Kriptografija
Vrsta: Seminarski | Broj strana: 13 | Nivo: Fakultet za poslovne studije, Banja Luka

Uvod
Kriptografija kao nauka, koja se bavi metodama očuvanja tajnosti informacija je postala sve važnija sa porastom kompjuterskih mreža i elektronskih transakcija. Kada se lične, finansijske, vojne ili informacije državne bezbjednosti prenose sa mjesta na mjesto, one postaju ranjive na prisluškivačke taktike koje potencijalno mogu izazvati katastrofalne posljedice. Ovakvi problemi mogu se izbjeći kriptovanjem (šifrovanjem) informacija koje ih čini nedostupnim trećoj strani.
Ovaj rad nema za cilj da detaljno opisuje algoritme za šifrovanje koji su danas u širokoj upotrebi. Naravno biće spomenuti većina od njih, međutim ovdje je akcent stavljen na napredne tehnike i rezultate do kojih se došlo u istraživanju algoritama za cjelobrojnu faktorizaciju (Integer factorization) sa osvrtom na aspekt kompleksnosti samih tih algoritama, kao algoritama na kojima se bazira sigurnost većine šifrovanih informacija današnjice, i kvantne kriptografije (Quantum cryptography). Kako su zaštita tajnosti, integritet i autentičnost informacija tri osnovna svojstva koja treba da posjeduje mehanizam šifrovanja, to će biti riječi i o njihovom obezbjeđivanju.
Jedna moguća šema postizanja tajnosti može da bude ova [5]: Entiteti A i B razmjenjuju ključ, par (e,d). U nekom sljedećem vremenu, ako A želi da pošalje poruku m entitetu B, potrebno je da izračuna c=Ee(m) i rezultat (šifrovanu poruku, odnosno šifrat) pošalje B. Po prijemu c, B računa Dd(c)=m regenerišući na taj način originalnu poruku m. Ee označava transformaciju šifrovanja, a Dd transformaciju dešifrovanja, pri čemu je potrebno da d tj. Dd bude tajno.
Zašto nije jednostavno odabrana funkcija za šifrovanje i odgovarajuća funkcija za dešifrovanje? Razlog je dalekosežan: u tom slučaju otkrivanje para koji omogućava šifrovanje/dešifrovanje uslovio bi redizajniranje čitave šeme šifrovanja, dok je u slučaju upotrebe ključeva dovoljno promjeniti par (e,d). Tajnost poruke se zasniva isključivo na tajnosti ključa; nijedan ozbiljan algoritam za kriptografiju ne zasniva tajnost poruke na tajnosti ili nedostupnosti algoritma. Štaviše, svi algoritmi za kriptografiju koji se danas upotrebljavaju su javni i lako dostupni.
Prema postupku nalaženja para (e,d) razlikujemo simetrično i asimetrično šifrovanje. Ako je znanjem e jednostavno odrediti d, tada cijeli par (e,d) mora biti tajan i radi se o simetričnom algoritmu, tj. o kriptografiji tajnih ključeva. Ukoliko znajući samo e nemamo praktičnog načina da odredimo d, radi se o asimetričnom algoritmu, tj. kriptografiji javnih ključeva. U ovom slučaju samo treba obezbjediti tajnost d. Stoga je struktura rada data u 3 glavna poglavlja:
Šifrovanje tajnim ključem,
Šifrovanje javnim ključem,
Kvantno šifrovanje,
gdje kvantno šifrovanje spada u simetrično šifrovanje, ali je metod generisanja ključeva bitno drugačiji pa stoga je obrađeno u posebnom poglavlju. U svakom od poglavlja biće kratko opisani načini na koji se informacija šifruje, zatim dešifruje, dokle se stiglo sa istraživanjem u tim oblastima, vjerodostojnost samih metoda kao mane i prednosti samih algoritama.
...