Kriptologija i osnovne kriptološke metode

Kriptografija

Kriptografija je nauka koja se bavi metodima očuvanja tajnosti informacija. Kada se lične, finansijske, vojne ili informacije državne bezbednosti prenose sa mesta na mesto, one postaju ranjive na prisluškivačke taktike. Ovakvi problemi se mogu izbeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim neželjenoj strani.

Šifarski sistemi

Šifra i digitalni potpis su kriptografske tehnike koje se koriste da bi se implementirali bezbednosni servisi. Osnovni element koji se koristi naziva se šifarski sistem ili algoritam šifrovanja. Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje.

Šifrovanje

Šifrovanje je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat). Obrnut proces, dešifrovanje, rekonstruiše otvoreni tekst na osnovu šifrata. Prilikom šifrovanja, pored otvorenog teksta, koristi se jedna nezavisna vrednost koja se naziva ključ šifrovanja. Slično, transformacija za dešifrovanje koristi ključ dešifrovanja. Broj simbola koji predstavljaju

ključ (dužina ključa) zavisi od šifarskog sistema i predstavlja jedan od parametara sigurnosti tog sistema.

Kriptoanaliza

Kriptoanaliza je nauka koja se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu šifrata, a bez poznavanja ključa. Uširem smislu, kriptoanaliza obuhvata i proučavanje slabosti kriptografskih elemenata, kao što su, heš funkcije ili protokoli autentifikacije. primer, Različite tehnike kriptoanalize nazivaju se napadi.

Kriptografija mora da obezbedi sledeće:

Integritet ili verodostojnost informacija koje se šifruju se brine o tome da ne dođe do neovlašćene promene informacija, kao što su menjanje informacije, brisanje informacije i zamena informacije. Da bi se osigurala verodostojnost, mora postojati način provere da li je informacija promenjena od strane neovlašćene osobe. Tajnost informacija osigurava da je sadržaj informacije dostupan samo ovlašćenim osobama odnosno samo onim koji poseduju ključ. Postoje brojni načini zaštite tajnosti, počev od fizičke zaštite do matematičkih algoritama koji skrivaju podatke. Provera identiteta korisnici koji počinju komunikaciju se trebaju prvo predstaviti jedan drugome pa tek onda počinju sa razmenom informacija. Nemogućnost izbjegavanja odgovornosti je vrlo važna stavka, pogotovo u novije vreme kada se veliki deo novčanih transakcija obavlja putem interneta.

Kriptovanje

Poruka se može slati putem računarske mreže kao izvorni tekst ili kao nerazumljiv sadržaj koji se naziva šifrovan ili kriptovan tekst. Postupak pomoću koga se izvorni tekst transformiše u šifrovan tekst se naziva kriptovanje. Kriptovanje se koristi da bi se obezbedilo da nijedan korisnik, osim korisnika kome jeporuka namenjena, ne može da sazna sadržaj poruke. Ako neovlašćeni korisnici dođu u posed kriptovanog teksta i vide njegov sadržaj ne mogu pročitati izvorni tekst. Kriptovanje izvornog teksta se obavlja pomoću određenog pravila za kriptovanje odnosno kriptografskog algoritma. -Svaki kriptografski algoritam kao ulazne podatke ima izvorni tekst i ključ a kao izlaz daje kriptovani tekst. Postupak koji omogućava da se od kriptovanog teksta dobije originalni izvorni tekst naziva sedekriptovanje. Dekriptovanje odnosno dešifrovanje predstavlja inverzni postupak od kriptovanja. Kriptovani tekst za koji nije poznat ključ zove se kriptogram.

Razlika između kodiranja i šifrovanja

Treba napomenuti razlike između termina kodiranje i šifrovanje. Pojam kodiranje se odnosi na transformaciju izvornog teksta koje se vrši na osnovu obimne," knjige" kodova, u kojoj se reči i fraze zamenjuju slučajnim nizom znakova. Na primer, "YWRT" može biti kod za "Ja se zovem Petar". Nasuprot tome, šifra radi na nižem nivou: na nivou pojedinačnih slova, malih grupa slova, ili u modernim šemama nad pojedinačnim bitovima. Uz to se umesto "Knjige" kodova koriste algoritmi koji su utemeljeni nekom matematičkom formulom.