\begin{aligned}
 M &= 11011110101011011011111011101111_2 \\
 K &= 11001010111111110101110101011110_2 \\
 C &= M_2 \oplus K_2 \\
 &= 11011110101011011011111011101111_2 \\
 &\oplus 11001010111111110101110101011110_2 \\
 &= 00010100010100110000010001010001_2 \\
 &= 145300451_{16}
 \end{aligned}$$

(b)

$$\begin{aligned}
 C &= 3522988314_{10} \\
 &= 11010001111111001000100100011010_2 \\
 K &= 11223344_{16} \\
 &= 00010001001000100011001101000100_2 \\
 M &= C_2 \oplus K_2 \\
 &= 11010001111111001000100100011010_2 \\
 &\oplus 00010001001000100011001101000100_2 \\
 &= 11000000110111101011101001011110_2 \\
 &= C0DEBA5E_{16}
 \end{aligned}$$

2.2 Square-and-Multiply

$$\begin{aligned}
 y &= 100000001_2 \\
 a_0 &= x & (y_0 \text{ muss } 1 \text{ sein wenn } y > 0 \rightarrow a = x) \\
 a_1 &= x^2 & (y_1 \% 2 = 0 \rightarrow a^2) \\
 a_2 &= x^4 & (y_2 \% 2 = 0 \rightarrow a^2) \\
 a_3 &= x^8 & (y_3 \% 2 = 0 \rightarrow a^2) \\
 a_4 &= x^{16} & (y_4 \% 2 = 0 \rightarrow a^2) \\
 a_5 &= x^{32} & (y_5 \% 2 = 0 \rightarrow a^2) \\
 a_6 &= x^{64} & (y_6 \% 2 = 0 \rightarrow a^2) \\
 a_7 &= x^{128} & (y_7 \% 2 = 0 \rightarrow a^2) \\
 a_8 &= x^{257} & (y_8 \% 2 = 1 \rightarrow a^2 * x) \\
 &\rightarrow 9 \text{ Multiplikationen}
 \end{aligned}$$