

ADATBIZTONSÁG KIS-ZH/1

2009. március 16.

1. Tekintsük a következő rejtjelező kódolást: nyílt üzenetek tere $X=\{a,b\}$, kulcsok tere $K=\{k_1,k_2,k_3,k_4,k_5\}$, rejtett üzenetek tere $Y=\{1,2,3,4,5\}$. A kódolást a következő mátrix írja le:

Pl. $E_{k_3}(a)=3$. A kulcs valószínűség-eloszlása $P_K=\{2/5, 1/5, 1/5, 1/10, 1/10\}$, az üzenet valószínűség-eloszlása $P_X=\{1/3, 2/3\}$.

- a.) Tökéletes rejtjelezés definíciója. (2p)
- b.) Tökéletes-e a fenti rejtjelezés? (3p)

2.

- a.) Üzenet-integritás védelem célja. (1p)
- b.) Biztonságos kulcsos hash módszer definiálása. (1p)
- c.) Kulcsprefix módszer biztonsága elemzése iteratív hash függvény esetén. (3p)

3.

- a.) Ütközésmentes hash függvény definíciója (1p)
- b.) Digitális aláírás alkalmazásban, milyen biztonsági problémát okoz, ha a hash függvény nem ütközésmentes (1p)
- c.) DM padding definiálása. A kapcsolatos tétel kimondása. (3p)

Pontozás: 1: ≤ 7 p, 2: 8-9, 3:10-11, 4:12-13, 5: 14-15

Adatbiztonság kis-ZH eredmények

2009. március 16.

(Ügyeljen a pontos fogalomhasználatra, pontos, formális definíciókra, részletes indoklásokra!)

1.

a.)

b.)

2.

a.)

b.)

c.)

3.

a.)

b.)

c.)

Név:

.....

Neptun

kód:

Adatbiztonság kis-ZH eredmények

2009. március 16.

(Ügyeljen a pontos fogalomhasználatra, pontos, formális definíciókra, részletes indoklásokra!)

1.) Nem. Pl. $P(Y=1|X=a)=2/5 \neq P(Y=1|X=b)=1/5$, azaz X és Y nem független

1.)

1a.) $a = c \cdot (k-1)^{-1} \pmod{29}$, $b = [d - c \cdot (k-1)^{-1}] \cdot k^{-2} \pmod{29}$,

$k \neq 0,1$

1b.) $k^{-1} = 10$, $(k-1)^{-1} = 15$, $[a,b]=[18,23]$

1c.) $[a=1, b \text{ tetszőleges}]$ nyílt szöveg választása esetén $k=c+1$.