**Tehnička škola Mladenovac**

**Javni i privatni ključevi   
u sistemima enkripcije i dekripcije**

**(Asimetrična kriptografija)**

*Mateja Dimić/Vukašin Bujagić*

*4-6*

**Asimetrična kriptografija**

Kriptografija javnog ključa ili asimetrična kriptografija je kriptografski sistem koji koristi 2 ključa:

-Javni ključ

Javni ključevi se mogu široko distribuirati

-Privatni ključ

Privatni ključevi su poznati samo vlasniku.

Generisanje takvih ključeva zavisi od kriptografskih algoritama zasnovanih na matematičkim problemima da bi se proizvele jednosmerne funkcije. Efektivna sigurnost zahteva samo čuvanje privatnog ključa; javni ključ se može otvoreno distribuirati bez ugrožavanja sigurnosti.

U takvom sistemu svaka osoba može šifrirati poruku koristeći javni ključ primaoca, ali ta šifrovana poruka može se dešifrovati samo privatnim ključem primaoca.

Pošiljalac može da kombinuje poruku privatnim ključem kako bi stvorio kratak digitalni potpis na poruci.

Svako sa pošiljateljevim odgovarajućim javnim ključem može kombinovati istu poruku i navodni digitalni potpis koji je s njom povezan da proveri da li je potpis važeći, tj. da li je napravljen od vlasnika odgovarajućeg privatnog ključa.



~Algoritmi:

Sve šeme javnih ključeva u teoriji su podložne "brute-force key search attack" („napadu pretraživanja grubih sila“). Takvi napadi su, međutim, nepraktični ako količina računanja koja je potrebna za uspeh nije dostupna svim potencijalnim napadačima.

U mnogim slučajevima se faktor rada može povećati jednostavnim odabirom dužeg ključa. Ali drugi algoritmi mogu imati mnogo niže faktore rada, što primorava otpor od napada grubih sila beznačajnim. Neki posebni i specifični algoritmi razvijeni su da pomognu u napadu na neke algoritme šifriranja javnih ključeva - i RSA i ElGamal enkripcija imaju poznate napade koji su mnogo brži od brute-force attack-a.

Otkrivene su velike slabosti za nekoliko ranije obećavajućih asimetričnih algoritama. Otkriveno je da je algoritam "knapsack packing" („pakiranja ruksaka“) nesiguran nakon razvoja novog napada.

Od nedavno su neki napadi zasnovani na pažljivim merenjima tačnog vremena koje je hardveru potrebno za šifrovanje običnog teksta. Trenutno je u toku veliki broj aktivnih istraživanja kako bi se otkrili novi algoritmi napada i zaštitili od njih.

Još jedna potencijalna bezbednosna ranjivost u korišćenju asimetričnih ključeva je mogućnost napada "man-in-the-middle" („čovek u sredini“), u kome komunikacija javnih ključeva presreće treća strana („čovek u sredini“) i zatim se modifikuje da pruža različite javne ključeve.

Ovaj napad može biti težak za sprovođenje u praksi, ali nije nemoguć i kada se koriste nesigurni mediji (npr. Javne mreže, poput Interneta ili bežičnih oblika komunikacije), zlonamerni pružalac Internet usluga(ISP) bi mogao to lako da izvede.

~Infrastruktura javnih ključeva:

Jedan pristup za sprečavanje takvih napada uključuje upotrebu infrastrukture javnih ključeva (PKI); skup uloga, polisa i procedura potrebnih za kreiranje, upravljanje, distribuciju, upotrebu, skladištenje i opoziv digitalnih potvrda i upravljanje šifrovanjem javnog ključa.

Međutim, to zauzvrat ima potencijalne slabosti.

Na primer, organu za izdavanje sertifikata, koji izdaje sertifikat mora se verovati da je pravilno proverio identitet vlasnika ključeva, mora da obezbedi ispravnost javnog ključa prilikom izdavanja sertifikata, mora biti zaštićen od kompjuterske piraterije i mora da je napravio aranžmane sa svim učesnicima da provere sve svoje sertifikate pre nego što započne zaštićena komunikacija.

Veb pregledači, na primer, dobijaju dugu listu "samopotpisanih potvrda identiteta" od PKI provajdera - oni se koriste za proveru dobrovernosti sertifikata, a zatim, u drugom koraku, sertifikate potencijalnih komunikatora.

Uprkos svojim teorijskim i potencijalnim problemima, ovaj pristup se široko koristi. Primeri uključuju TLS i njegov prethodni SSL, koji se obično koriste za pružanje sigurnosti za transakcije putem veb pretraživača (na primer, za sigurno slanje podataka o kreditnoj kartici za internetsku trgovinu).

Pored otpora napadu određenog para ključeva, prilikom implementacije sistema javnih ključeva mora se uzeti u obzir i sigurnost hijerarhije sertifikata. Neki autoritet sertifikata - obično namenski program koji radi na serveru računara - potvrđuje identitete dodeljene određenim privatnim ključevima stvarajući digitalni sertifikat.

Digitalni sertifikati javnih ključeva obično važe nekoliko godina, tako da se pridruženi privatni ključevi moraju sigurno držati tokom tog vremena. Kada je privatni ključ koji se koristi za kreiranje sertifikata viši u hijerarhiji PKI servera ugrožen ili slučajno otkriven, tada je moguć “man-in-the-middle attack”(„napad čoveka u sredini“), čineći svaki podređeni sertifikat u potpunosti nesigurnim.