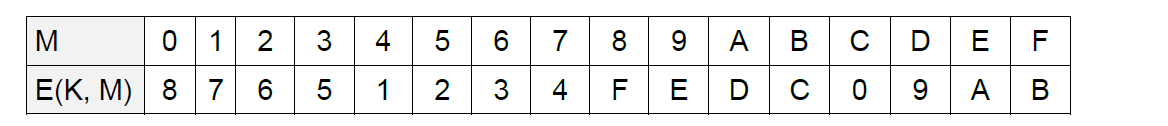
**13.17 Aufgabe: Betriebsmodi von Blockchiffren an einem Beispiel**

**a)**

Klartext „1A2B“

IV0 = „0“ =0000

Blocklänge 4



+ steht für XOR

M1=1=0001

IV1=0001 + 0000=0001=1

C1=E(K,1)=7

M2=A=1010

IV2= 0111 + 1010´= 1001=9

C2=E(K,B)=C

M3=2=0010

IV3=1001+ 0010= 1100

C3=E(K,9)=C

M4=B=1011

IV4= 1100 + 1011=0111

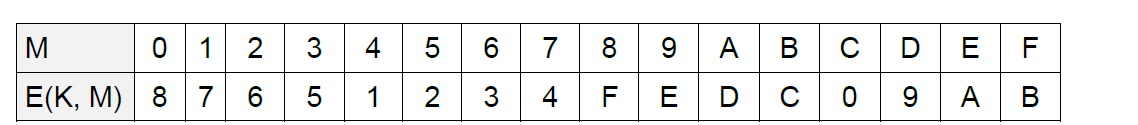
C4=E(K, 2)=4

* C=79C4

\*Hier richtig Korrigiert vgl PDF falsch

b)

Entschlüsseln Sie C=“EFFE“ mittels ECB.



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

Übung

14 dezimal

1010 + E(K,(14+1)mod16)=0001=1

1111 + E(K, (14+2) mod 16)=0111=7

1111 + E(K, (14+3) mod 16=1000=8

8