ASIMETRIČNO ŠIFROVANJE I DEŠIFROVANJE

Milutin Milosavljević

ASIMETRIČNA KRIPTOGRAFIJA

- 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.

Tvorci asimetrične kriptografije su Whitefield Diffie i Martin Hellman koji su 1976. godine opisali ideju kriptografije koja se temelji na dva ključa, privatnom (ili često zvanim tajnim) i javnom ključu.

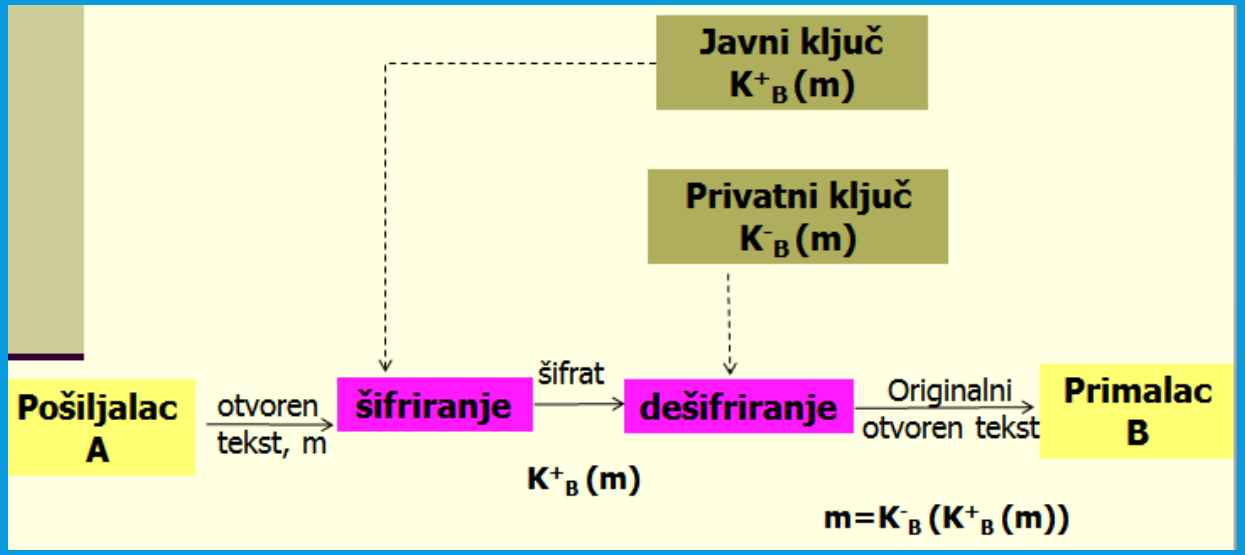
- Prvi takav sistem koji su oni definisali bio je protokol, poznat pod imenom razmena ključeva Difi-Helman. 1977. godine objavljen je najčuveniji i najpopularniji algoritam za simetričnu kriptografiju RSA, čije ime predstavlja skraćenicu sačinjenu od prvih slova prezimena autora Rona Riversta, Adi Šamira i Leonarda Ejdlmana.

- 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.

KRIPTOGRAFIJA JAVNOG KLJUČA

Pošiljalac i primalac nemaju isti tajni ključ

- Javni ključ je poznat svima
- Privatni ključ za dešifrovanje poznat je samo primaocu



Algoritmi asimetričnih kriptosistema zasnivaju se na određenim svojstvima brojeva.

- Pri kriptovanju se izvorni tekst tretira kao niz prirodnih brojeva koji se odabranom funkcijom kriptovanja i ključem Kb preračunavaju u kriptovani niz teksta.
- Funkcija kriptovanja mora biti takva da se iz kriptovanog teksta ne može odrediti izvorni tekst, čak ako je poznat i ključ za kriptovanje.
- Međutim, ukoliko se zna ključ dekriptovanja Kd moguće je lako računanje izvornog teksta.
- Svaki od sagovornika mora posedovati dva ključa (javni i tajni). Iako su različiti, ključevi su međusobno povezani određenim transformacijama

nedostatak ovog načina kriptovanja je njegova sporost i neprikladnost za kriptovanje velikih količina podataka.

- pitanje autentičnosti poruke, odnosno kako da osoba B bude sigurna da je poruku koju je primila uistinu poslala osoba A.
- Najčešće se koriste sledeći asimetrični algoritmi: RSA (eng. Rivest-Shamir-Adleman), Diffie-Hellman, ElGamal, Eliptic, Curves, Rabin i drugi.

RSA ALGORITAM

- Za generisanje javnog i tajnog ključa se koriste prosti brojevi.
  - Tajni ključ predstavlja uređeni par brojeva (N,d).
  - Javni ključ je takođe uređeni par brojeva (N,e). Treba uočiti da je broj N zajednički za oba ključa.
- Osoba koja šalje poruku vrši kriptovanje pomoću sledeće jednačine :
- $C = P^e \bmod N$
- P, izvorni tekst koji je prikazan u obliku broja;
- C, broj koji predstavlja kriptovan tekst;
- brojevi e i N su komponente javnog ključa.

Kada se poruka primi potrebno je dekriptovati pomoću sledeće jednačine:

$P = Cd \bmod N$

- P i C isto kao i u predhodnoj formuli, a N i d predstavljaju komponente tajnog ključa
- Osnovni problem kod RSA algoritma je kako izvršiti izbor brojeva N, d i e (veoma velike vrednosti dužine od 1024 do 2048), a da ujedno zadovoljavaju formule algoritma.
- koristi teoriju prostih brojeva i sledeću proceduru

PREDNOSTI I NEDOSTACI ASIMETRIČNIH ALGORITAMA

- rešava nedostatake deljenja ključa kod simetričnih algoritama prilikom komunikacije
- svaka osoba kreira po dva ključa, tajni koji osoba čuva, i javni koji se razmenjuje sa drugima.
- Svaki od entiteta je nezavistan i svoj par ključeva može koristiti u komunikaciji sa bilo kime
- smanjenju broja ukupno potrebnih ključeva. U sistemu od milion korisnika, potrebno je samo 2 miliona ključeva, dok bi u slučaju korišćenja simetričnog kriptovanja bilo potrebno bar 500 milijardi ključeva.

- Najveći nedostatak je kompleksnost algoritama koji se koriste prilikom kriptovanja. Ako se želi efektno kriptovanje to povlači da algoritam koristi ogromne ključeve prilikom rada, pa nisu preporučljivi za rad sa velikim izvornim podacima
- Komunikacija između dve strane i javni ključ moraju verifikovati. Kako osoba A šalje svoj javni ključ osobi B putem elektronske pošte, osoba B na neki način mora biti sigurna da je dobijeni ključ upravo poslat od strane osobe A.

Milutin Milosavljević