Grundlagen der Informationssicherheit/Datensicherheit, Blatt 1

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

6. November 2017

Problem 1

a)

D(x, k)	A	B	C
K_1	a	b	c
K_2	c	a	b
K_3	b	c	a

b)

Ja. Da hier aber 'c' immer eindeutig auf 'C' gemapped wird, ist dies kein sicheres Verschlüsselungsschema. Gleichzeitig sind K_1 und K_3 indentische Keys.

D(x, k)	A	B	C
K_1	a	b	c
K_2	b	a	c
K_3	a	b	c

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. D ist hier nicht injektiv.

Problem 2

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

ASCII (Base 256) = Hitchhiker

Problem 3

a)

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

$\nexists : D(E(x,k),k) = x$

$D((r \oplus k || x \oplus 1^l), k) = x$
$(x \oplus 1^l) \oplus 1^l = x$
$x \oplus 0^l = x$
$x = x$ □

b)

Bei der Verschlüsselung wird nur die Nachricht invertiert und mit einem 'zufälligen' Bitstring(vorne) aufgefüllt. Eine Invertierung ist keine Verschlüsselung.

Game:

1. Definiere $Z_0 := 1^l$
   Definiere $Z_1 := 0^l$
2. Sende an Alice (Z_0, Z_1) und erhalte c
3. Z_0' :=Verschlüssele Z_0 von Alice
4. Vergleiche die letzen l bits von Z_0' und c bei Gleichheit gib 0 zurück, ansonsten 1.