Asimetrično šifrovanje i dešifrovanje

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. 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.

Postoji više algoritama za generisanje asimetričnih ključeva.

Jedan od vodećih je RSA algoritam, koji je dobio ime po trojici svojih pronalazača (Rievst, Shamir, Adleman). On funkcioniše pre svega na teškoći faktorizacije velikih brojeva, kao i na osobinama operacije mod i na Euler-ovoj funkciji ϕ.

Alisa Bobanu treba da pošalje neku poruku. Ona odlazi na Bobanov sajt i uzme javno dostupan ključ (n,e) koji je Boban napravio na sledeći način: Boban je izabrao dva prosta broja p i q sa oko 150 dekadnih cifara. Zatim je izračunao n=pq i $\phi(n)=(p-1)(q-1)$. Nakon toga je odredio neki broj e takav da je nzd(e, $\phi(n)$)=1 i odredio je tajni broj $d=e\text{-}1(\text{mod}\phi(n))$.

Brojeve n i e je objavio na svom sajtu, a brojeve d,p,q čuva u tajnosti. Alisa kriptuje poruku M pomoću javnog ključa (n,e).

Ona izračunava C=Me (mod n), i dobijeno C šalje Bobanu. Boban izračunava C d (mod n) i dobija M, jer je C d=(Me) d=Med=M1=M (mod n).

Težina javnog ključa ogleda se u tome što je određivanje činioca broja n sporo i neefikasno. Očekuje se da će postojeći razvoj hardvera ovaj posao olakšati za oko petnaestak godina. Na sledećem primeru (sa znatno manjim brojem n) je pokazano kako bi se na osnovu javnog ključa šifrovala poruka, odredio tajni broj d, i dešifrovala poruka.