Bezbednost podataka i informacija - kriptografija

Vrsta: Seminarski | Broj strana: 30 | Nivo: Kriminalističko policijska akademija

SADRŽAJ :

1. UVOD

Kriptologija je matematički orijentisana naučna disciplina koja daje neophodnu osnovu za ostvarivanje informacione bezbednosti. Cilj ovoga rada je dvojak: (i) da ukaže na kritičnu ulogu
kriptologije kroz ilustrativne primere vezane za GSM sistem mobilne telefonije i (ii) da ilustrativno ukaže na rezultate iz oblasti kriptologije ostvarene u Matematičkom
institutu SANU koje ovu instituciju svrstavaju u red međunarodno priznatih partnera za rešavanje problema informacione bezbednosti.

Kriptografski mehanizmi se realizuju u kriptosistemima. Kriptosistem čine: jedan ili više algoritama šifrovanja,
jedan ili više ključeva, sistem upravljanja ključevima, tekst poruke koji se predaje, algoritmi randomizacije i
pripreme teksta za rad sa algoritmima šifrovanja I šifrovani tekst. Kriptosistemi mogu biti realizovani hardverski, softverski i hardversko-softverski. Konkretna softverska realizacija kriptosistema se naziva kriptopaket.

Osnovna obeležja kriptosistema su:

- relativna bezbednost prenosa informacija (npr.♣
šifrovanje i lozinka)
- postojanje nekakve tajne (poznata učesnicima, a♣
nepoznata protivniku – npr. ključ) i
- u slučaju asimetričnih kriptosistema, bezbednost je♣
osigurana postojanjem treće poverljive strane (TTP
- third trusted party)

Kriptotehnologije su bazne metode transformacija informacija sa kojima raspolaže savremena kriptografija.

U savremenoj kriptografiji razmatraniju se samo kriptotehnike koji se realizuju pomoću kompjutera5. Pomoću njih se grade postojeći kriptografski, odnosno informacioni sistema [5]. Ilustrativna klasifikacija osnovnih kriptografskih alata data je na slici 26. Osnovne kriptotehnologije, na osnovu kojih se formiraju kriptoalgoritmi i kriptografski protokoli su:

- algoritmi šifrovanja (simetrični i asimetrični),•
- izračunavanje heš-funkcije,•
- generisanje elektronskog-digitalnog potpisa i•
- generisanje nizova pseudo-slučajnih brojeva•

2. KRIPTOGRAFSKI POJMOVI I ALGORITMI

Šifrovanje (engl. encryption) obuhvata matematičke postupke modifikacije podataka takve da šifrovane podatke mogu pročitati samo korisnici sa odgovarajućim ključem.

Dešifrovanje (engl. decryption) je obrnut proces: šifrovani podaci se pomoću ključa transformišu u originalnu poruku ili datoteku.

Nulta šifra (engl. null cipher) – u lingvističkoj stenografiji - za skrivanje informacija uz pomoć nekog skupa pravila (na primer: „čitaj svaku četvrtu reč“ ili „čitaj svaki treći znak u svakoj drugoj reči“).

LSB supstitucija – metoda sakrivanja informacije u okviru neke slike, audio ili video datoteke.