## 13.17 Aufgabe: Betriebsmodi von Blockchiffren an einem Beispiel

## a)

Klartext „1A2B“

IV0 = „0“ =0000
Blocklänge 4

| M | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E(K, M) | 8 | 7 | 6 | 5 | 1 | 2 | 3 | 4 | F | E | D | C | 0 | 9 | A | B |

+ steht für XOR

M1=1=0001

IV1=0001 + 0000=0001=1

C1=E(K,1)=7

M2=A=1010

IV2= 1010 + 0001= 1011=B

C2=E(K,B)=C

M3=2=0010

IV3=0010 + 1011= 1001=9

C3=E(K,9)=E

M4=B=1011

IV4= 1011 + 1001=0010=2

C4=E(K, 2)=6

➔ C=7CE6

+

b)

Entschlüsseln Sie C=“EFFE“ mittels ECB.

| M | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E(K, M) | 8 | 7 | 6 | 5 | 1 | 2 | 3 | 4 | F | E | D | C | 0 | 9 | A | B |

E(K,M)=M

C1=E -> 9

C2=F->8

C3=F->8

C4=E→9

C=9889

C)

Verschlüsseln Sie den Klartext „AFFE“ im CTR-Mode mit IV=14.
IV=14? Geht nicht. Blocklänge beträgt 4. Ich nehme an das IV nicht Hexadezimal ist sondern dezimal.

Bzw IV=E

In Binär IV=1110

E(K, 1111)=B -> B+A= 1011 + 1010=0001

E(K, 0001)=7 -> 7 + F= 0111 + 1111=1000

E(K,0010)=6 ->6 + F = 0110 +1111 =1001

E(K, 0011)=5 -> 5 + E = 0101 + 1110 = 1011

Verschlüsselt: 189B