13.28 Aufgabe: Merkle-Damgård Konstruktion

Gegeben sei die Bitfolge Y = 11110 und die „Einwegfunkton“ F mit

$$F: \{0,1\}^4 \rightarrow \{0,1\}^2 \text{ und } F(x_1, x_2, x_3, x_4) = (x_1 \oplus x_4, x_2 \oplus x_3)$$

Die Blocklänge ist 2. Der Initialisierungsvektor H_0 ist 10. Der Padding-Wert ist 0.

a) Berechnen Sie den Hashwert H(Y) nach der Merkle-Damgård Konstruktion.
b) Geben Sie ein Beispiel für eine Kollision von H an.

a)

Y erweitern mit Padding : Y= 11 11 00

\+ steht für XOR Zeichen

K=3

y1= 11

y2=11

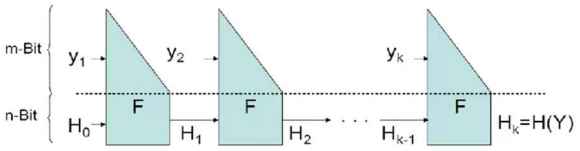
y3=00

Y=(y1,y2,y3)

H1= f(y1, H0)=(1+0 , 1+1)=(1,0)

H2= f(y2, H1)=(1+0 , 1+1)=(1,0)

H3=f(y3, H2) = (0+0, 0+1)=(0,1)



Der Hashwert ist Hk=H3=H(Y)=01

b)

Wir müssen finden ein H(x) so das gilt H(x)=H(y) mit x!=y

Sei X= 10 00 10

Dann

H1= f(x1, H0)=(1+0 , 0+1)=(1,1)

H2= f(x2, H1)=(0+1 , 0+1)=(1,1)

H3=f(x3, H2) = (1+1, 0+1)=(0,1)

Hk=H3=H(X)

Es gilt: H(X)=H(Y) mit X!=Y => Kollision mit X= 10 00 10