Napadi na kriptosustave

– uvod u kriptoanalizu

Cilj: doznati tajni ključ K

Vrste napada prema onome što je na napadaču dostupno:

- Napad s odabranim čistim tekstom (chosen-plaintext attack) – napadač posjeduje neograničene količine parova (M, C), primjer s pametnim karticama
- Napad s odabranim kriptiranim tekstom (chosen-ciphertext attack) – napadač posjeduje po svojoj volji odabrani C i pripadni M (također neograničene količine parova)
- Napad s poznatim čistim tekstom (known-plaintext attack) – napadač posjeduje neke parove (M, C) – odgovaraju mu svi parovi, ali treba mu za napad određena količina parova
- Napad s poznatim kriptiranim tekstom (only cipher-text attack) – napadač posjeduje samo C a pokušava saznati K i M – napadaču je ovaj napad najteže uspješno provesti

Pretraživanje cijelog prostora rješenja

- Napadač pokušava dekriptirati kriptirani tekst sa svim mogućim ključevima
- Najjednostavnija i najsporija vrsta napada
- Nije moguće spriječiti ovaj napad
- Uspješnost svih napada na kriptosustave mjeri se usporedbom s pretraživanjem cijelog prostora
- **Napad koji ima veću složenost od složenosti pretraživanja cijelog prostora smatra se neuspješnim**
- Pretpostavka: napadač ili već ima na raspolaganju čisti tekst ili pretpostavlja da čisti tekst ima neku standardnu strukturu koju je moguće prepoznati. Inače, u slučaju dekriptiranja poruke bez prepoznatljive strukture, napadač nema nikakve šanse da pretraživanjem cijelog prostora sazna koji je pravi ključ.

Pretraživanje pola prostora rješenja

- Može se ostvariti kod mnogih kriptosustava za koje vrijedi simetrija:
    - *C = DES (M, K)* i *C' = DES(M', K')*
        - (X' oznaka za bitovni komplement vrijednosti X)
- Fiksno se postavi jedan bit ključa u '0'
- Za svaki K se uspoređuje dobiveni kriptirani tekst C“ sa C i C' i ukoliko vrijedi jednakost, radi se o K odnosno K'
- Ušteda je vrlo blizu 50%
- Vrijedi i za DES!

- Zaštita od napada pretraživanjem pola prostora: koristiti kriptosustav za koji ne vrijedi navedeni tip simetrije ☺

Napadi na DES

- Bilo kakvim linearnim promjenama u postupku generiranja ključeva i u funkciji F, DES ne postaje otporniji na napade
- Promjena u nelinearnom dijelu algoritma (S tablice) utječe na ranjivost algoritma
- **DES bitno oslabljuje:**
    - Promjena redoslijeda S tablica
    - Slučajno odabrane S tablice
    - Umjesto XOR neka složenija funkcija
- Pristup: analiza pojednostavljenog kriptosustava (s manje iteracija ili rundi, za primjerice DES sa samo tri runde).

Diferencijalna kriptoanaliza

- Eli Biham, Adi Shamir, knjiga Differential analysis of DES-like cryptosystems, 1990.
- **Tehnika kojom se analizira učinak razlike između dva čista teksta na razliku između dva rezultirajuća kriptirana teksta**
- Razlike služe za određivanje vjerojatnosti mogućih ključeva
- Napad s odabranim/poznatim čistim tekstom