Grundlagen der Informationssicherheit/Datensicherheit, Blatt 1

Lukas Baur, 3131138
Felix Bühler, 2973410
Marco Hildenbrand, 3137242

30. Oktober 2017

Problem 1

a)

Ja.

b)

Ja. Da hier aber 'c' immer eindeutig auf 'C' gemapped wird, ist dies kein sicheres Verschlüsselungsschema.

c)

Nein. Hier besteht ein großes Problem, egal welcher Key = K_X gewählt wird, wird es immer ein Problem mit 'a' oder 'c' geben. Wenn die Daten verschlüsselt werden, werden beide auf den selben Buchstaben gemapped. Beim entschlüsseln hat man das Problem, dass man nicht exakt weiß welcher Buchstabe ursprünglich an dieser Stelle war. Es ist also nicht möglich, die Daten wieder exakt herzustellen, wie sie früher waren.

Problem 2

ASCII (Base 256) = Hitchhiker

y =		96	c4	ca	8c	4b	2a	7e	79	c5	8c
k =	$\oplus$	de	ad	be	ef	23	42	17	12	a0	fe
x =		48	69	74	63	68	68	69	6b	65	72

Problem 3

a)

```
function D(y, k)
        y1 = y[l, 2l-1]
        x = y1 XOR 1^l
        return x;
end function
```

b)