UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Problem kriptografov pri večerji

Anonimno pošiljanje sporočil

Seminar iz kriptografije in teorije kodiranja

Mentor:
prof. dr. Aleksandar Jurišić

Avtorica:
Meta Kirn

Ljubljana, 2004

Kazalo

Uvod

Zakaj sploh *anonimnost*? V šoli nas nadleguje sošolec, ki je precej močnejši od nas. Radi bi ga zatožili učiteljici, vendar se ga bojimo. Lepo bi bilo, če bi ga lahko zatožili tako, da ne bi nihče vedel, da smo ga zatožili prav mi. Učiteljica bi izvedela za njegove lumparije, mi pa bi ostali neimenovani, torej *anonimni*.

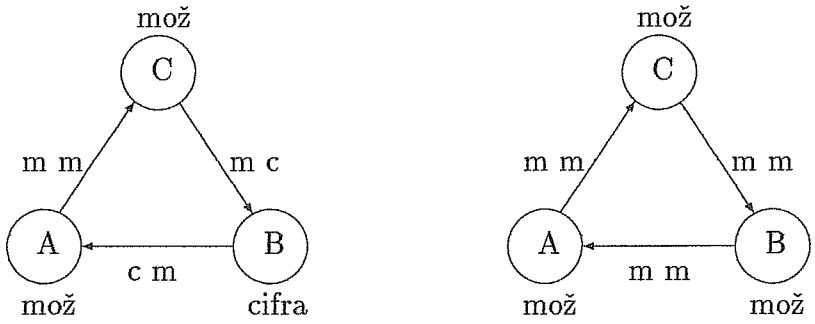
V današnjih računalniških časih pa se sploh zdi nemogoče nadzirati, kje vse krožijo in se uporabljajo naši podatki, ki smo jih morda čisto nevede razkrili med brskanjem po internetu ali v spletni klepetalnici. Tudi pri nakupu preko interneta ali kataloga ni niti najmanj nujno, da prodajalec ve, kdo smo ali da celo izve za naše osebne podatke.

Po drugi strani pa so tudi organizacije ranljive za zlorabe s strani posameznikov. Ta problem bi lahko omejile z uvedbo večjega nadzora posameznikov, kar pa nas zopet pripelje k prejšnjemu problemu. Mogoče pa je razviti pristop, s pomočjo katerega se lahko v precejšnji meri izognemo tem težavam. Pogledali si bomo postopek, ki omogoča pošiljanje sporočil, ne da bi bil pri tem razkrit njihov izvor.

Najprej bomo razložili, kako je lahko znanstvenik vedel, da je eden od njegovih kolegov plačal večerjo, ni pa mogel ugotoviti kateri. V nadaljevanju znanstveniki ugotovijo, da se da postopek uporabiti tudi za pošiljanje daljših sporočil med več udeleženci, pri čemer pa je anonimnost lahko tudi ogrožena, če se nekateri od udeležencev odločijo združiti moči z namenom, da odkrijejo izvor sporočila katerega od sodelujočih. Poskusili bomo najti način, da se takim pastem kar v največji možni meri izognemo. Videli bomo, da lahko model zelo nazorno predstavimo z grafom. Postopek pa je mogoče uporabiti tudi za anonimno pošiljanje sporočil v računalniških omrežjih. Ogledali si bomo nekaj praktičnih vidikov ter kakšne so možnosti za preprečevanje zlorab anonimnega pošiljanja sporočil.

Večerja

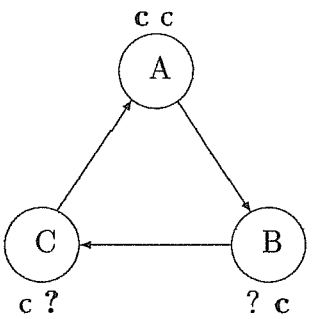
Znanstveniki Andrej, Bojan in Cene se dobijo pri večerji, da bi se pogovorili o skrivnem projektu, ki ga morajo skupaj izpeljati. Po večerji jim natakar pove, da je njihova večerja že plačana in da želi ostati plačnik večerje anonimen. Bodisi je to podjetje, ki je naročilo projekt, bodisi plača eden izmed njih. Znanstveniki se odločijo spoštovati pravico vsakega od njih, da anonimno plača večerjo, vseeno pa bi radi izvedeli, ali je račun poravnalo podjetje. Zato izvedejo naslednji postopek: Vsak znanstvenik skrivaj za svojim jedilnim listom vrže kovanec, nato pa si ogleda še rezultat svojega levega soseda in pove, če sta kovanca, ki ju vidi, pokazala isti ali različni strani. Dogovorijo se, da če je plačnik eden od trojice, potem ta pove ravno nasprotno od tistega, kar vidi. Sodo število razlik pomeni, da je plačnik podjetje, liho pa, da je večerjo plačal eden od znanstvenikov (Slika 1)



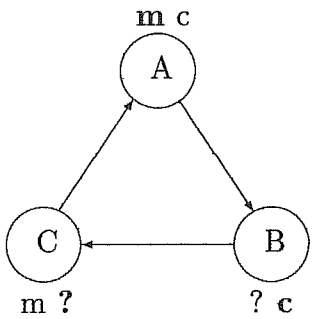
Slika 1: Možna sta dva izida: bodisi pri enem od znanstvenikov pokaže kovanec različno stran kot pri drugih dveh bodisi pade pri vseh treh na isto stran. V prvem primeru vidita različna izida Bojan in Cene, torej dva, v drugem pa nihče.

Prepričajmo se, da v primeru, ko je plačnik eden od trojice, znanstvenik, ki to ni, res ne more ugotoviti, kateri od drugih dveh plača večerjo. Recimo, da Andrej, ki ni plačnik, vidi dve cifri, Bojan trdi, da vidi dva enaka izida, Cene pa različna. Andrej ne vidi, kaj je vrgel Cene. Če je vrgel moža, je plačnik on, sicer plača Bojan (Slika 2).

Če Andrej vidi različna izida in druga dva trdita, da vidita različna izida, je plačnik tisti, pri katerem je izid, ki ga Andrej pozna, enak kot skriti izid. Če pa oba trdita, da vidita enaka izida, je plačnik tisti, pri katerem je znani izid različen od skritega (Slika 3). Ker sta v vseh primerih oba izida enako verjetna, Andrej ne more ugotoviti, kateri od drugih dveh je plačnik večerje.



Slika 2: Andrej vidi enaka izida.



Slika 3: Andrej vidi različna izida.

Z uporabo zgornjega postopka je torej plačnik poslal enostavno sporočilo: „Plačal sem.“, ki ga ostala dva ne moreta izslediti. Za to je bil potreben samo en met kovanca.

Med večerjo se znanstveniki spustijo v pogovor, kako bi bilo s pomočjo zgornjega postopka mogoče pošiljati sporočila poljubne dolžine, ne da bi bil pri tem odkrit njihov

izvor. Seveda bi bilo potrebno postaviti nekaj pravil, ki bi se jih udeleženci morali držati. Taki zbirki pravil bomo rekli *protokol*.

Daljše sporočilo lahko predstavimo z zaporedjem znakov, ki jih imenujemo *biti*. Vsak bit ima lahko vrednost 0 ali 1, zato taki predstavitvi sporočila pravimo *dvojiški zapis* sporočila. Udeleženci ponavljajo zgornji protokol in ko želi eden od njih poslati sporočilo, začne objavljati obratno od tistega, kar vidi, v tistih krogih, ki ustrezajo enkam v dvojiškem zapisu njegovega sporočila. Če ugotovi, da istočasno z njim oddaja še kateri od preostalih udeležencev, počaka nekaj krogov, nato pa začne ponovno oddajati. Število krogov, ko čaka, izbere naključno izmed možnosti, ki so vnaprej dogovorjene.

Posplošitev

Pri pogovoru znanstveniki ugotovijo, da bi bilo zgornji protokol mogoče uporabiti tudi za pošiljanje sporočil med več udeleženci. Poglejmo, kako bi to izvedli. Vsak udeleženec ima z vsakim od preostalih udeležencev skupen nek skrivni bit, ki ga bomo imenovali *ključ*. Ko pride vrsta nanj, udeleženec objavi parnost vsote vseh svojih bitov. Če želi oddati sporočilo, svoji vsoti prišteje 1. Če eden od udeležencev (ali liho število udeležencev) oddaja sporočilo, je vsota vseh bitov vseh udeležencev liha, sicer pa soda, saj v njej vsak od bitov nastopi dvakrat. Za n krogov ima vsak od udeležencev z vsakim skupen n-bitni ključ in i-ti bit v ključu uporabi samo v i-tem krogu. Če udeleženec pri oddajanju svojega sporočila ugotovi, da istočasno oddaja sporočilo še nekdo drug (vsota vseh bitov je soda, čeprav bi morala biti liha), počaka naključno število krogov, nato pa poskusi ponovno. Tudi če sporočila istočasano oddaja liho število udeležencev, morajo le-ti najkasneje po nekaj krogih ugotoviti, da niso edini, ki oddajajo. To se ne bi zgodilo samo takrat, ko bi liho število udeležencev istočasno oddajalo povsem enaka sporočila.

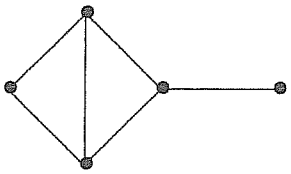
Če želimo, da pošiljatelj sporočila v resnici ostane anonimen, mora vsak od udeležencev varovati dve skrivnosti:

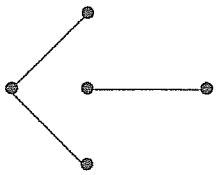
- ključe, ki jih deli z ostalimi udeleženci,
- dejstvo, ali v določenem krogu oddaja ali ne.

Podatka, za katera ni nujno, da sta skrivnost, pa sta:

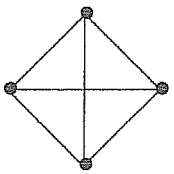
- kdo deli ključe s kom (v praksi ni nujno, da udeleženci delijo ključe vsak z vsakim),
- prispevek posameznega udeleženca v določenem krogu.

Model delitve ključev lahko nazorno predstavimo z grafom, to je matematično strukturo, sestavljeno iz vozlišč in povezav. V našem primeru z vozlišči predstavimo udeležence, s povezavami pa ključe. Vozlišči sta povezani natanko takrat, ko si udeleženca, ki ju predstavljata, delita ključ. Rekli bomo, da je graf *povezan*, če lahko od kateregakoli vozlišča v njem pridemo po povezavah do kateregakoli drugega (Slika 4).





Slika 4: Prvi graf je povezan, drugi pa ne.



Slika 5: poln graf

V nadaljevanju bomo predpostavili, da je model delitve ključev povezan graf. V nasprotnem primeru lahko namreč posebej obravnavamo vsakega od povezanih grafov iz katerih je sestavljen naš model. Če udeleženci delijo ključe vsak z vsakim, pa je model delitve *poln graf (polno povezan graf)*. To pomeni, da je vsako od vozlišč povezano z vsakim (Slika 5).

Rekli bomo še, da *množica ključev vidi množico vozlišč* v (povezanem) grafu, ki ga dobimo, če iz prvotnega grafa odstranimo povezave, ki predstavljajo te ključe.

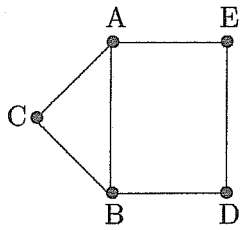
PRIMERA:
Množica vozlišč, ki jo vidi prazna množica (opazovalec, ki ni udeležen), je kar celoten graf. Celotna množica ključev pa vidi samo množice z enim elementom. Ker je anonimnost možna le v neki skupini, je seveda očitno, da en sam udeleženec ne more anonimno pošiljati sporočil.

Sodelovanje udeležencev

Nekateri od udeležencev lahko sodelujejo med seboj in tako poskusijo izslediti sporočila drugih udeležencev. To lahko storijo tako, da drug drugemu odkrijejo vse svoje ključe ali le nekatere od njih, lahko pa tudi drug drugemu izdajo, ali oddajajo sporočilo ali ne.

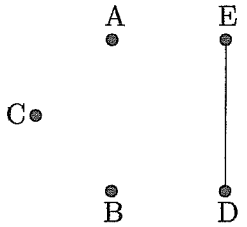
Če udeleženci delijo ključe vsak z vsakim, odkrijejo pošiljatelja le, če se vsi združijo proti njemu. V tem primeru ni nujno, da drug drugemu odkrijejo svoje ključe, saj zadostuje že, če poznajo svojo skupno parnost oddanih bitov v določenem krogu.

Po večerji se Andreju, Bojanu in Cenetu pridružita še znanstvenici Dora in Eva in odločijo se preizkusiti protokol. Model delitve ključev je graf na Sliki 6.

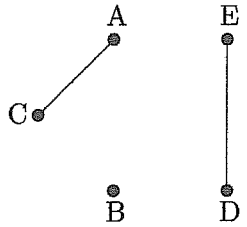


Slika 6

Če v grafu, ki ni poln, neka skupina udeležencev združi vse svoje ključe, potem ta množica ključev vidi vsakega od njih kot množico z enim elementom – zarotniki torej popolnoma žrtvujejo svojo anonimnost. Če pa pri takem sodelovanju graf razpade na več grafov, lahko ugotovijo, iz katere od njih prihaja sporočilo. Število možnih pošiljateljev se tako zmanjša. Andrej in Bojan združita svoje ključe in na ta način prvotni graf razpade na dva grafa (Slika 7). V tem primeru oba poznata vse ključe, ki jih deli Cene in zato vesta za vsako njegovo sporočilo. Vesta pa tudi za vsa sporočila drug drugega.



Slika 7



Slika 8

Seveda ni nujno, da udeleženci združijo vse svoje ključe, lahko se odločijo izdati samo nekatere od njih. Pri dobrem izboru lahko tudi v tem primeru prvotni graf razpade na več grafov. Če se naprimer Andrej odloči, da Bojanu ne bo izdal ključa, ki ga deli s Cenetom, Bojan lahko ugotovi le, če sporočilo prihaja iz grafa, ki predstavlja Bojana in Ceneta, ali iz tistega, ki predstavlja Doro in Evo, medtem ko Andrej lahko izsledi sporočilo, če to prihaja od Bojana ali od Ceneta (Slika 8).

Možnosti za praktično izvedbo protokola

Znanstvenikom se porodi ideja, da bi ta protokol lahko uporabili tudi za izmenjavo sporočil v zvezi z njihovim skrivnim projektom kar od doma. To bi lahko počeli kar preko računalniškega omrežja, v katerem pa so vključeni tudi ostali uporabniki. Če so računalniki med sabo povezani v obroč, lahko to storijo na podoben način kot pri

večerji. Eden od udeležencev pošlje sporočilo (bit), ki potem potuje od enega udeleženca do drugega, pri čemer vsak prišteje vsoto svojih ključev, preden ga pošlje naprej. Ko sporočilo prepotuje cel krog, je le-to vsota vseh bitov, ki so jih objavili udeleženci. Da bi to sporočilo prišlo res do vseh uporabnikov, pa mora prepotovati še en krog.

Tak način pošiljanja sporočil seveda zahteva precej zmogljivo omrežje, saj mora vsak bit sporočila celotno pot prepotovati dvakrat, za razliko od sporočil, kjer sta naslovnik in pošiljatelj znana – tu sporočilo potuje samo od pošiljatelja do naslovnika. Prav tako je potrebno v različnih računalniških omrežjih izvedbo protokola prilagoditi njihovim lastnostim (gl. Chaum [1] in Tannenbaum [9]).

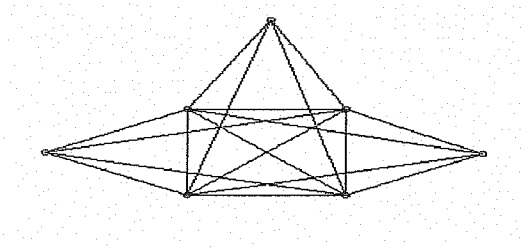
Razdeljevanje ključev

V pogovoru po večerji se znanstvenikom postavita še dve pomembni vprašanji. Prvo je, na kak način razdeliti ključe, da bi bila možnost za njihovo neželeno odkritje čim manjša ter da bi kar v največji meri preprečili sodelovanje nekaterih uporabnikov na škodo drugih. Drugo vprašanje pa je, kakšne so možnosti za preprečevanje in odkrivanje zlorab.

Za ključe se lahko uporabniki dogovorijo vnaprej. Lahko bi naprimer eden od dvojice, ki bo delila ključ izvedel več metov kovancev, zapisal rezultate, nato pa jih posredoval udeležencu, s katerim jih bo delil. Lahko pa si jih razdelijo preko omrežja z uporabo metod za razdeljevanje ključev.(gl. Merkle [6])

Omenili smo že, da je zelo pomembno tudi kdo bo s kom delil ključe. V praksi bi radi imeli manj kot $n(n-1)/2$ ključev, kolikor jih potrebujemo za n udeležencev, da bi bil model poln graf in bi udeleženci imeli najmanjšo možnost za izsledite sporočila. Če pa je model cikel, posameznik ne more odkriti nič, katerakoli dva udeleženca, ki sodelujeta, pa razbijeta graf v dve komponenti in če delita ključ z istim udeležencem, izvesta vse o njegovih sporočilih.

Pri deljenju ključev je zelo dobro, če najdemo tako skupino udeležencev, za katere ni verjetno, da bodo sodelovali med seboj (recimo udeležence z nasprotnimi interesi). Ti udeleženci delijo ključe vsak z vsakim, ostali pa vsak z vsemi od teh (Slika 9). Tako posameznika ni možno odkriti, razen če vsi udeleženci polno povezanega grafa sodelujejo med seboj, kar pa po predpostavki ni verjetno.



Slika 9

V velikih skupinah sodelujočih je koristno vzpostaviti hierarhijo. Recimo, da ima vsaka skupina, katere model je poln graf, predstavnika, množica predstavnikov skupin pa je tudi polno povezana. Vsak od predstavnikov vsoti svoje skupine prišteje še svoj bit, preden pošlje sporočilo naslednjemu predstavniku. V tem primeru bi morali vsi predstavniki, razen morda enega, sodelovati med seboj, da bi ugotovili, iz katere skupine prihaja sporočilo, da pa bi odkrili posameznika, bi morali sodelovati vsi člani skupine.

Pošiljanje sporočil s kriptosistemom javnih ključev

Kaj pa, če bi Andrej želel poslati sporočilo samo Bojanu in bi želel, da Bojan tudi ve, da mu sporočilo pošilja Andrej, vsi ostali, ki bi bili takrat priključeni v omrežje pa ne bi smeli vedeti niti kdo pošilja sporočilo, niti komu? V tem primeru lahko Andrej sporočilo digitalno podpiše in ga zašifrira z Bojanovim javnim ključem. Digitalni podpis je digitalna različica lastnoročnega podpisa, ki pa omogoča še precej več (gl. npr. http://www.sigov.si/tecaj/kripto/kr-podp.htm). O šifriranju z javnimi ključi pa si lahko več prebereš npr. v [7]. Vsak od udeležencev potem poskuša sporočilo odšifrirati s svojim zasebnim ključem, vendar bo to uspelo samo Bojanu. Seveda je to početje zelo zamudno, zato se lahko udeleženci vnaprej dogovorijo za neko zaporedje bitov, ki ga dodajo na začetek sporočila. Tako posameznik poskuša odšifrirati sporočilo le, če prepozna kombinacijo.

Zlorabe in njihovo preprečevanje

Poglejmo si še, kako pri uporabi protokola lahko odkrijemo in ustavimo udeležence, ki sistem anonimnega pošiljanja sporočil uporabljajo na neprimeren način. Ne da se preprečiti, da bi kateri od uporabnikov neprestano oddajal in tako povsem zaprl kanal. Možno pa je zlonamerne uporabnike odkriti in tudi ustaviti, če sistem izpolnjuje tri zahteve:

- Graf deljenja ključev je javno odobren. Že v začetku smo omenili, da ni skrivnost, kdo deli ključe s kom, tukaj pa *zahtevamo*, da je ta podatek znan vsem udeležencem in da se z njim tudi strinjajo.

- Nobeden od udeležencev ne more spremeniti svojega prispevka v določenem krogu, potem ko je videl, kaj so objavili drugi. Ta zahteva prepreči zlonamernemu uporabniku, da bi spremenil svoj prispevek, potem ko je videl, kaj so objavili ostali uporabniki. Vsi udeleženci se namreč na nek način zavežejo svojim prispevkom, preden jih pošljejo v omrežje. V računalniških omrežjih je to mogoče uresničiti z *enosmerno funkcijo*. To je taka funkcija f, za katero velja, da je praktično nemogoče izračunati x, če poznamo samo f in $y = f(x)$ (gl [10], str. 119).

- V nekaterih krogih je objavljeno, kdo je vsoti svojih ključev prištel 1. To lahko izvedemo tako, da po več krogov združimo v bloke in prvi blok uporabimo za to, da udeleženci rezervirajo kroge, v katerih želijo oddajati. To storijo tako, da v nekem naključno izbranem krogu prvega bloka vsoti svojih ključev prištejejo 1. Udeleženec, ki je „povzročil“ liho vsoto naprimer v 5. krogu prvega bloka, bo začel oddajati sporočilo v 5. krogu 2. bloka itd. Dogovorimo se še, da vsak od udeležencev rezervira enkrat v vsakem bloku, ki je določen za rezervacijo. Če kateri od udeležencev želi s svojim oddajanjem preplaviti omrežje, bo v bloku, v katerem je rezerviral, število lihih objav precej večje od števila udeležencev. Če razkrijemo, kdo je oddajal v takem bloku za rezervacijo, s tem ne odkrijemo uporabnikov, ki so sistem uporabljali na primeren način.

Poglejmo primer, ko eden od uporabnikov zlorabi sistem, v katerem so izpolnjene zgornje tri zahteve. Lahko se naprimer zgodi, da kateri od udeležencev želi sistem uporabiti v kriminalne namene. Če nekdo pošlje npr. grožnjo, bi izvor tega sporočila radi našli in v tem primeru lahko sodišče odredi, da morajo vsi udeleženci razkriti svoje bite za krog, v katerem je bilo poslano sporočilo. Zlonamernež pa lahko seveda laže o nekem številu bitov, ki jih deli. Če laže o sodem številu bitov, je sumljiv, saj je njihova vsota različna od tiste, ki jo je objavil. Če pa laže o lihem številu bitov, ki jih deli, postane sumljiv uporabnikom, s katerimi deli ključe. Tako vrže sum na vse uporabnike, ki z njim delijo ključe (tudi nase), pri tem pa tisti uporabniki, ki so nedolžni vedo, da so bili po krivem obtoženi in tudi, kdo jih je obtožil, tako da je najmanj kar lahko storijo to, da ne delijo več ključev s to osebo.

Da bi se izognili temu, da neodgovorni uporabnik razprši krivdo na skupino vseh, ki z njim delijo ključe, bi načeloma lahko vsak od udeležencev od tistega, s katerim deli bite, zahteval digitalni podpis za vsak bit. Vendar bi bilo za večino aplikacij zelo zamudno razbirati digitalne podpise za vsak bit posebej, zato se temu izognemo tako, da večje število bitov v ključu najprej stisnemo, dodamo naključne bite in šele nato digitalno podpišemo. To pa seveda vpliva na anonimnost, saj moramo pri preverjanju digitalnega podpisa razkriti cel blok sporočila.

Zaključek

Opisani protokol je nastal na osnovi tako imenovanega problem kriptografov pri večerji (ang. Dining Cryprographers Problem), zato ga imenujemo tudi DC-net protokol. Poznamo pa še druge protokole, ki jih prav tako lahko uporabimo za anonimno pošiljanje sporočil. Eden od takih je naslednji poenostavljen postopek, ki pa ga lahko uporabimo

pri elektronskem plačevanju ali volitvah. Pri tem pa ne razkrijemo svoje identitete niti banki niti trgovini, v kateri opravimo nakup.

Uporabnik v ovojnico zapečati prazen papir in kos indigo papirja ter jo odnese v banko. V banki dvignejo z njegovega računa želeno vsoto, na zunanjo stran neodprte ovojnice potrdijo dvignjeno vrednost ter uporabniku vrnejo neodprto ovojnico. Ko želi posameznik opraviti plačilo, odstrani ovojnico ter pošlje papir, na katerem je viden odtis potrdila banke, v trgovino, v kateri je opravil nakup. Iz trgovine pošljejo potrdilo v banko in od tam prejmejo plačilo, ki je navedeno na papirju. Banka je seveda izdala več takih potrdil, tako da ne ve, komu je bilo izdano potrdilo, ki ga prejme iz trgovine (gl. Chaum [4]).

Literatura

[1] D. Chaum,
http://www.cam.cornell.edu/~sharad/herbivore/dcnets.html

[2] A. Acquisti,
http://smg.media.mit.edu/cscw2002-privacy/submissions/alessandro.pdf

[3] http://www.sigov.si/tecaj/kripto/kr-podp.htm

[4] D. Chaum, Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, vol. 28, 1985, str. 1030-1044.

[5] D. Chaum, Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM, vol. 24, 1981, str. 84-88.

[6] R. C. Merkle, Secure Communications over Insecure Channels. Communications of the ACM, vol. 21, 1978, str. 294-299.

[7] M. Vencelj, Šifriranje z javnim ključem, Presek, letn. 22, 1994-1995, str. 354-357.

[8] S. A. Brands, Rethinking Public Key Infrastructures and Digital Certificates, Building in Privacy. Library of Congress Cataloging-in-Publication Data, 2001.

[9] A. S. Tannenbaum, Computer Networks. New Jersey: Prentice Hall, Englewood Cliffs, 1981.

[10] D. R. Stinson, Cryptography, Theory and Practice. Boca Raton, A CRC Press Company, 2000.