Grundlagen Informations Sicherheit
Übungsblatt 01

Max Kurz (3265240) Mohamed Barbouchi (3233706)
Daniel Kurtz 123456

Problem 1

a)

$D()$	A	B	C
k_1	a	b	c
k_2	c	a	b
k_3	b	c	a

b)

$D()$	A	B	C
k_1	a	b	c
k_2	b	a	c
k_3	a	b	c

c) Klappt nicht, da $\forall x \in X, k \in K : D(E(x,k),k) = x$ gelten muss und wir hier aber $D(A,k_1) = a$ und $D(A,k_1) = c$ bekommen. Die Entschlüsslelung ist also nicht eindeutig.

Problem 2

Das Wort lautet: Hitchhiker Man wandelt die Zahlen in Binär um, und xort die beiden Strings. Das Ergebnis wird wieder in Dezimal umgewandelt.

Problem 3

a) Sei $x \in \{0,1\}^l$, dann gilt $x^l \oplus x^l \oplus x^l = x^l \oplus 0^l$ wobei 0^l hier die Identität ist. Für die Identität gilt: $x \oplus 1_m = x$.

Algorithm 1 $D(Y)$

1: $z_1.\texttt{concat}(z_2) := Y$ mit $|z_1| = |z_2|$
2: $l := |z_2|$
3: $r := z_2 \oplus 1^l$
4: `return` r

Algorithm 2 Attack

b)
1: Let $x \in \{0^l\}$ and $y \in \{1^l\}$
2: `send`(x)
3: `send`(y)
4: `receive`(w)
5: `if`$(w == 0^l)$ $b = 1$ `else` $b = 0$
6: `return` b

Die Wahrscheinlichkeit für den Angreifer so die richtige Nachricht zu erkennen und das passende b zurückzugeben liegt bei 1. Siehe Aufgabe a).