Predmet: Zaštita informacionih sistema

Profesor: Srđan Maričić

Vezba br. 1

Asimetricno sifrovanje i desifrovanje

Dragana Mijailovic IV-6

Asimetrični kriptosistemi

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.

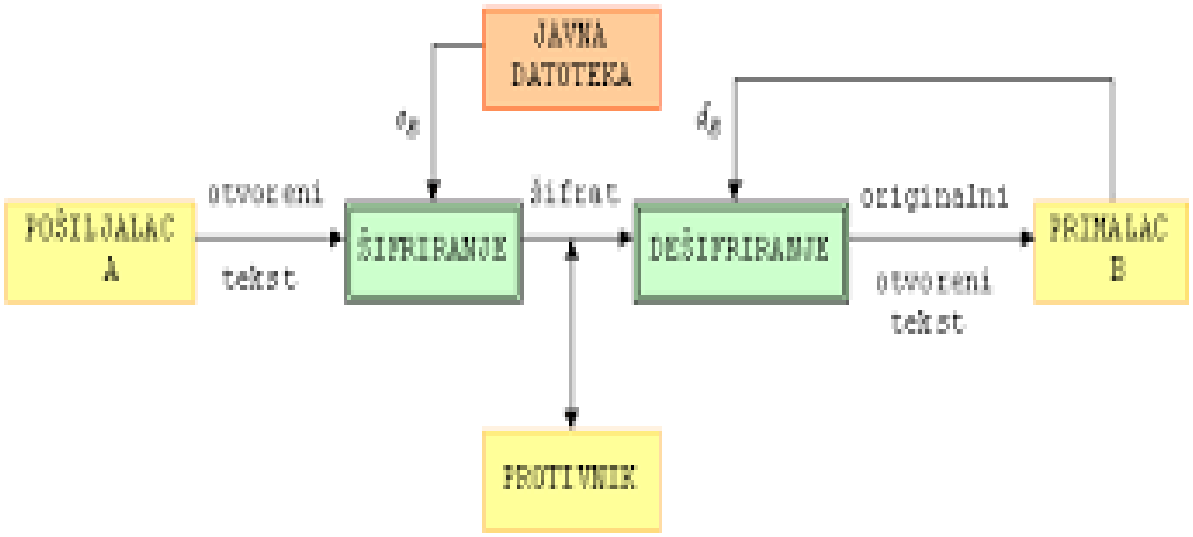
Asimetričnog kriptovanja ili **asymmetric-key** ili **public-key** kriptovanje.

Kriptografija javnog kljuca

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:

$P = C^d \bmod N$

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:

RSA: Izbor ključeva

1. Choose two large prime numbers p, q.

(e.g., 1024 bits each)

2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e<n$) that has no common factors with z. (e, z are "relatively prime").
4. Choose d such that $ed-1$ is exactly divisible by z. (in other words: ed mod $z = 1$).
5. *Public* key is (n,e). *Private* key is (n,d).

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.