SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINARSKI RAD IZ PREDMETA
SUSTAVI ZA PRAĆENJE I VOĐENJE PROCESA

ASIMETRIČNI ALGORITMI KRIPTIRANJA

Ivan Murat
JMBAG: 0036389224
INE

Zagreb, 05.06.2005.

1 Uvod

Sigurnost računalnih sustava postaje sve važnija jer u današnjem svijetu sve više korisnika na sve više načina koristi sve više informacija koje su raspršene u raspodijeljenim sustavima. U takvom svijetu postoji sve veća opasnost od neovlaštene uporabe informacija, podmetanja krivih informacija ili uništavanja informacija. Iz tih razloga postaju sve zanimljiviji različiti zaštitni mehanizmi koji osiguravaju sigurnost računalnih sustava. Sigurnosni zahtjevi ovise o vrsti informacija koje želimo zaštititi.

Po važnosti sigurnosne zaštite može se načiniti približni redoslijed informacijskih sustava:

- Vojni informacijski sustavi
- Bankovni informacijski sustavi
- Zdravstveni i bolnički informacijski sustavi
- Informacijski sustavi državnih institucija
- Informacijski sustavi osiguravajućih društava
- Poslovni informacijski sustavi gospodarskih subjekata

Opća koncepcija sigurnosti ima svoje moralne i pravne aspekte koji se reguliraju zakonodavstvom i odgovarajućim kaznenim mjerama.

Ugrožavanje sigurnosti računalnih sustava moguće je klasificirati na različite načine. Jedna od mogućih podjela sigurnosnih mehanizama je sljedeća:

- Zaštita od vanjskih utjecaja
- Zaštita ostvarena sučeljem prema korisniku
- Unutarnji zaštitni mehanizmi
- Komunikacijski zaštitni mehanizmi

Sigurnost računalnih sustava se zasniva na ispunjavanju triju osnovnih sigurnosnih zahtjeva. To su:

- *Povjerljivost* ili *tajnost* – informacije u sustavu smiju biti pristupačne samo ovlaštenim korisnicima

- *Raspoloživost* – informacije moraju uvijek biti na raspolaganju ovlaštenim korisnicima
- *Besprijekornost* – informacije u sustavu mogu mijenjati samo za to ovlašteni korisnici

Mnoga korisna ostvarenja uporabe računalnih mreža u gotovo svim područjima ljudske djelatnosti dobrim dijelom ovise o razvitku pouzdanih zaštitnih mehanizama koji osiguravaju primjerenu sigurnost sustava.
Svi se sigurnosni zahtjevi (osim raspoloživosti) mogu zadovoljiti uvođenjem kriptiranja sadržaja koji se razmjenjuje u umreženim računalnim sustavima.

2 Osnove kriptografije

2.1 Osnovni kriptografski pojmovi

S obzirom da je u komunikacijskom kanalu nemoguće spriječiti prisluškivanje podataka, pokazalo se razumnim načiniti podatke nerazumljivim neovlaštenim uljezima. Podaci koji u svom izvornom obliku predstavljaju neku korisnu informaciju mogu se postupkom kriptiranja prevesti u oblik u kojem se ta informacija više ne prepoznaje.

S obzirom da su počeci kriptiranja povezani s prenošenjem pisanih informacija u obliku tekstova, u kriptografskoj se terminologiji izvorni oblik podataka naziva razgovijetnim ili jasnim tekstom (engl. *plaintext, cleartext*).

Postupkom kriptiranja (engl. *encription, enciphering*) jasni tekst se prevodi u kriptirani tekst (engl. *ciphertext*). Obrnuti postupak prevođenja kriptiranog teksta u jasni teks naziva se dekriptiranjem (engl. *decryption, deciphering*).

U današnje se vrijeme, kada nam na raspolaganju stoje vrlo moćna računala, ne može primjenjivati neke naivne stare metode kriptiranja koje su se, u načelu, zasnivale na zamjeni znakova prema nekim složenim pravilima. Današnji kriptografski postupci su parametarske matematičke funkcije odnosno algoritmi kojima se nizovi bitova jasnog teksta preračunavaju u nizove bitova kriptiranog teksta i obrnuto.

Kriptiranje se formalno može zapisati u sljedećem obliku:

$$C = E(P, K_E),$$

gdje je:

P – jasni ili razgovijetni tekst,
C – kriptirani tekst,
E – funkcija kriptiranja,
K_E – parametar ili ključ kriptiranja (engl. *encryption key*).

Formalni opis dekriptiranja nekaka je:

$$P = D(C, K_D),$$

Gdje je:

P – jasni tekst,
C – kriptirani tekst,
D – funkcija dekriptiranja,
K_D – parametar ili ključ dekriptiranja
(engl. *decryption key*).

Funkcija dekriptiranja mora biti inverzna funkciji kriptiranja, tako da vrijedi

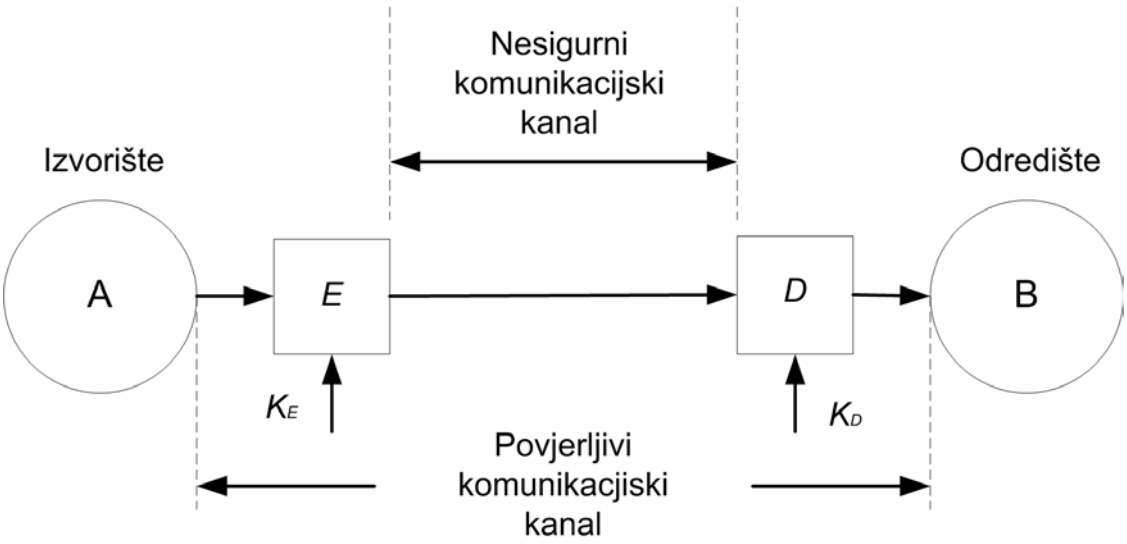
$$P = D(E(P, K_E), K_D),$$

tj. dekriptiranjem kriptiranog jasnog teksta dobiva se opet jasni tekst.

Ako se kriptiranje obavi u izvorištu i dekriptiranje u odredištu onda se kriptiranjem komunikacijski kanal štiti od prisluškivanja te se time postiže povjerljivost informacija.

2.2 Kriptosustavi, povjerljivi komunikacijski kanal

Funkcije kriptiranja E i dekriptiranja D sačinjavaju kriptosustav. Korisnik A (umjesto *korisnik A* ili *strana A* se u literaturi o kriptiranju koristi ime *Alica*) je izvorište informacija. On obavlja kriptiranje svojim ključem K_E. Kriptirana poruka šalje se preko komunikacijskog kanala koji nije zaštićen od uljeza i zbog toga ga nazivamo nesigurnim komunikacijskim kanalom (engl. *unsecure channel*).



Slika 2.1 Komunikacijski kanal

Korisnik B (kojeg u literaturi obično nazivaju *Bob*) nakon dekriptiranja poruke svojim ključem K_D dobiva razgovijetni tekst. Međutim, uljez koji ne zna ključ dekriptiranja poruku neće razumjeti.

Uz pretpostavku da nitko osim Boba ne zna ključ dekriptiranja, kriptosustav transformira nesigurni komunikacijski kanal u povjerljivi informacijski kanal (engl. *trusted channel*) između Alice i Boba.

Današnji kriptosustavi koriste postupke koji se efikasno mogu izvoditi na računalima i to bilo sklopovski ili programski. Ti se postupci zasnivaju na algoritmima koji su u pravilu opće poznati, ali s ključevima koji imaju vrlo veliki broj mogućih vrijednosti što omogućuje stvaranje vrlo velikog broja različitih oblika kriptiranog teksta, a osnovni razlog kriptiranja je stvaranje nerazgovijetnog teksta za sve uljeze koji ne znaju ključ dekriptiranja.

"Razbijanje" kriptiranja svodi se na pronalaženje ključa dekriptiranja. Jasno je da je postupak pronalaženja tog ključa teži ako on može poprimiti veliki broj vrijednosti.

Dobrota kriptosustava određena je težinom otkrivanja ključa dekriptiranja K_D. Pri utvrđivanju dobrote kriptosustava mora se voditi računa o tome kako napadač ili uljez (kojeg u ovom slučaju nazivaju kriptoanalitičarem) pokušava otkriti ključ K_D.

Kriptoanalitičar može pokušavati otkriti ključ dekriptiranja:

- Uz poznavanje samo kriptiranog teksta
- Uz poznavanje samo ograničene količine kriptiranog i razgovijetnog teksta
- Uz poznavanje neograničene količine kriptiranog i njemu pripadajućeg razgovijetnog teksta

Razumljivo je da je posljednje spomenuti način za kriptoanalitičara najpovoljniji i stoga se tim načinom i ispituje otpornost kriptosustava. Smatra se da je najbolji način ispitivanja kriptosustava njegova uporaba. Ako kroz stanovito vrijeme nije potvrđen ni jedan uspješan pokušaj njegova razbijanja on se može smatrati razmjerno sigurnim.

Danas su u uporabi dva osnovna oblika kriptosustava:

- Simetrični kriptosustavi
- Asimetrični kriptosustavi

Asimetrični kriptosustavi imaju različite ključeve kriptiranja K_E i dekriptiranja K_D i mogu se opisati već navedenim izrazima:

$$C = E(P, K_E),$$
$$P = D(C, K_D),$$
$$P = D(E(P, K_E), K_D).$$

U simetričnim kriptosustavima ključ kriptiranja K_E jednak je ključu dekriptiranja K_D. Zajednički ključ se može označiti jednim simbolom K. Prema tome, za takav sustav vrijedi:

$$C = E(P, K),$$
$$P = D(C, K),$$
$$P = D(E(P, K), K).$$

3 Asimetrični kriptosustavi, sustavi s javnim ključem

3.1 Neke činjenice i algoritmi iz teorije brojeva

Asimetrični sustavi zasnivaju se na određenim svojstvima brojeva koji se istražuju u teoriji brojeva. Pri kriptiranju se razgovijetni tekst kodira kao niz prirodnih brojeva koji se odabranom funkcijom kriptiranja i ključem kriptiranja K_E preračunavaju u niz brojeva kriptiranog teksta. Funkcija kriptiranja mora biti takva da iz niza brojeva kriptiranog teksta napadač samo s velikim naporima može odrediti izvorni niz brojeva.

Neke činjenice iz teorije brojeva.

Djeljivost

Broj a djeljiv je s brojem d kada je a višekratnik od d. Postoji nekoliko načina označavanja djeljivosti:

$d\|a$	d dijeli a, d je djelitelj od a;
$a=k*d$	a je višekratnik od d.

Najmanji djelitelj od a je $d=1$, a najveći $d=a$. To su trivijalni djelitelji. Netrivijalni djelitelji zovu se faktori.

Prosti ili prim brojevi

Broj $a>1$ koji nema faktora (ima samo djelitelje 1 i a) je prosti ili prim broj.

Teorem dijeljenja

Za svaki cijeli broj a i bilo koji pozitivni cijeli broj n postoje jedinstveni cijeli brojevi:

- Kvocijent, količnik q i
- Reziduum, ostatak r (uz $0\leq r\leq n$),

tako da vrijedi:

$$a=q*n+r.$$

Možemo pisati:

$$q=floor(a/n) \text{ i}$$

$$r=a \bmod n,$$

odnosno:

$$a=floor(a/n) + (a \bmod n),$$

$$a \bmod n = a - floor(a/n)*n.$$

Ekvivalentnost po modulu, kongruentnost

Broj "*a* je ekvivalentan broju *b* po modulu *n*", ako je

$$a \bmod n=b \bmod n.$$

Kaže se da su *a* i *b* kongruentni po modulu *n* i piše se:

$$a=b \ (mod \ n).$$

Relativno prosti brojevi

Brojevi *a* i *b* su relativno prosti ako je najveći zajednički djelitelj brojeva *a* i *b* jednak 1, tj. brojevi *a* i *b* nemaju zajedničkih faktora ili *nzd (a,b)*=1.

Eulerova phi funkcija

Neka je $Z_n=\{0,1,2,...n-1\}$ prsten u kojemu su definirane operacije zbrajanja, oduzimanja i množenja po modulu *n*.

Neka je Z_n^* podskup koji se sastoji od elemenata skupa Z_n koji su relativno prosti u odnosu na *n*, tj.:

$$Z_n^*=\{a \text{ element } Z_n \ , \ nzd(a,n)=1\}$$

Broj elemenata skupa Z_n^*, tj. kardinalnost skupa $|Z_n^*|$ jednaka je Eulerovoj *phi* ili *totient* funkciji $\varphi(n)$.

Ako je $n=p$ prosti broj onda je $\varphi(p)=p-1$. Ako *n* ima rastav na proste faktore $n=p_1^{e1} \ ,p_2^{e2} \ ...p_n^{en}$ onda je

$$\varphi(n)=(1-1/p_1)\ (1-1/p_2)\ldots\ (1-1/p_k).$$

Ako je $n=p*q$, gdje su p i q prosti brojevi onda je

$$\varphi(n)=n(1-1/p)\ (1-1/q)=(p-1)(q-1).$$

Eulerov teorem

Za svaki prirodni broj $n>1$ vrijedi

$a^{\varphi(n)}=1\ (mod\ n)$ za sve *a element* Z_n^*

Fermatov teorem

Posebno za proste brojeve p vrijedi

$a^{p-1}=1\ (mod\ p)$ za sve *a element* Z_p^*

S obzirom da je $Z_p^*=\{1,2,\ldots,p-1\}$ Fermatov teorem vrijedi za sve brojeve iz Z_p s izuzetkom broja 0.

Diskretni logaritam ili indeks

Neka je a osnovni korijen od Z_n^* i b jedan element od Z_n^*. Postoji takav x tako da je

$$a^x \equiv b\ (mod\ n).$$

Broj x je diskretni logaritam ili indeks broja $b\ (mod\ n)$ u odnosu na bazu a.

Primjena kineskog teorema ostatka

Kineski teorem ostatka (Sun-Tsu, oko 100. godine) dovodi u vezu sustav jednadžbi po modulima koji su međusobno po parovima relativno prosti s jednadžbom po modulu koji je jednak njihovu umnošku.

Neka je $n=n_1 * n_2 *... * n_{1k}$ gdje su svi parovi faktora relativno prosti. Teorem kaže da je struktura Z_n identična kartezijevom produktu $Z_{n1} * Z_{n2} *... * Z_{nk}$.
Konkretno, za $n_1=p$ i $n_2=q$ to znači da za bilo koja dva cijela broja x i a vrijede jednadžbe:

$$x \equiv a \pmod{p},$$
$$x \equiv a \pmod{q}$$

onda i samo onda ako je

$$x \equiv a \pmod{n}.$$

3.2 Asimetrični kriptosustav RSA

Kao što je već rečeno, asimetrični kriptosustavi imaju različite ključeve kriptiranja K_E i dekriptiranja K_D i mogu se opisati već navedenim izrazima:

$$C = E(P, K_E),$$
$$P = D(C, K_D),$$
$$P = D(E(P, K_E), K_D).$$

Jedan od takvih sustava (koji je postao standard u svijetu) razradili su autori Ron Rivest, Adi Shamir i Len Adleman, po čijim je početnim slovima prezimena sustav dobio svoj naziv RSA.
Taj je sustav razrađen na osnovi svojstava brojeva objašnjenima u prethodnom odjeljku.

3.2.1 Izgradnja RSA sustava

1) Odabiru se dva velika prosta broja p i q ($p > 10^{100}$, $q > 10^{100}$).
2) Izračunava se umnožak $n=p*q$.
3) Izračunava se umnožak $\varphi(n)=(p-1)(q-1)$
4) Odabire se broj $d < \varphi(N)$ i relativno prost u odnosu na $\varphi(n)$, tj. koji nema zajedničkih faktora s $\varphi(n)$.

5) Izračunava se broj $e< \varphi(N)$ tako da bude $e*d=1(mod\ \varphi(N))$, što se drugačije može napisati kao $e*d=k*\varphi(N)+1$.
6) Par $K_E=(e, n)$ obznanjuje se i proglašava javnim ključem (engl. *public key*)
7) Par $K_D=(d, n)$ se taji i postaje privatni ključ (engl. *private key*)

Kriptiranje se obavlja funkcijom kriptiranja

$$C = E(P, K_E) = RSA(P, K_E) = P^e \bmod n,$$

a dekriptiranje funkcijom dekriptiranja

$$P = D(C, K_D) = RSA^{-1}(C, K_D) = C^d \bmod n.$$

3.2.2 Zašto je RSA kriptosustav korektan?

Pogledajmo što se dobiva dekriptiranjem kriptiranog teksta, tj. što daje:

$$RSA^{-1}(RSA(P, K_E), K_D).$$

Odnosno:

$$(P^e \bmod n)^d \bmod n = P^{e*d} \bmod n.$$

S obzirom da je

$$e*d = k*\varphi(n)+1 = k*(p-1)(q-1)+1,$$

može se za one P koji nisu kongruentni s 0 ($mod\ p$) upotrebom Fermatova teorema pisati:

$$\begin{aligned} P^{e*d} &\equiv P^{k(p-1)(q-1)+1} && (\bmod p) \\ &\equiv P(P^{(p-1)})^{k(q-1)} && (\bmod p) \\ &\equiv P(1)^{k(q-1)} && (\bmod p) \\ &\equiv P && (\bmod p) \end{aligned}$$

To je, također, trivijalno ispunjeno i za

$$P \equiv 0 \qquad (\bmod p).$$

Jednako tako vrijedi i:

$$
\begin{aligned}
P^{e*d} &\equiv P^{k(p-1)(q-1)+1} && (\text{mod } q) \\
&\equiv P(P^{(q-1)})^{k(p-1)} && (\text{mod } q) \\
&\equiv P(1)^{k(p-1)} && (\text{mod } q) \\
&\equiv P && (\text{mod } q)
\end{aligned}
$$

Dakle vrijedi:

$$
\begin{aligned}
P^{e*d} &\equiv P && (\text{mod } p), \\
P^{e*d} &\equiv P && (\text{mod } q),
\end{aligned}
$$

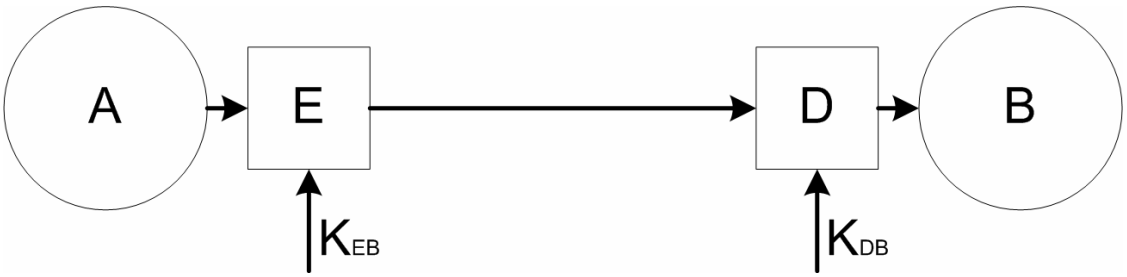
što je u skladu s kineskim teoremom ostataka ispunjeno samo ako je

$$P^{e*d} \equiv P \qquad (\text{mod } n).$$

Prema tome RSA sustav je korektan.

3.2.3 Komuniciranje upotrebom kriptosustava RSA

Bob koji želi komunicirati s drugim učesnicima obznanjuje svoj javni ključ kriptiranja K_{EB} i čuva samo za sebe svoj privatni ključ dekriptiranja K_{DB}. Alica koji koji želi poslati poruku P Bobu saznaje njegov javni ključ K_{EB}, kriptira poruku s tim ključem i šalje je Bobu. Jedino Bob zna svoj privatni ključ dekriptiranja K_{EB} i jedino on može dekriptirati poruku.



Slika 3.1 Komunikacija Alica i Boba

Kriptiranje bi se moglo obavit tako da se razgovijetni tekst P podijeli na niz brojeva jednake bitovne duljine:

$$P = P_0\, P_1\, P_2 \ldots P_i..$$

Kriptirani tekst dobio bi se tako da se kriptira svaki P_i

$$C_i = RSA(P_i, K_E) = P_i^e \bmod n$$

i dobije

$$C = C_0\, C_1\, C_2 \ldots C_i..$$

Na odredišnoj bi se strani tada obavilo dekriptiranje svakog C_i i ponovno uspostavilo razgovijetni tekst.

3.2.4 Dobrota RSA kriptosustava

Dobrota RSA kriptosustava zasniva se na teškoći faktoriziranja velikih brojeva. Naime, uz objavljeni javni ključ $K_E=(e,n)$ uljez bi mogao odrediti privatni ključ $K_D=(e,n)$ ako uspije faktorizirati broj n tj. saznati proste brojeve p i q.
Tada bi on mogao izračunati $\varphi(n)$ i odrediti pripadni d iz uvjeta

$$e*d=k*\varphi(n)+1.$$

Međutim, faktoriziranje velikih brojeva je vrlo teško. Do danas nema drugog načina do dijeljenja nizom brojeva 2,3,5,..,√n. U najgorem slučaju kada je n prosti broj imat ćemo $O(\sqrt{n})$ operacija. Ako broj n ima m bitova onda je:

$$n \approx 2^{m/2}$$

te je složenost faktoriziranja $O(2^{m/2})$.
Do sada, osim faktoriziranja broja n, nisu pronađeni drugi načini za razbojanje RSA kriptosustava. Pokazuje se da je s današnjom računalnom snagom moguće faktorizirati 512 bitne brojeve, ali je već nemoguće u razumnom vremenu faktorizirati 1024 bitne brojeve. To bi značilo da uz $n=p*q$ zadovoljavaju prosti brojevi koji imaju po 512 bitova. S obzirom da je $2^{512} \approx 10^{150}$, to znači da bi trebalo pronalaziti proste brojeve s oko 150

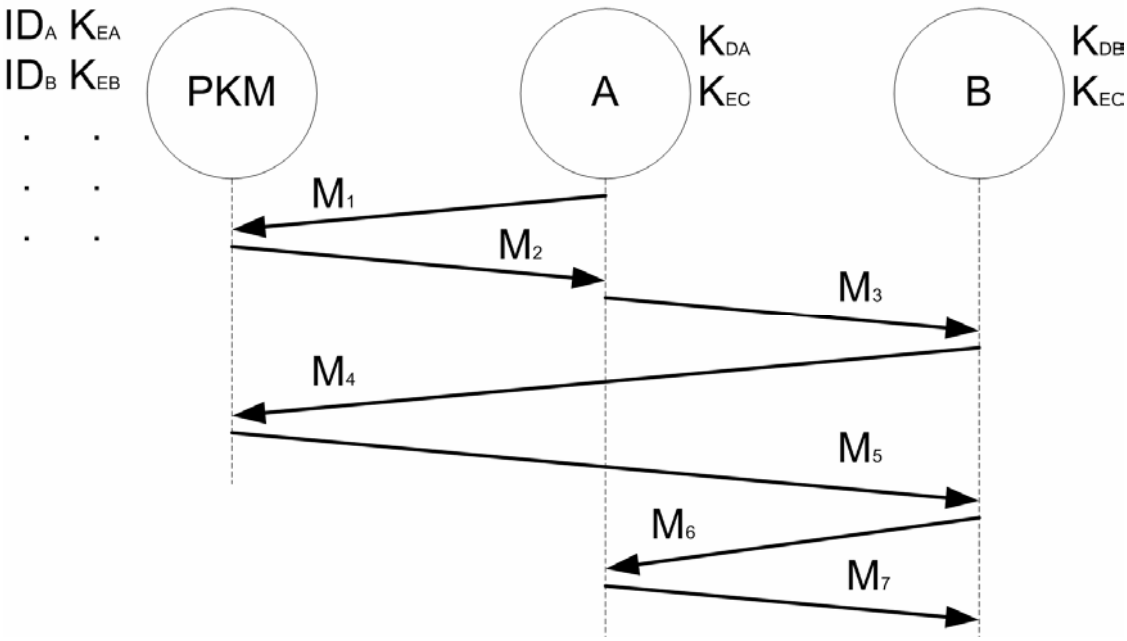
znamenaka. Takvih se brojeva može pronaći mnogo. U intervalu između 10^{140} i 10^{150} ima $2.89*10^{147}$ prostih brojeva.

3.2.5 Raspodjela ključeva u zatvorenom asimetričnom kriptosustavu

U asimetričnom kriptosustavu raspodjeljuju se samo javni ključevi. Ti ključevi ne moraju biti tajni i zbog toga se na prvi pogled čini da s njihovim prijenosom nema problema.

U jednom zatvorenom sustavu svi potencijalni sudionici moraju se prijaviti. Prilikom prijava njima se dodjeljuje par ključeva. Svoj privatni ključ oni čuvaju kod sebe dok se pripadni javni ključ pohranjuje zajedno s njihovim identifikatorom u tablicama pouzdanog poslužitelja kojeg možemo nazvati centrom za raspodjelu javnih ključeva (engl. *public key manager - PKM*).

Kada sudionik A želi komunicirati sa sudionikom B sigurnim kanalom on će zatražiti od PKM njegov javni ključ. Time se izbjegava mogućnost da neki napadač generira svoj par ključeva i ponudi svoj javni ključ te uspostavi prividno sigurni komunikacijski kanal sa sudionikom A. Dodatno je potrebno u postupak raspodjele, odnosno obznanjivanja javnih ključeva sudionika ugraditi autentifikacijske mehanizme.



Slika 3.2 Raspodjela ključeva u zatvorenom asimetričnom kriptosustavu

Dakle, svakom sudioniku prijavljenom u sustav dodjeljuje se javni K_{EI} i privatni K_{DI} ključ. Centar za raspodjelu ključeva također ima svoj javni ključ K_{EC} i privatni ključ K_{DC}. Svaki sudionik sustava čuva svoj privatni ključ i javni ključ centra za dodjelu ključeva. Centar čuva svoj privatni ključ i tablicu u kojoj su uz identifikatore pohranjeni javni ključevi svih prijavljenih sudionika.

4 Literatura

1. prof. d. sc. Leo Budin: "Predavanja iz predmeta Operacijski sustavi II",
2. http://sigurnost.zemris.fer.hr/
3. http://en.wikipedia.org/wiki/RSA/
4. http://www.rsasecurity.com/