Digitalni potpis
Vrsta: Seminarski | Broj strana: 20 | Nivo: Fakultet organizacionih nauka, Beograd

Sadržaj:

Uvod

Kriptologija

Kriptologija je termin koji potiče od grčkih reči kriptos (skriven, tajan) i logos (nauka), i označava naučnu disciplinu koja se bavi sigurnim (tajnim) komunikacijama. Dve osnovne, tesno povezane grane kriptologije su: kriptografija i kriptoanaliza.
Predmet kriptografije je, pre svega, sinteza postupaka za obezbeđivanje tajnosti informacija, tzv. kripto-zaštitu informacija.
Predmet kriptoanalize je razmatranje metoda kojim se kompromituju ("razbijaju" od strane neovlašćenih korisnika) postupci kripto-zaštite informacije.
Primenom kriptografije realizuju se četiri osnovna bezbednosna zahteva (servisa):
tajnost – obezbeđuje da informacioni sadržaj poruke bude dostupan samo ovlašćenim korisnicima
integritet – obezbeđuje otkrivanje neovlašćene izmene informacionog sadržaja poruke
autentičnost – omogućava proveru identiteta učesnika u komunikaciji
neporecivost – sprečava mogućnost poricanja realizacije određenih aktivnosti učesnika u komunikaciji (kao što su slanje poruke, transakcija i dr.).

Istorija

Simetrična kriptografija ili tzv. kriptografija tajnih ključeva je najstariji oblik kriptografije, stara gotovo koliko i ljudska komunikacija. Ona se razvijala i koristila kao alat u zaštiti informacija, naročito u vojnim, diplomatskim i državnim komunikacijama. Za proces kriptovanja u simetričnoj kriptografiji potrebno je znati algoritam kriptovanja i tajni ključ, a sigurnost zavisi od sigurnosti algoritma i dužine ključa. Najpoznatiji simetrični algoritmi su DES (eng. Data Encryption Standard), koji koji koristi ključeve dužine 56 bita i AES (eng. Advanced Encryption Standard), koji koristi ključeve dužine 128, 192 i 256 bita.
Osnovni nedostatak simetričnih algoritama, odn. sistema zasnovanih na simetričnoj kriptografiji jeste upravljanje ključevima tj. njihova distribucija. Pre početka sigurne komunikacije subjekti komunikacije moraju razmeniti ključeve. Budući da se sigurnost svih zaštićenih (kriptovanih) informacija zasniva na sigurnosti ključa, razmena ključeva postaje vrlo ozbiljan problem, koji se usložava ako se komunikacija odvija na većoj udaljenosti i u njoj učestvuje više subjekata. Za n subjekata u komunikaciji potrebno je n(n - 1)/2 ključeva. Generisanje i upravljanje ovako velikim brojem ključeva najčešće je nepraktično, a njihova razmena je nesigurna.
Javni interes za kriptografiju drastično je porastao 1976. god. kada se prvi put javila ideja o infrastrukturi sa javnim ključevima (eng. Public Key Infrastructure, PKI). Naime Whitfield Diffie i Martin Hellman u svojoj publikaciji "New Directions in Cryptography" predstavili su ideju kriptografije bazirane na javnom i privatnom ključu. Tako je utemeljena asimetrična kriptografija ili tzv. kriptografija javnih ključeva čime se dobila mogućnost postizanja tajnosti informacija bez prethodne razmene tajnog ključa putem (ne)sigurnog komunikacionog kanala. Osnova sigurnosti asimetričnih algoritama temelji se na nemogućnosti (ili vrlo teškoj mogućnosti) izračunavanja privatnog ključa iz javnog ključa.

---------- OSTATAK TEKSTA NIJE PRIKAZAN. CEO RAD MOŽETE PREUZETI NA SAJTU. ----------

www.maturskiradovi.net

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com