TEHNIČKA ŠKOLA MLADENOVAC

Vuka Karadžića 75, 11400 Mladenovac, тел.011/8231-985, [tsm@gmail.com](mailto:tsm@gmail.com)

**ASIMETIRČNO ŠIFROVANJE I DEŠIFROVANJE**

**rofesor:** **Učenik:**

**Srđan Maričić Stefan Todorović IV6**

**Uvod**

Za razliku od simetrične kriptografije, asimetrična koristi dva ključa — javni i privatni. Princip je sledeći: u isto vreme se prave privatni i odgovarajući javni ključ. Javni ključ se daje osobama koje šalju šifrovane podatke. Pomoću njega te osobe šifruju poruku koju žele da pošalju. Kada primalac dobije šifrat, dešifruje ga pomoću svog privatnog ključa. Na taj način svaki primalac ima svoj privatni ključ a javni se može dati bilo kome, pošto se on koristi samo za šifrovanje, a ne i dešifrovanje.

Prednost ovog načina šifrovanja je u tome što ne mora da se brine o slučaju da neko presretne javni ključ, jer pomoću njega može samo da šifruje podatke. Takođe, programi sa ovakvim načinom šifrovanja imaju opciju da potpisuju elektronske dokumente (o tome će biti reči nešto kasnije). Pojam sistema sa javnim ključevima uveli su Difi i Helman 1976. godine. Prvi takav sistem koji su oni definisali bio je protokol, poznat pod imenom razmena ključeva Difi-Helman. [1977](https://sh.wikipedia.org/wiki/1977). godine objavljen je najčuveniji i najpopularniji algoritam za simetričnu kriptografiju RSA, čije ime predstavlja skraćenicu sačinjenu od prvih slova prezimena autora Rona Riversta, Adi Šamira i Leonarda Ejdlmana.

U asimetričnim kriptosastavima, privatni ključ je uvijek matematički povezan s javnim ključem. Zbog toga je uvijek moguće napasti asimetrične sustave izvodeći privatni ključ iz javnog. U pravilu obrana od takvih napada je da je problem izvođenja privatnog ključa iz javnog što je moguće teži. Prednost ovog sustava je u jednostavnosti stvaranja sigurnog komunikacijskog kanala izmedu dvije osobe, nema problematične razmjene ključa kao u simetričnim kriptosustavima. No nedostatak je duže vrijeme potrebno za obavljanje operacije šifriranja i dešifriranja pa se kod slanja dužih poruka koristi simetrični kriptosastav.

**Upotreba**

Kriptografija javnih ključeva se često koristi za obezbeđivanje elektronske komunikacije putem otvorenog mrežnog okruženja kao što je internet, bez oslanjanja na skrivene ili tajne kanale, čak ni za razmenu ključeva. Otvorena mrežna okruženja su podložna raznim bezbednosnim komunikacionim problemima, kao što su napadi „čovek u sredini“ (man-in-the-middle) i druge prevare.

Bezbednost komunikacije obično uključuje zahteve da komunikacija ne sme biti čitljiva tokom prenosa (što održava poverljivost), komunikacija se ne sme modifikovati putem prenosa (što čuva integritet komunikacije), komunikacija mora poteći od identifikovane osobe (autentičnost pošiljaoca) a primalac ne sme biti u stanju da odbije primanje komunikacije. Kombinacija kriptografije sa EPKE (Enveloped Public Key Encryption) metodom omogućava bezbedno slanje komunikacije putem otvorenog mrežnog okruženja. Drugim rečima, ukoliko lice koje želi da zloupotrebi informacije sasluša čitav razgovor uključujući i razmenu ključeva, on neće moći da rastumači razgovor.

Tehnika razlikovanja koja se koristi u kriptografiji javnih ključeva jeste korišćenje algoritama asimetričnog ključa, gde ključ koji se koristi od strane jednog lica radi šifrovanja nije isti kao ključ koji koristi druga strana radi dešifrovanja. Svaki korisnik ima par kriptografskih ključeva, javni ključ za šifrovanje i privatni ključ za dešifrovanje. Na primer, par ključeva koji se koristi za digitalne potpise se sastoji od privatnog ključa potpisa i javnog ključa verifikacije. Javni ključ se može javno distribuirati sve dok je privatni ključ poznat samo svom vlasniku. Ključevi su matematički povezani ali su parametri izabrani tako da je izračunavanje privatnog ključa preko javnog ključa nepraktično.

**Slabosti**

Potencijalna bezbedonosna ranjivost u korišćenju asimetričnih ključeva jeste mogućnost napada „man-in-the-middle” (čovek iznutra), u kojem se komunikacija javnih ključa presreće od strane treće strane i zatim se modifikuje da pruži drugačije javne ključeve. Šifrovane poruke kao i odgovori takođe se moraju presresti, dešifrovati i ponovo šifrovati od strane napadača korišćenjem odgovarajućih javnih ključeva za različite komunikacione segmente, i to u svim slučajevima, da bi se izbegla sumnja. Ovaj napad možda izgleda težak za implementaciju u praksi ali nije nemoguć pri korišćenju nebezbednih medija (kao što su javne mreže tj. bežični oblici komunikacije).

Jedan pristup sprečavanju takvih napada uključuje korišćenje treće strane koja je odgovorna za verifikovanje identiteta korisnika sistema. Ova strana učesnicima daje nepromenljivi digitalni potpis koji je otporan na zloupotrebu. Takvi sertifikati su potpisani blokovi podataka koji kažu da ovaj javni ključ pripada toj osobi, kompaniji ili drugom entitetu. Ovaj pristup takođe ima i svoje nedostatke. Na primer, strani koja izdaje sertifikat se mora verovati da je ispravno proverila identitet vlasnika ključa, mora osigurati ispravnost javnog ključa kada daje sertifikat, mora biti bezbedna od računarske piraterije i mora napraviti dogovore sa svim učesnicima u vidu provere svih njihovih sertifikata pre nego što zaštićena komunikacija otpočne.

**Asimetrični algoritmi**

Neki od najpoznatijih su:

* ELGamal
* Rabin
* RSA
* ECC

**ELGamal**

ElGamal je asimetrični kriptografski algoritam temeljen na problemu diskretnih logaritama. Sastoji se od enkripcijskog i algoritma za digitalno potpisivanje. Algoritam za kriptiranje sličan je po prirodi Diffie-Helman-ovom algoritmu za dogovaranje ključeva. Njegova sigurnost se temelji na tvrdokornosti problema diskretnih algoritama i na Diffie-Helmanovom problemu. Analize temeljene na najboljim dostupnim algoritmima za faktoriziranje i diskretnim logaritmima pokazuju da RSA i ElGamal imaju slične razine sigurnosti za jednake duljine ključeva. Glavni nedostatak ElGamala je potreba za slučajnošću i manja brzina. Još jedan potencijalni nedostatak je da tijekom kriptiranja poruke dolazi do povećanja poruke za faktor dva. Unatoč tome takvo povećanje poruke je zanemarivo ako se kriptosustav koristi samo za izmjenu privatnih ključeva.

**Rabin**

Poželjno svojstvo bilo kojeg enkripcijskog algoritma je dokaz da je razbijanje jednako složeno kao rješavanje računarskog problema koji se općenito smatra vrlo složenim, kao primjerice faktoriziranje cijelih brojeva ili diskretni logaritamski problem. Rabinov asimetrični enkripcijski algoritam je prvi primjer dokazano sigurnog asimetričnog algoritma, problem s kojim je suočen pasivni protivnik, izračunavanje kvadratnog korijena c mod n je računski jednak faktoriziranju n.

Mana Rabinovog algoritma je da je primatelj suočen sa zadatkom izbora pravog nekriptiranog teksta izmedu četiri mogućnosti. Te neodređenosti kod dekriptiranja u praksi možemo nadvladati dodavanjem unaprijed određene redundancije originalnoj poruci prije kriptiranja. (npr. zadnjih 64 bita mogu biti dodani na kraj poruke) Tada, s visokom vjerojatnošću, točno jedan od četiri kvadratnih korijena m1, m2, m3, m4 valjanog kriptiranog teksta c će posjedovati tu redundanciju i primatelj će izabrati taj kao pravi nekriptirani tekst. Ako nijedan kvadratni korijen od c ne posjeduje tu redundanciju, tada bi primatelj trebao odbaciti c kao krivotvoren.

**RSA**

Jedan od najpoznatijih algoritama asimetričnog kriptiranja je zasigurno RSA (to je zapravo kratica od prvih slova prezimena autora algoritma, Ron Rivest, Adi Shamir, Len Adelman). Sigurnost RSA algoritma zasniva se na problemu faktoriziranja velikih brojeva. Javni i privatni ključ su funkcije dva velika prosta broja. Upravo je zato težina generiranja izvorne poruke na temelju javnog ključa i kriptirane poruke jednaka težini faktoriziranja umnoška dvaju prosta brojeva. To znači da je gotovo nemoguće, bar ne u razumnom vremenu, otkriti privatni ključ metodom pokušaja i pogrešaka.

**ECC**

Kriptografija eliptičkih krivulja ( engl. Elliptic curve cryptography ) je predstavljena od Victora Milera i Neal Koblitza 1985. ECC je predložena kao alternativa postojećim sustavima javnog ključa kao DSA i RSA. EEC je u zadnje vrijeme dobio dosta pažnje od industrije i znanosti. Glavni razlog privlačnosti ECC-a je činjenica da ne postoji niti jedan algoritam s pod-eksponencijalnom složenošću za koji se zna da rješava diskretni logaritamski problem na pravilno izabranoj eliptickoj krivulji. To znači da se kod ECC-a mogu koristiti značajno manji parametri nego kod drugih konkurentskih sustava kao RSA i DSA, ali s jednakom razinom sigurnosti. Neke prednosti korištenja ključeva manje veličine uključuju brže izračune, smanjenje potrebne računalne snage, memorije i širine pojasa ( engl. bandwidth ). To čini ECC idealnom za skučena okruženja kao što su pageri, PDA-ovi, mobilni telefoni i pametne kartice. Implementacija ECC-a, u drugu ruku, zahtjeva izbor nekoliko parametara kao što su tip konačnog polja, algoritmi za implementiranje aritmetike konačnih polja, tip eliptične krivulje. Mnogi od ovih izbora mogu imati velik učinak na sveukupno izvođenje.

**Ostali asimetrični algoritmi**

Najpoznatiji asimetrični algoritam je zasigurno RSA koji svoju sigurnost zasniva na problemu faktoriziranja velikih brojeva, koristi se kod enkripcije, distribucije ključeva i digitalnog potpisivanja. Još jedan poznati algoritam je Diffie-Hellman algoritam ugovaranja ključa, algoritam dozvoljava dvama korisnicima da izmijene tajni ključ preko nesigurnog kanala, sigurnost algoritma se temelji na diskretnom logaritamskom problemu. ElGamal algoritam služi za enkripciju i za digitalno potpisivanje, po prirodi je slican Diffie-Helman algoritmu jer se takoder njegova sigurnost temelji na diskretnom logaritamskom problemu. Od poznatijih algoritama tu je i Rabin kao primjer dokazivo sigurnog algoritma. Još jedan zanimljivi algoritam je Merkle-Hellmanov algoritam. Iako je algoritam razbijen, vrijedan je spomena. Merkle-Hellmanov algoritam se temelji na problemu sume podskupa (posebnom slučaju problema naprtnjače). Takoder zanimljiv algoritam je i McElice algoritam. Algoritam se temelji na kodovima za provjeravanje grešaka. McEliece algoritam je prvi asimetrični algoritam koji koristi randomizaciju u postupku šifriranja. Iako vrlo efikasan, McElice algoritam se r ijetko primjenjuje u praksi zbog jako velikih javnih ključeva. Osim ovih postoji i grupa vjerojatnosnih asimetričnih algoritama. Neki od poznatijih vjerojatnosnih mnkk0p algoritama su Blum-Goldwasser i Goldwasser-Micali algoritmi.