Teorija kodiranja in kriptografija 2013/2014

Tokovne šifre

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 18. 3. 2014

Vsebina

- Tokovne šifre
- LFSR

Tokovne šifre

Besedilo b razdelimo na bloke: $b = b_1 b_2 \dots b_t \in \mathcal{B}^t$.

Imamo zaporedje (tok) ključev: $z_1, z_2, z_3, \cdots \in \mathcal{K}$.

Kodiranje:

za $i = 1, 2, \dots t$ **ponovi**

$$c_j = E_{z_j}(b_j)$$

$c = c_1 c_2 \dots c_t \in \mathcal{C}^t$

Dekodiranje:

za $j = 1, 2, \dots t$ **ponovi**

$$b_j = D_{z_j}(c_j)$$

$b = b_1 b_2 \dots b_t \in \mathcal{B}^t$

Aditivne tokovne šifre

Naj bo $(G, +)$ grupa, $\mathcal{B} = \mathcal{C} = \mathcal{K}$.
Naj bo $z_1, z_2, z_3, \ldots$ tok ključev. Potem je

Kodiranje:

$$E_{z_i}(b_i) = b_i + z_i \quad (\text{v } G)$$

Dekodiranje:

$$D_{z_i}(c_i) = c_i - z_i \quad (\text{v } G)$$

Opomba: večina tokovnih šifer v uporabi je aditivnih.

Samokodirna šifra (autokey cipher)

Izumil jo je Blaise de Vigenère v 16. stoletju.

$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$.

Začetni ključ izberemo, $z_1 \in \mathbb{Z}_{26}$
$z_i = b_{i-1}$ za $i > 1$

Kodiranje:

$$E_{z_i}(b_i) = b_i + z_i \equiv \begin{cases} b_1 + z_1 \pmod{26} & \text{če } i = 1 \\ b_i + b_{i-1} \pmod{26} & \text{sicer} \end{cases}$$

Dekodiranje:

$$D_{z_i}(c_i) = c_i - z_i \equiv \begin{cases} c_1 - z_1 \pmod{26} & \text{če } i = 1 \\ c_i - b_{i-1} \pmod{26} & \text{sicer} \end{cases}$$

Slabost: za dekodiranje je treba preizkusiti samo 26 začetnih ključev. Popravek: izberemo daljši začetni ključ.

Zgled

Naj bo $z_1 = 8$.

Kodirajmo: ”jutri v napad”

Lastnosti tokovnih šifer

Tokovna šifra je **sinhrona**, če je zaporedje ključev odvisno le od začetnega ključa.

Torej: samokodirna šifra ni sinhrona.

Tokovna šifra je **periodična** s periodo d kadar, je

$$z_{i+d} = z_i \quad \text{za vsak } i \geq 1.$$

Zgled: Vigenèrjeva šifra kot tokovna šifra

Naj bo ključ $k_1 k_2 \ldots k_n$, $k_i \in \mathbb{Z}_{26}$.

Zaporedje ključev je
$z_i = k_i$ za $i = 1, 2, \ldots n$ (začetni ključ)
$z_{i+n} = z_i$ za $i \geq 1$.

Vernamova šifra

Vernamova šifra ali enkratni ščit, *angl. one-time pad* (Gilbert Vernam, 1917, patentiral 1919).

$\mathcal{B} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$,
ključ k iz $\{0,1\}^n$ izberemo naključno.

Kodiranje:

$$E_k(b) = b \oplus k.$$

Dekodiranje:

$$D_k(c) = c \oplus k.$$

To je pravzaprav Vigenèrjeva šifra, le da je ključ enako dolg kot besedilo.

Demonstracija

Pri aditivni tokovni šifri smemo isti ključ uporabiti samo enkrat!
Sicer: $c_1 = b_1 + k$, $c_2 = b_2 + k$ in lahko izračunamo:

$$c_1 - c_2 = b_1 - b_2.$$

Z ugibanjem pogostih besed lahko (ponavadi) rekonstruiramo večji del besedil b_1 in b_2.

Problem izmenjave ključev pri Vernamovi šifri

Da je uporaba Vernamove šifre varna, mora biti ključ enako dolg kot besedilo, popolnoma naključen in vsakič drugačen!

Problem: če je ključ neko smiselno besedilo, je mogoče besedilo (delno) rekonstruirati že iz enega samega kriptograma!

Vprašanje: kako bo prejemnik dobil vsakič nov ključ?
Ali ni to enako težko, kot da mu dostavimo kar celo besedilo?

- Ključ(e) lahko dostavimo vnaprej.
- Za dostavo ključev ni potrebna tolikšna previdnost kot pri besedilu.

Ideja: kratek ključ za generiranje dolgega toka psevdonaključnih bitov.

Zahteve:

- dolga perioda
- dobre statistične lastnosti (ključ mora izgledati čim bolj naključen)
- šibka korelacija med tokom ključa in začetnim ključem
- odpornost na znane napade (in bodoče)
- hitrost in/ali majhna kompleksnost strojne opreme

Linearna rekurzivna šifra (LFSR)

Linearna rekurzivna šifra je sinhrona tokovna šifra, pri kateri je

$$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_s,$$

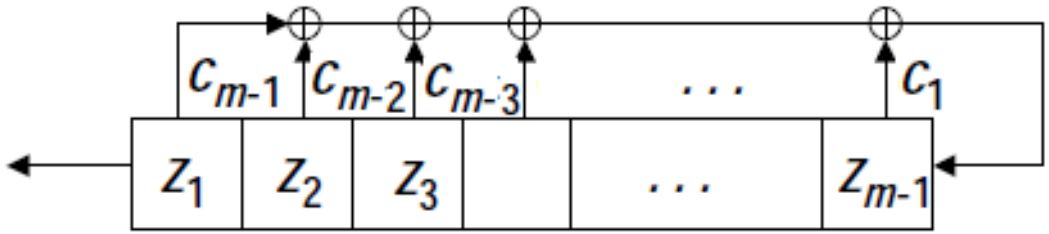
zaporedje ključev pa je določeno z linearno rekurzivno enačbo reda m s konstantnimi koeficienti nad $\mathbb{Z}_s$:

Naj bo $z_1 z_2 \ldots z_m$ začetni ključ. Potem je za $i > m$

$$\begin{aligned} z_i &= c_1 z_{i-1} + c_2 z_{i-2} + \cdots + c_m z_{i-m} \pmod{s} \\ &= \sum_{j=1}^{m} c_j z_{i-j} \pmod{s} \end{aligned}$$

Pomični register z linearno povratno zanko (LFSR)

Linearno rekurzivno šifro enostavno implementiramo v strojni opremi s pomičnim registrom LFSR (*angl.* linear feedback shift register).



- V pomičnem registru je na začetku inicializacijski vektor $(z_1, \ldots, z_m)$ (ključ).
- Na vsakem koraku izpišemo z_1 in nato $z_2, \ldots, z_m$ pomaknemo za eno v levo, 'nov' ključ z_m pa izračunamo.

Lastnosti linearne rekurzivne šifre

- Dobre statistične lastnosti.
- Dolga perioda.
- Nizka linearna zahtevnost.

Zaradi prvih dveh lastnosti se linearne rekurzivne šifre uporablja kot sestavni del ‘pravih’ tokovnih šifer. Linearno zahtevnost izboljšamo z dodajanjem nelinearnih elementov.

Bločne šifre kot tokovne šifre

Zakaj sploh potrebujemo tokovne šifre, če imamo dobre bločne šifre?

- hitrost pri šifriranju velikih količin podatkov (video)
- majhna kompleksnost strojne opreme (pametne kartice)

Nekaj šifer v vsakdanji uporabi

- E0 (bluetooth),
- A5/1, A5/2, A5/3 (GSM)
- RC4 (WEP)

A5/1

- Simetrična šifra za šifriranje telefonskih pogovorov v standardu GSM (1987)
- Algoritem so na začetku skrivali, a je bil 1999 razkrit s pomočjo inverznega inženeringa.
  Pokazalo se je, da ima precej šibkih točk.
- Danes ne velja več za varnega.
  Večina napadov je napadov na protokol: način uporabe šifre A5/1 v GSM.
- Osnovni gradnik: tri LFSR-ji

eSTREAM - natečaj za izbor tokovne šifre

Projekt eSTREAM je bil razpisan na pobudo
ECRYPT (European Network for Exellence in Cryptology)
v začetku leta 2005, rok za oddajo predlogov je bil 29. april 2005.

Prispelo je 34 predlogov, ki so bili vsi sprejeti.
Po treh fazah izbora je komisija izbrala nekaj najboljših šifer.

Rezultati so objavljeni na strani

`http://www.ecrypt.eu.org/stream/`