Teorija kodiranja in kriptografija 2013/2014

Kriptoanaliza bločnih šifer

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 4. 3. 2014

Kriptologija

- **Kriptografija**: načrtovanje in uporaba kriptosistemov oziroma protokolov.

- **Kriptoanaliza**: varnostna analiza in “razbijanje” kriptosistemov oziroma protokolov

Kriptoanaliza bločnih šifer

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

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

Cilji nasprotnika

- odkriti dekodirni ključ
- dešifrirati kriptogram
- dešifrirati del kriptograma
- odkriti vsaj neko informacijo o kriptogramu (razen dolžine)

Vrste napadov na kriptosisteme

Pasivni napadi:

1. Napad z golim kriptogramom (*angl.* ciphertext only attack)
   Nasprotnik pozna (enega ali) več kriptogramov.
   - izčrpni pregled vseh ključev
   - statistične metode (frekvenčna analiza...)
2. Napad z znanim besedilom (*angl.* known plaintext)
   Nasprotnik pozna (enega ali) več parov
   (*besedilo*, *kriptogram*).
   - izčrpni pregled vseh ključev
   - izkoriščanje algebraične strukture kriptosistema za izračun ključa

Vrste napadov na kriptosisteme, nadaljevanje

Aktivni napadi:

1. Napad z izbranim besedilom (*angl.* chosen plaintext)
   Nasprotnik ima (začasen dostop) do kodirnega postopka.
   - Generira pare (b, c) za izbrana besedila b in preizkuša domneve.
   - Primer: kriptosistemi z javnim ključem.
2. Napad z izbranim kriptogramom (*angl.* chosen ciphertext)
   Nasprotnik ima (začasen dostop) do dekodirnega postopka.
   - Generira pare (b, c) za izbrane kriptograme c, vendar ne pozna dekodirnega ključa.
   - Primer: kriptosistemi z javnim ključem.
     Nasprotnik pozna kodirni ključ, zato lahko igra vlogo "srednjega moža": prestreza sporočila med A in B in se izdaja za enega izmed njiju.

Zgledi kriptoanalize pri klasičnih šifrah

1. Napad z golim kriptogramom:
   - frekvenčna analiza pri substitucijski šifri,
   - test Kasiskega pri Vigenérjevi šifri,
   - indeks koincidence pri Vigenérjevi šifri.
2. Napad z znanim besedilom:
   - izračun ključa pri Hillovi šifri,
   - izračun ključa pri afini bločni šifri.