13.31 Aufgabe: CBC-MAC

Für einen ausgewählten Schlüssel K sei die Blockchiffre E(K, M) mit der Blocklänge 4 Bit (Hexadezimal codiert) durch die folgende Tabelle gegeben. Der IV ist 0x9 für alle Teilaufgaben. K und IV sind dem Sender und Empfänger bekannt und müssen nicht mit übertragen werden.

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

a) Wie lautet der zur Nachricht 0xABBA gehörende CBC-MAC?
b) Sie erhalten die Nachricht 0xEFFE und den CBC-MAC 0x6. Wurde die Nachricht manipuliert?
c) Sie erhalten die Nachricht 0xFADE und den CBC-MAC 0x5. Wurde die Nachricht manipuliert?

a)

ABBA= 1010 1011 1011 1010

IV=9= 1001

1010

1001

0011=3

C0=E(K,3)= 5=0101

1011

0101

1110=14=0xE=

C1=E(K,E)=C=1100

1011

1100

0111=7

C2=E(k , 7)=9=1001

1010

1001

0011=3

C3=E(k, 3)=5

⇨ CBC-MAC C3=5, für Nachricht ABBA

b)

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

0xEFFE
CBC-MAC 0x6.
d.h. c4=6 müsste gelten
EFFE= 1110 1111 1111 1110
IV=9= 1001

1110 + 1001=0111=7
C1=E(k , 7)=9=1001

1111+1001=0110=6
C2=E(k, 6) =B=1011

1111+1011=0100=4
C3=E(k, 4)=1=0001

1110+0001=1111=F
C4=E(k,F)=6

=>C4=6 => Stimmt mit CBC-MAC überein, die Nachricht ist nicht manipuliert

c)

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

0xFADE
IV=9= 1001

CBC-MAC 0x5
d.h. C4=5 wenn nicht manipuliert

FADE= 1111 1010 1101 1110

1111+1001=0110=6

C1=E(k, 6) =B=1011

1010+1011=0001=1

C2=E(k,1)=4=0100

1101+0100=1001=9

C3=E(k,9)=0=0000

1110 + 0000=1110=E

C4=E(k, E)=C

=>C4!=5, die Nachricht wurde Manipuliert! Ich → ☹