

ADATBIZTONSÁG KIS-ZH/2

2009. március 16.

1.

Tekintsük az alábbi rejtjelezést: $a, b, c, d, k \in \{0,1,2,\dots,28\}$

nyílt szöveg: $x=[a, b]$,

rejtett szöveg: $y=[c, d]$, ahol $c=(k \cdot a - a) \bmod 29$, $d=(a + b \cdot k^2) \bmod 29$

kulcs: k

- a.) Van-e megszorítás a lehetséges kulcsokra? (1p)
- b.) Adja meg a dekódoló transzformációt! (2p)
- c.) Dekódolja az $y=[7,22]$ rejtett blokkot $k=3$ kulcs esetén. (2p)

2.

- a.) Kulcskonfirmáció definíciója. Adjon meg módszert kulcskonfirmációra. (2p)
- b.) Diffie-Hellman kulcscsere protokoll leírása és biztonsága. (3p)

3

- a.) CBC rejtjelezési mód definíciója (blokkséma vagy formula) (2p)
- b.) Kivág és beszúr (cut and paste) támadás definiálása és elemzése. (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.)

c.)

2.

a.)

b.)

3.

a.)

b.)

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
($H(K) \geq H(X)$ csak szükséges, de nem elégséges feltétel)

1.)

1a.) $a = c \cdot (k-1)^{-1} \bmod 29$, $b = [d - c \cdot (k-1)^{-1}] \cdot k^{-2} \bmod 29$,
 $k \neq 0,1$

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

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