# 1. izpit iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

11. junij 2014

REŠITVE

Priimek in ime: ______________________

Vpisna št.: ____________ Vrsta: ____________ Kolona: ____________

1. Prestregli smo kriptogram

$$0,1,1,0,1,1,1,0,1,0,1,1,1,0,0,1,1,1,0,1,$$

ki je dobljen s seštevanjem besedila (v dvojiškem zapisu) in izhoda LFSR po modulu 2. Uganemo, da se besedilo začne z nizom

$$1,0,0,1,1,1,1,0,0,1,0,0.$$

Odkodirajte še preostanek besedila (pri predpostavki, da ima LFSR, ki vrne ustrezno zaporedje ključev, najmanjšo možno stopnjo).

c = 01101110 1011 ‖ 1 00 111 0 1
b = 1 0011110 0100 ‖ 1 00 100 1 0
z = 11110000 1111 ‖ 0000 1111

Preostanek besedila je $\boxed{10010010}$

4 zaporedne ničle: red LFSR je vsaj 5

Sistem enačb

$$z_{j+5} = c_0 z_{j+4} + c_1 z_{j+3} + c_2 z_{j+2} + c_3 z_{j+1} + c_4 z_j$$

$$\begin{array}{ccccc|c} c_4 & c_3 & c_2 & c_1 & c_0 & \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}$$

$c_1 = c_2 + c_3 + c_4 = 0$
$c_2 = c_3 + c_4 = 0$
$c_3 = 1$
$c_4 = 1$
$\Rightarrow c_0 = 1$

$$z_{j+5} = z_{j+4} + z_{j+3} + z_j$$

$$z = 1111\ 0000\ \underbrace{1111|0}_{5\text{x jih ponovi}}$$

2. Za kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ je $\mathcal{B} = \{x, y, z, w\}$, $\mathcal{C} = \{X, Y, Z, W\}$ in $\mathcal{K} = \{k_1, k_2, k_3\}$, družina kodirnih funkcij pa je podana s spodnjo tabelo:

| | $x$ | $y$ | $z$ | $w$ |
|---|---|---|---|---|
| $k_1$ | $Z$ | $W$ | $Y$ | $X$ |
| $k_2$ | $Z$ | $X$ | $W$ | $Y$ |
| $k_3$ | $W$ | $Z$ | $X$ | $Y$ |

Kriptosistem $\mathcal{S}$ opremimo še z verjetnostnimi porazdelitvami $B$, $C$ in $K$ na množicah $\mathcal{B}$, $\mathcal{C}$ in $\mathcal{K}$: $P[B = x] = 0.25$, $P[B = y] = 0.3$, $P[B = z] = 0.15$, $P[B = w] = 0.3$, $P[K = k_1] = P[K = k_3] = 0.25$, $P[K = k_2] = 0.5$. Predpostavimo, da sta $B$ in $K$ neodvisni.

(a) Poiščite družino dekodirnih funkcij.

(b) Izračunajte $P[C = X]$ in $P[C = Z]$.

(c) Ali ima kriptosistem $\mathcal{S}$ lastnost popolne tajnosti?

a)

| $D$ | $X$ | $Y$ | $Z$ | $W$ |
|---|---|---|---|---|
| $k_1$ | $w$ | $z$ | $x$ | $y$ |
| $k_2$ | $y$ | $w$ | $x$ | $z$ |
| $k_3$ | $z$ | $w$ | $y$ | $x$ |

b) $P(C=X) = P(C=X \mid B=x) \cdot P(B=x) +$
$P(C=X \mid B=y) \cdot P(B=y) +$
$P(C=X \mid B=z) \cdot P(B=z) +$
$P(C=X \mid B=w) \cdot P(B=w) =$

$= 0 + P(K=k_2) \cdot 0.3 + P(K=k_3) 0.15 + P(K=k_1) \cdot 0.3$
$= 0.5 \cdot 0.3 + 0.25 \cdot 0.15 + 0.25 \cdot 0.3 = 0.2625$

$$P(C=Z) = \sum_{b \in \mathcal{B}} P(C=Z \mid B=b) \cdot P(B=b) =$$

$$= \underbrace{P(C=Z \mid B=x)}_{k_1, k_2 \;\; 0.75} \cdot \underset{0.25}{P(B=x)} + \underbrace{P(C=Z \mid B=y)}_{k_3 \;\; 0.25} \underset{0.3}{\ } = 0.2625$$

c)

? $P(C=X) \overset{?}{=} P(C=X \mid B=x)$ Ni CPT

$\underset{0.2625}{\parallel} \neq \underset{0}{\parallel}$

Hitreje: $|\mathcal{K}| < |\mathcal{B}| \Rightarrow$ ni PT

3. Alenka in Bojan bi se rada dogovorila za skupen ključ po ne-varnem kanalu s pomočjo Diffie-Hellmanovega algoritma. Izbrala sta praštevilo $p = 239$ in bazo $\alpha = 7$

   (a) Preverite, da je $\alpha$ generator grupe $\mathbb{Z}_{239}^*$.

   (b) Alenka je izbrala naključno število $a = 10$ in Bojanu poslala $A = \alpha^a$. Bojan je izbral naključno število $b$ in Alenki poslal $B = \alpha^b = \cancel{110}$. Izračunajte skupni ključ!

2

a)

$$|\mathbb{Z}_{239}^*| = 238 = 2 \cdot 7 \cdot 17$$

$$\frac{238}{2} = 119$$

$$\frac{238}{7} = 34$$

$$\frac{238}{17} = 14$$

Preveriti je treba:

$$7^{14} \not\equiv 1 \pmod{239}$$
$$7^{34} \not\equiv 1$$
$$7^{119} \not\equiv 1$$

$$7^2 = 49 \pmod{239}$$
$$7^4 \equiv 11$$
$$7^8 \equiv 121$$
$$7^{16} \equiv 62$$
$$7^{32} \equiv 20$$
$$7^{64} \equiv 161$$

$$7^{14} = 7^8 \cdot 7^4 \cdot 7^2 \equiv 211 \not\equiv 1 \pmod{239}$$
$$7^{34} = 7^{32} \cdot 7^2 \equiv 24 \not\equiv 1$$
$$7^{119} = 7^{64} \cdot 7^{32} \cdot 7^{16} \cdot 7^4 \cdot 7^2 \cdot 7 \equiv 238 \not\equiv 1$$

$\Rightarrow$ 7 je generator $\mathbb{Z}_{239}^*$

b) $$K = (\alpha^b)^a = 2^{10} \equiv 68 \pmod{239}$$

4. Kodne besede dvojiškega kode dobimo iz sporočil dolžine $k$ tako, da jim dodamo 5 "parnostnih bitov". ~~Poiščite~~ Če je lin., se največjega ... največji $k$, da bo takšen kod lahko popravil 2 napaki. Sestavite tudi primer takšnega koda (podajte ga z nadzorno matriko).

$n = k + 5$ 2 napaki: $d \geq 5$

~~Kaj če kod ni linearen:~~

~~00 | 00000~~
~~01 | 11110~~
~~10 | 01111~~ $\}$ ~~$d=4$~~
~~11 |~~

Hammingova meja:

$$2^k \leq \frac{2^n}{1+n+\binom{n}{2}}$$

$$2^{n-5} \leq \frac{2^n}{1+n+\binom{n}{2}}$$

$$1+n+\binom{n}{2} \leq 2^5 = 32$$

$n = 6$ : $1 + 6 + \frac{6\cdot 5}{2} = 22 \leq 32$

$n = 7$ : $1 + 7 + \frac{7\cdot 6}{2} = 29 \leq 32 \leftarrow$

$n = 8$ : $1 + 8 + \frac{8\cdot 7}{2} = 37 \nleq 32$

$n$ največ 7

$n = 7 \Rightarrow k = 2$

Ali tak kod obstaja? Poljubni 4 stolpci lin. neodvisni $\to$ v prvih 4 stolpcih vsaj po 4 enke takšna stolpca pa se morata ~~razlikovati~~ razlikovati vsaj na ~~dveh~~ treh mestih tam imamo z dvema stolpcema iz zadnjega dela vsoto 0 $\to$ ⊥

$$H = \left[\begin{array}{cc|ccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$n = 6,\ k = 1$; takšen kod pa obstaja; poljubnih 5 stolpcev je lin. neodv.

$$H = \left[\begin{array}{c|c} 1 & \\ 1 & \\ 1 & I_5 \\ 1 & \\ 1 & \end{array}\right]$$

Kod ima samo dve besedi:

000000
111111