Digitalni potpis
Vrsta: Seminarski | Broj strana: 9

Sadržaj: Stranica:

Uvod- Općenito o digitalnom potpisu

Današnji opće prihvaćeni način ovjeravanja dokumenata vlastoručnim potpisom vuče korijene od samih početaka ljudske pismenosti. Potpisi se danas nalaze na najrazličitijm dokumentima, od različitih ugovora, naloga, čekova pa sve do privatnih pisama. Prema postojećim zakonima potpisom se smatra ne samo vlastoručni potpis, već i bilo koji drugi znak na dokumentu načinjen s ciljem ovjeravanja dokumenta. Ipak, na računalima se ne smatra svaki potpis digitalnim potpisom. Različite znakovne ili tekstualne oznake u datotekama ili elektronskoj pošti ili kopije vlastoručnog potpisa krajnje su neprimjerene i nepouzdane, prije svega zbog trivijalnog krivotvorenja. Razvojem i širenjem računala a napose računalnih mreža, postalo je jasno da je potreban posve novi način ovjeravanja. Temelji za pouzdanu provjeru porijekla informacija, «digitalni potpis», stvoreni su 1976. godine otkrićem kriptografije javnog ključa (Diffie-Hellman), koja se još naziva i asimetričnom kriptografijom. Zanimljivo je napomenuti da je ovaj način kriptiranja podataka, prema nekim informacijama bio poznat britanskoj tajnoj službi nekoliko godina prije nego spomenutoj dvojici istraživača. Danas, kada većina razvijenih zemalja u svoje zakone uvodi i zakon o digitalnom potpisu, ovo područje se nalazi na granici dva svijeta, kriptografije i prava. Osim pravnih problema oko primjene digitalnog potpisa, postoje i pravni problemi vezani uz implementaciju algoritama digitalnog potpisa, uglavnom zbog softverskih patenata kojima je velik broj algoritama zaštićen, ali i zbog restriktivnih regulativa pojedinih zemalja vezanih uz kriptografske proizvode općenito. Tako je npr. izvoz «jakog» enkripcijskog softvera iz SAD-a bio zabranjen sve do pred kraj 1999. godine. Isto tako, u Francuskoj je upotreba alata za enkripciju bila zabranjena do početka 1999. Ipak, naglim širenjem elektronskog poslovanja postalo je nužno ovakve odredbe ukinuti, i omogućiti kako sigurnu zaštitu informacija šifriranjem tako i zaštitu od mogućih prijevara, autentifikacijom. Upravo idealnim za ovo potonje nameće se digitalni potpis.

Osnovni principi rada digitalnog potpisa

Pretpostavimo da dvoje ljudi Luka i Petar, žele razmjenjivati potpisane poruke (podatke) tj. žele biti sigurni u identitet osobe od koje su poruku dobili. Kao prvo, obje osobe kreiraju par komplementarnih ključeva, javni i tajni ključ. Važno je naglasiti da se poznavanjem javnog ključa ne može izračunati tajni ključ u nekom razumnom vremenu (vrijeme potrebno za izračunavanje tajnog ključa iz poznatog javnog ključa, tj. razbijanje šifre, mjeri se milijunima godina na danas najjačim raspoloživim računalima). Nakon kreiranja ključeva, Luka i Petar razmjenjuju svoje javne ključeve, a potom Luka, koristi svoj tajni ključ za šifriranje sažetka poruke koji je izračunao nekom od «Hash» funkcija. Hash funkcija je funkcija koja iz zadane poruke (podataka) računa sažetak fiksne duljine. Kada Petar uspije dešifrirati sažetak poruke javnim ključem od Luke, on još računa i sažetak primljene poruke koji potom uspoređuje s upravo dešifriranim, i ako je izračunati sažetak jednak onom dešifriranom, primatelj može biti siguran u porijeklo poruke (podataka), jer je poruka mogla biti šifrirana jedino Lukinim tajnim ključem, kao i u integritet poruke.