Teorija kodiranja in kriptografija 2013/2014

Arjana Žitnik

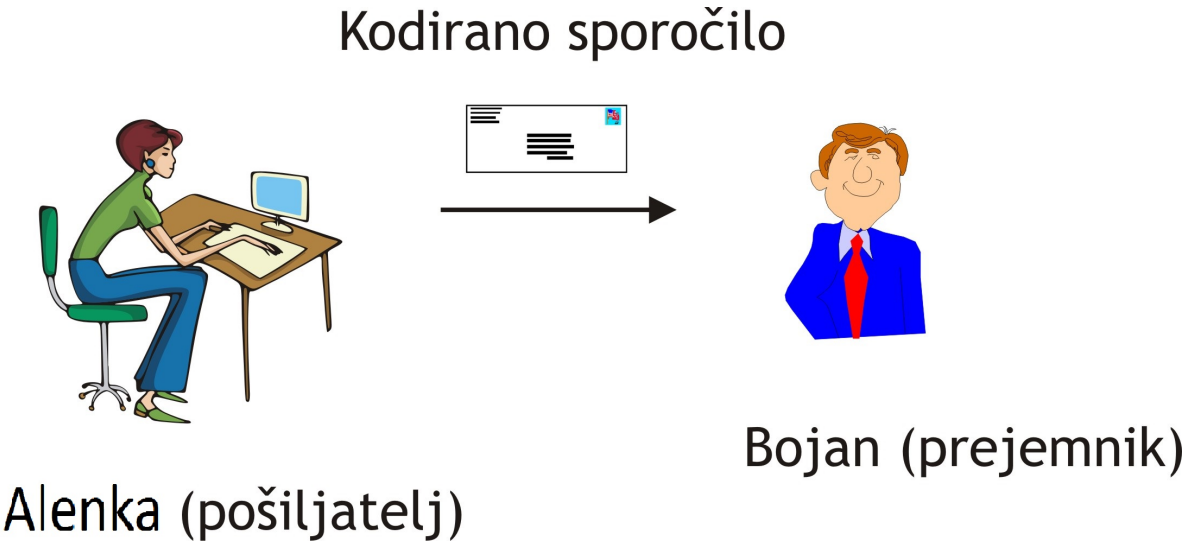
Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 25. 2. 2014

Vsebina

- Kratek pregled snovi
- Cilji predmeta
- Pogoji pri predmetu (glej spletno učilnico)

Kodiranje sporočil pri komunikaciji



Kodiranje: zapis sporočila v spremenjeni obliki.
Kod: sistem pravil za kodiranje.

Cilji (nameni) kodiranja

- ekonomičnost prenosa (sporočilo naj bo čim krajše)
- tajnost sporočila (vsebina sporočila dostopna le prejemniku)
- avtentikacijo pošiljatelja oz. sporočila
- zanesljivost prenosa (možnost odkrivanja/popravljanja napak pri prenosu)

Prvi cilj je dosežen s stiskanjem podatkov (*angl.* data compression), z drugim in tretjim ciljem se ukvarja kriptografija (*angl.* cryptography), s četrtim pa teorija kodiranja v ožjem smislu (kodi, ki popravljajo napake - *angl.* error-correcting codes).

Kaj je kriptografija?

- Kriptografija je veda o komunikaciji v prisotnosti aktivnega napadalca: bere/spreminja podatke.
- Kriptografija je pomemben del širšega področja informacijske in računalniške varnosti, ki opisuje vse preventivne postopke in sredstva s katerimi preprečimo nepooblaščeno uporabo digitalnih podatkov ali sistemov.

Pravilna uporaba kriptografije pomembno prispeva k varnosti celotnega informacijskega sistema. Ni pa ”čudežna tabletka”, z dodatkom katere bi postal celoten sistem varen. Sistem je varen le toliko, kolikor je varen njegov najšibkejši člen.

S kriptografijo se srečujemo vsak dan...

1. varna komunikacija
   - splet: HTTPS
   - brezžična komunikacija: WPA2, GSM, Bluetooth
2. šifriranje datotek na disku: EFS, TrueCrypt
3. zaščita vsebine (DVD, Blu-ray): CSS, AACS
4. overjanje uporabnikov
5. ...

Cilji kriptografije

1. zasebnost/zaupnost/tajnost
2. celovitost podatkov
3. overjanje
4. preprečevanje nepriznavanja
5. drugi kriptografski protokoli

Torej: Kriptografija je več kot samo šifriranje (enkripcija).

Zasebnost/zaupnost/tajnost

- Želimo doseči varovanje informacij pred tistimi, ki jim vpogled ni dovoljen,
- to dosežemo s šifriranjem.
- Uporaba: zaupni podatki v vladah/vojski/podjetjih, podatkovne baze,

Celovitost podatkov

- Zagotovilo, da informacija ni bila spremenjena z nedovoljenimi sredstvi (neavtoriziranimi sredstvi).
- Nimamo zagotovila, da je informacija prišla od prave osebe in je bila izdana v pravem roku: napadalec lahko potrdilo o celovitosti informacije shrani in uporabi kasneje.

Overjanje

- Overjanje sporočila (ali izvora podatkov): potrditev izvora informacij.
- Uporaba: komuniciranje preko spleta, elektronsko plačevanje, pogodbe

Preprečevanje tajenja

Preprečevanje, da bi nekdo zanikal dano obljubo ali storjeno dejanje.

Kako doseči te cilje

- začnemo z osnovnimi gradniki: kriptografiskimi funkcijami ali primitivi
- iz njih zgradimo kriptosisteme,
- nadaljujemo s protokoli za varno komunikacijo

Osnovni gradniki: kriptografski primitivi

- Šifriranje/odšifrirnje. Ločimo
  - simetrične sisteme: ključ za šifriranje je enak ključu za odšifriranje
  - asimetrične sisteme: ključa za šifriranje in odšifriranje sta različna
- Zgoščevalne funkcije: daljše besedilo preslikajo v krajši povzetek. Iz povzetka naj bi bilo težko izračunati originalno besedilo.
- Digitalni podpis

Potrebujemo najprej še:

- Implementacijo primerne aritmetike (končni obsegi...)
- Dobre generatorje (psevdo-)naključnih števil

Protokoli in druge sheme

- Protokoli za dogovor o ključu (komunikacija prek spleta)
- Infrastruktura javnih ključev (certifikatna agencija)
- Delitev skrivnosti.
- Dokazi brez razkritja znanja.

Drugi kriptografski protokoli

S pomočjo osnovnih gradnikov in protokolov lahko zgradimo še kompleksnejše protokole, za kar pa žal ne bomo imeli časa.

- grb/cifra po telefonu
- skupinski podpisi
- poker preko interneta
- shema elektronskih volitev (anonimno glasovanje brez goljufanja)
- (anonimni) elektronski denar

Kodi za popravljanje napak

- Komunikacija preko kanala s šumom, kjer se sporočila delno okvarijo
- Cilj: zanesljivost prenosa
- Kodi za odpravljanje napak: sporočila podaljšamo z namenom, da pri okvari posameznih bitov lahko odpravimo napake
- Teorija: zgornje meje za število besed
- Shannonova teorija: kaj je mogoče doseči
- Primeri kodov za odpravljanje napak: Linearni, Hammingovi, ciklični in Reed-Mullerjevi kodi.

Cilji predmeta

- Spoznati osnovne tehnike sodobne kriptografije in TK
- Spoznati matematične postopke, ki se pri tem uporabijo
- Analiza varnosti
  (kriptoanaliza: ”razbijanje”kriptosistemov)
- Kritičnost pri uporabi komunikacijskih kanalov in računalniških sistemov s stališča informacijske varnosti.