Teorija kodiranja in kriptografija 2013/2014

1. Kodiranje sporočil

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 25. 2. 2014

Kriptografija

Kriptografija je veda o varni komunikaciji po nezaščitenem kanalu.

Pošiljatelj pred oddajo sporočilo šifrira (kodira). Prejemnik prejeto sporočilo odšifrira (dekodira).

Pogoj za tajnost komunikacije: nasprotnik ne sme poznati dekodirnega ključa.

Kriptosistem

Kriptosistem (kodirna shema, šifra) je peterka $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ za katero velja:

1. $\mathcal{B}$ je končna množica besedil (čistopisov) (angl. *plaintext*),
2. $\mathcal{C}$ je končna množica kriptogramov (tajnopisov) (angl. *ciphertext*),
3. $\mathcal{K}$ je končna množica ključev,
4. $\mathcal{E} = \{E_k : \mathcal{B} \to \mathcal{C};\ k \in \mathcal{K}\}$ je družina kodirnih funkcij,
5. $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{B};\ k \in \mathcal{K}\}$ je družina dekodirnih funkcij.
6. Za vsak $e \in \mathcal{K}$ obstaja $d \in \mathcal{K}$ da velja

$$D_d(E_e(b)) = b \quad \text{za vsak } b \in \mathcal{B}.$$

Trditev

Vsaka kodirna funkcija $E_k \in \mathcal{E}$ je injektivna.

1.1 Nekaj klasičnih kriptosistemov

Kriptografija ima dolgo in zanimivo zgodovino.

- David Kahn: The Codebreakers (The Story of Secret Writing)
- Simon Singh: The Code Book (v slovenščini: Knjiga šifer)

Cezarjeva šifra

Šifra s pomikom, angl. shift cipher.

Znake a, b, c,..., ž izenačimo s števili 0, 1, 2,..., 24.

- $\mathcal{B} = \mathcal{C} = \mathcal{K} = \{0, 1, \ldots, 24\} = \mathbb{Z}_{25}$,
- Kodiranje: $E_k(b) \equiv b + k \pmod{25}$
  Dekodiranje: $D_k(c) \equiv c - k \pmod{25}$
  Računamo v Abelovi grupi $(\mathbb{Z}_{25}, +)$.

Preverimo zahtevo 6: $d = e$,

$$D_e(E_e(b)) \equiv (b + e) - e \pmod{25} \equiv b \pmod{25}.$$

Kerckhoffovo načelo

Držali se bomo **Kerckhoffovega načela**,
ki pravi, da

nasprotnik pozna kriptosistem oziroma algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.

Torej, varnost temelji na tajnosti ključev, ne pa na tajnosti sistema (“security by obscurity”, na primer GSM: A5/1).

Izčrpno iskanje ključev (angl. exhaustive key search)

Podatki: $b \in \mathcal{B}, c \in \mathcal{C}$ za kriptosistem $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

Iščemo : $k \in \mathcal{K}$, za katerega je $E_k(b) = c$

Postopek :

za vsak $k \in \mathcal{K}$

    če velja $E_k(b) = c$

        izpiši k

Napad z izčrpnim iskanjem ključev ne deluje, če je $|\mathcal{K}|$ dovolj veliko: za srednjeročno varnost vsaj 2^{128} ključev; 2^{80} ključev je na meji zmogljivosti.

Kriptosistem je razbit, če lahko ključ najdemo “dosti hitreje” kot s preverjanjem vseh ključev.

Substitucijska šifra

- $\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}, \quad \mathcal{K} = S(\mathbb{Z}_{25})$ (permutacije množice $\mathbb{Z}_{25}$)
- ključ $\pi \in \mathcal{K}$
  Kodiranje: $E_\pi(b) = \pi(b)$
  Dekodiranje: $D_\pi(b) = \pi^{-1}(b)$.

Preverimo zahtevo 6: kodirnemu ključu π pripada dekodirni ključ π.

$$D_\pi(E_\pi(b)) = \pi^{-1}(\pi(b)) = b.$$

Opomba: Cezarjeva šifra je poseben primer substitucijske, ki uporabi le 25 od 25! permutacij.

Ali je 25! veliko?

$25! \approx 1.55 \cdot 10^{25} \approx 2^{84}$
1 leto $= 365 \cdot 24 \cdot 3600s \approx 3.1 \cdot 10^7 s.$

Najhitrejši superračunalnik 2013:
Tianhe-2 zmore 33.86 PFLOPS

peta: 10^{15}
FLOPS: FLoating Point Operations Per Second

Če bi za pregled ključa zadostoval čas ene operacije, bi za pregled vseh ključev potrebovali

$$\frac{1.55 \cdot 10^{25}\ op}{33.86 \cdot 10^{15}\ op/s} \approx 4.6 \cdot 10^8 s \approx 14.5 \text{ let.}$$

S frekvenčno analizo lahko ključ najdemo veliko hitreje (vaje).