Tehnike digitalnog potpisa
Vrsta: Seminarski | Broj strana: 18 | Nivo: Univerzitet za poslovne studije

Sadržaj:

Uvod:

Opšte prihvaćeni način ovjeravanja dokumenata je ručni potpis i on vuče korjene od samih početaka ljudske pismenosti.

Potpisi se danas nalaze na različitim dokumentiama, ugovorima, čekovima, pismima i oni potvrđuju vjerodostojnost tih dokumenata. Prema postojećim zakonima potpisom se smatra ne samo vlastoručni potpis, već i bilo koji drugi znak na dokumentu načinjen s ciljem ovjeravanja dokumenta.

Razvojem i širenjem kompijutera i kompijuterskih mreža postalo je jasno da je potreban sasvim novi način ovjeravanja dokumenata. Različiti znakovi ili tekstualne oznake u datotekama ili elektronskoj pošti ili kopije ručnor potpisa bile su neprimjerene i nepouzdane zbog mogućnosti krivotvorenja.

Temelji za pouzdanu provjeru porjekla informacija , digitalni potpis, stvoreni su 1976. godine pronalaskom kriptografije javnod ključa (Diffe-Hellman), koja se naziva i asimetričnom kriptografijom.

Digitalni potpis predstavlja prvi stepen u identifikaciji stranaka koje razmjenjuju poruke. On se koristi za provjeru autentičnosti (provjera autentičnosti: postupak koji se provjerava jesu li ljudi i proizvodi ono što tvrde da jesu) digitalnih informacija.

Digitalni potpis pruža sljedeća osiguranja:

Autentičnost – digitalni potpis potvrđuje da je potpisnik onaj za kojeg se izdaje.

Integritet – digitalni potpis potvrđuje da sadržaj nije mijenjan ili iskvaren otkako je digitalno potpisan.