**SVEUČILIŠTE U ZAGREBU**

**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**

**MATEMATIČKI ODSJEK**

Mirna Hanžek

# ELEKTRONIČKO GLASANJE

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Filip Najman

Zagreb, rujan, 2018.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

# Sadržaj

# Uvod

Elektroničko glasanje (poznato i kao *e-glasanje*) odnosi se na glasanje pomoću elektroničkih sredstava koja pomažu pri procesu glasanja.
Ovisno o konkretnoj provedbi, elektroničko glasanje može koristiti samostalni elektronički uređaj za glasanje (takozvani *EVM*) ili računala povezana s internetom. Može obuhvaćati čitav niz internetskih usluga, od najosnovnijeg prijenosa rezultata glasanja pohranjenih u tablici, do potpuno funkcionalnog glasanja putem interneta pomoću kućanskih uređaja spojenih na internet. Unatoč tome, glasanje još uvijek nije u potpunosti automatizirano.
Stupanj automatizacije može biti ograničen na obilježavanje glasačkih listića ili se ručno može koristiti sustav unosa glasova, snimanje glasova, šifriranje podataka i prijenos podataka na poslužitelje te poredak i tabeliranje izbornih rezultata.
Upotrebljiv sustav elektroničkog glasanja mora zadovoljiti niz standarda koje su utvrdila regulatorna tijela i mora biti sposoban uspješno se nositi sa jakim zahtjevima koji se odnose na *sigurnost*, *točnost*, *integritet*, *brzinu*, *privatnost*, *provjerljivost*, *pristupačnost*, *ekonomičnost*, *zaštitu osobnih podataka*, *skalabilnost* i *ekološku održivost*.

Općenito, razlikujemo dvije glavne vrste elektroničkog glasanja:

- elektroničko glasanje koje fizički nadziru predstavnici vladinih ili nezavisnih izbornih tijela (npr. strojevi za elektroničko glasanje koji se nalaze na biračkim mjestima);
- daljinsko e-glasanje putem interneta (zvano *i-glasanje*), gdje birač elektroničkim putem dostavlja svoje glasove izbornim tijelima.

Zagovornici elektroničkog glasanja ističu da elektroničko glasanje može smanjiti troškove izbora i povećati građansko sudjelovanje tako što će postupak glasovanja učiniti prikladnijim. Iznimno je pogodno kada se gledaju rezultati glasanja iz dijaspore, koji se bilježe i prebrojavaju istovremeno kao i rezultati glasanja iz države. Smatra se da je način ovakvog glasanja bolji zbog bržeg bilježenja i prebrojavanja glasova.

S druge strane, kritičari tvrde da je bez papirnatog zapisa prebrojavanje teže, a elektronička manipulacija glasačkim listićima ili čak slabo pisani programski kod, mogla bi utjecati na rezultate izbora. Jedan od najvećih problema je kako osigurati da glasovi koji se šalju ne budu promijenjeni i kako potvrditi identitet glasača. U rješavanju tog problema koristi se **kriptografija**.
U ovom radu ćemo reći nešto općenito o povijesti elektroničkog glasanja, u kojim državama se provodilo i naravno kako se matematika i kriptografija koriste u elektroničkom glasanju.
Diplomski ispit napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 -
Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

# Poglavlje 1

# Povijest elektroničkog glasanja

## 1.1 Razvoj tehnologije

Kako bismo bolje shvatili razvoj elektroničkog glasanja kroz povijest, predstavljamo tehnologije koje su se koristile i prethodile elektroničkom glasanju.
To su *Glasački listići*, *Stroj s mehaničkom polugom*, *Bušene kartice*, *Optičko skeniranje glasačkih listića* i *Direktno bilježenje rezultata*. Za detaljniji opis navedenih tehnologija korišteni su isječci iz članaka [28].

### Glasački listići

Glasački listić je komad papira na kojem pišu imena kandidata pored kojih glasač može označiti svoj izbor kandidata. Glasanje je anonimno, a nakon što glasač označi svojeg kandidata, stavlja svoj glasački listić u glasačku kutiju. Takav stil glasačkog listića kasnije je nazvan "*Australian Secret Ballot*", a ime je dobio po državi u kojoj se prvi put upotrijebio - Australiji, 1856. godine. Troškove za glasačke listiće snosi vlada, a glasovi se prebrojavaju ručno.

### Stroj s mehaničkom polugom

Stroj s mehaničkom polugom (engl. *Mechanical Lever Machine*) patentirao je Jacob H. Myers 1889. godine te se njemu u čast tehnologija koja se zasniva na stroju s mehaničkom polugom naziva *Myers Automatic Booth*. U sistemu glasanja u kojem se koristi ovakav stroj, glasač najprije ulazi u kabinu s pregradom gdje se nalazi spomenuti stroj. Glasač povlači polugu dok ne dođe do imena kandidata za kojeg želi glasati i koji je onda označen te u tom trenutku staje povlačiti polugu. Kada je glasač gotov sa glasanjem tada izlazi iz kabine, a poluga se vraća u prvobitno stanje. U tom trenutku okreće se kotač koji se nalazi

u mehanizmu stroja. Kada se kotač okrene za puni krug, on pokreće drugi kotač koji radi na isti način kao i njegov prethodnik.
Ovakav mehanizam omogućava brojanje glasova, uz pretpostavku da je prije početka glasanja pozicija kotača bila postavljena na nulu. Ovakva tehnologija ima svoje prednosti u tome što spriječava višestruke odabire glasača, ubrzava proces glasanja i omogućava donekle pošteno glasanje, jer glasove broji stroj, a ne ljudi. Prvi strojevi s mehaničkom polugom su bili upotrebljeni 1892. godine u SAD-u, u državi New York, koja je i zadnja država u SAD-u koja je ukinula ovakav način glasanja. Očiti nedostatak ovakve tehnologije glasanja je taj što stroj ne ostavlja trag na papiru i ukoliko se pokvari poluga, ostali glasači više ne mogu glasati. [29]

Slika 1.1: Stroj s mehaničkom polugom

## Bušene kartice

Sustav glasanja koji koristi bušene kartice pojavio se sredinom dvadesetog stoljeća, iako se ideja takvog načina glasanja pojavila još u 1890-im godinama. Glasač buši rupu pored imena kandidata za kojeg želi glasati pomoću dobivenog uređaja. Nakon glasanja glasač ubacuje karticu u glasačku kutiju ili u poseban uređaj koji bilježi rezultate glasanja.
U SAD-u se koristio sustav *Votomatic*, kojeg je razvio Joseph P. Harris. Sustav Votomatic je bio prilično uspješan, budući da se do 1996. godine koristio od strane 37.3% registriranih glasača u SAD-u. Ipak, navedeni sustav je doživio krah 2000. godine kada je zbog neravnomjernog korištenja utjecao na rezultate predsjedničkih izbora. [1]

## Optičko skeniranje glasačkih listića

Sustav glasanja čija tehnologija se svodi na stroj koji se naziva optički skener prvi put se pojavljuje u državi Kalifornija u SAD-u 1962. godine. Ovakav način glasanja omogućuje

glasaču da zabilježi svoj izbor direktno na glasački listić ili karticu. Optički skener tada ”čita” izbor glasača i bilježi rezultate.

Postoje tri vrste sustava koji koristi optičko skeniranje. To su:

- **marksense sustavi** (engl. marksense systems)
- **sustavi koji koriste označivač elektronskih listića** (engl. electronic ballot marker, skraćeno *EBM*)
- **sustavi koji koriste digitalnu olovku** (engl. digital pen voting systems)

**Marksense sustavi** su najstariji od navedenih sustava. Glasač bilježi svoj odabir na način da ispunjava krug, pravokutnik ili elipsu, ili nastavlja niz ponuđen na glasačkom listiću. Neki sustavi, npr. *Sequoia Voting Systems* koriste analogne komparatore koji broje oznake koje su tamnije od originalnih i to označuju kao glas. Sustav *Avante Vote-Trakker* broji tamne i svijetle piksele na mjestu gdje je glasač trebao označiti svoj izbor te tako bilježe glas. Neki algoritmi su osjetljivi na oblik oznake i sveukupnu tamniju pozadinu, kao npr. *Election Systems & Software Model 100*.

**Označivač elektronskih listića** je uređaj koji osim što bilježi glasačev izbor, pomaže glasačima s invaliditetom. Naime, uređaj sadrži zaslon koji reagira na dodir i ostale tehnološke uređaje koji pomažu ljudima koji imaju problema sa sluhom, vidom itd. Prvi koji je patentirao ovakav uređaj bio je Belgijac Julien Anno 1991. godine. Taj uređaj je pomogao razvoju elektroničkog glasanja u Belgiji, budući da su glasački listići bili tiskani na više jezika, što je olakšalo glasanje manjinama zastupljenim u Belgiji. Eugene Cummings je 2003. godine patentirao označivač elektronskih listića nazvan *Automark*, dizajniran prvenstveno da bi se ispunio kriterij dostupnosti. Ovaj stroj se do 2016. godine koristio u deset država u SAD-u te devetnaest država širom svijeta. [10]

**Sustavi koji koriste digitalnu olovku** također koriste listiće na digitalnom papiru, a izbor glasača se prepoznaje pomoću male kamere u olovci koja bilježi što je glasač odabrao. Nakon glasanja, glasač listić ubacuje u glasačku kutiju i vraća digitalnu olokvu nadležnome za izbore da bi mogao unijeti podatke u tablicu. Ovakva tehnologija se prvi put koristila na lokalnim izborima u Škotskoj 2006. godine, a očekivalo se da će se koristiti na izborima u Hamburgu 2008. godine, ali to se nije dogodilo zbog polemika oko točnosti glasanja. [43] Prednost ovakvog sustava glasanja je što je brz i jednostavan za upotrebu. Također, prije je navedeno da olakšava glasanje ljudima s invaliditetom. Nedostatak sustava je što se slično kao kod tradicionalnih glasačkih listića može manipulirati glasovima, a postoji opasnost od elektronske prevare, koja se rješava dodavanjem *kriptografske verifikacije*.

## Direktno bilježenje rezultata

Sličan sustav glasanja je **Direct-recording electronic voting system**, koji koristi stroj za direktno bilježenje rezultata (engl. direct-recording electronic, skraćeno *DRE*). Taj uređaj se najčešće sastoji od zaslona koji reagira na dodir i gumbova, a glavna razlika između ovog i prijašnjeg sustava glasanja je u tome da se glasovi bilježe u internoj memoriji stroja, dakle na ispisuju se na listić. Kada se izbori završe, tiskaju se rezultati izbora koji su zapisani u tablicu.
Ideja glasanja pomoću pritiska gumba ili zaslona podsjeća na mehanički stroj s polugom. Ipak, prvi patenti su se pojavili tek u šezdesetim godinama dvadesetog stoljeća. Prvi puta se ova tehnologija upotrijebila 1974. godine u blizini američkog grada Chicaga. Korišten je stroj nazvan *Video Voter*.


Slika 1.2: Stroj za direktno bilježenje rezultata

Na sličan način radi **sustav za direktno bilježenje rezultata putem javne mreže** (engl. public network DRE voting system). Razlika je u tome što se glasovi šalju putem javne mreže. Osim glasanja putem **interneta**, ovakav način glasanja se odnosi i na glasanje putem **telefona**. Američki astronauti Edward Michael Fincke i Greg Chamitoff 1997. godine imali su mogućnost glasanja iz svemira. Oni su se tada nalazili 220 milja iznad Zemlje, na svemirskoj stanici "Mir", a glasali su putem **e-maila**. [3]
Ovaj način glasanja javno se koristi u SAD-u, UK-u, Švicarskoj i Estoniji. Većina glasača u Estoniji mogu glasati putem interneta. Sve što glasaču treba je računalo, čitač elektronske kartice, osobna iskaznica i njen PIN i onda može glasati iz bilo kojeg dijela svijeta.

Prednosti ovakve tehnologije glasanja su slične kao kod sustava koji koristi optičko skeniranje. Glavni nedostatak je što bilo kakva greška nastala prilikom programiranja može utjecati na rezultate izbora. Također, rezultati se mogu namještati i izmijeniti ukoliko hakeri upadnu u sustav.

## 1.2 Elektroničko glasanje u svijetu

U ovom odjeljku ćemo malo detaljnije opisati načine na koje se provodi elektroničko glasanje u pojedinim državama svijeta.
U posljednjih nekoliko godina države iz Latinske Amerike, Azije i Afrike, kao što su Ekvador, Meksiko, Nigerija, Nepal, Peru i Ujedinjeni Arapski Emirati, polako uvode elektroničko glasanje u svoje države. **Namibija** je 2014. godine postala prva afrička država koja je za svih 1.2 milijuna glasača implementirala strojeve koji se koriste u elektroničkom glasanju. Dvije države koje već godinama koriste elektroničko glasanje pomogle su susjednim državama nabaviti opremu za elektroničko glasanje. Zahvaljujući **Indiji**, **Butan** je 2013. godine građanima omogućio potpuno elektroničke državne izbore, dok je **Brazil** posudio svoju opremu za glasanje **Paragvaju**.

### Brazil

Brazil je prvi dodir s elektroničkim glasanjem imao 1996. godine na lokalnim izborima. Kako je taj projekt prošao uspješno, do 2000. godine svi izbori u Brazilu se odvijaju na potpuno elektronički način. Glavni razlozi za uvođenje elektroničkog glasanja u ovu površinom veliku državu su *brzina prebrojavanja glasova* i *prevencija prijevare*. Na predsjedničkim izborima 2014. godine prebrojano je 114 milijuna glasačkih listića na 500 000 elektroničkih jedinica za glasanje rasprostranjenih diljem zemlje. Izborni rezultati pušteni su u javnost samo dva sata nakon što su zatvorena biračka mjesta.
Glasački sustav u Brazilu široko je prihvaćen kao legitiman od strane domaćih aktera i međunarodnih promatrača. Političke stranke dobile su pristup softveru za glasovni stroj za provjeru, a 2009. Brazil je bila zemlja domaćin "*hack-a-thon*"- a gdje je trideset osam sudionika iz privatnih i javnih informacijskih tehnologija, radeći u timovima, bezuspješno pokušalo manipulirati softverom opreme. Kao dio kontinuiranog procesa nadogradnje tehnologije, *identifikacija birača pomoću otisaka prstiju* ugrađena je u sustav. Zahvaljujući modernizaciji sustava, zadobiveno je povjerenje glasača u Brazilu.

### Estonija

Prva i jedina država koja je omogućila svojim građanima internetsko glasanje je Estonija. Takav način glasanja u ovoj državi koristi se od 2005. godine i tadašnjih lokalnih izbora. Kao što sam naziv kaže, **internetsko glasanje** [13] je sustav koji glasačima omogućuje glasanje preko bilo kojeg računala povezanog internetom. Za razliku od već navedenih sustava glasanja, ovakav način glasanja je jednostavan i siguran.

Tijekom određenog razdoblja prije glasanja, birač se prijavljuje na sustav pomoću osobne iskaznice ili mobilnog ID-a[1] i šalje svoj glasački listić. Identitet glasača uklanja se iz glasačke liste prije nego što stigne do *Nacionalnog izbornog povjerenstva za prebrojavanje* čime se osigurava anonimnost.
Problem kod daljinskog glasanja je mogućnost da su glasači glasali pod prisilom ili da su glasovi kupljeni. Estonsko rješenje tog problema je omogućavanje glasačima da se ulogiraju u sustav i glasaju koliko god puta žele tijekom perioda predviđenog za glasanje. Kako svaki glas poništava posljednji, glasač ima priliku promijeniti svoj izbor kasnije.

## Europska Unija

U rujnu 2000. godine Europska komisija lansirala je *CyberVote projekt*. Cilj tog projekta bio je omogućiti "*potpuno provjerljive on-line izbore koji jamče apsolutnu privatnost glasova i korištenje fiksnih i mobilnih internetskih uređaja*". [6] Taj projekt se počeo koristiti u **Švedskoj**, **Francuskoj** i **Njemačkoj**.

**Švedski izborni odbor**, koji se sastoji od predstavnika svih političkih stranaka, predložio je 2013. godine da bi nekoliko općina trebalo eksperimentirati s glasovanjem putem interneta na općim izborima 2018. godine. Ipak, sudeći po članku iz 2016. godine [16], švedski ministar Morgan Johansson odbio je zahtjev za internetskim glasanjem na izborima 2018. godine.

Što se **Francuske** tiče, 2003. godine za izbor zastupnika u *Skupštinu francuskih građana u inozemstvu*, francuski su građani imali dopuštenje za glasovanje putem interneta. Više od 60% birača odlučilo je glasovati putem interneta umjesto glasačkih listića. Na predsjedničkim izborima 2007. godine po prvi puta je omogućeno elektroničko glasanje, u vidu daljinskog elektroničkog glasanja i uređaja koji reagira na dodir i koji se nalazi na biračkim mjestima. [41]
Unatoč tome, 2017. godine Francuska je objavila da internetsko glasanje neće biti dopušteno na izborima koji su se održali te godine zbog sigurnosnih razloga. [44]

**Njemačka** je 1998. svoje prve strojeve za elektroničko glasanje, koje je dobila od nizozemske tvrtke *NEDAP*, počela koristiti u Kölnu. Proba je bila uspješna, a godinu dana kasnije Köln je koristio elektroničke uređaje za glasanje za cjelokupne izbore za Europski parlament. Ubrzo su ga slijedili i drugi gradovi, a na općim izborima 2005. godine gotovo 2 milijuna njemačkih birača koristilo je *NEDAP* strojeve za glasanje. Reakcija na korištenje tih elektroničkih glasačkih strojeva općenito je bila vrlo pozitivna među biračima zbog jednostavne uporabe te među izbornim upraviteljima koji su bili u mogućnosti smanjiti broj

[1] Mobilni ID je vrsta Estonskog državnog digitalnog identiteta koji se generira pomoću mobitela.

biračkih mjesta i osoblja na svakom biračkom mjestu.
Međutim, nakon izbora 2005. godine, dva birača podnijela su žalbu pred njemačkim Ustavnim sudom nakon što im je odbijena žalba od strane Odbora za kontrolu izbora. Tvrdili su da je korištenje elektroničkih strojeva za glasanje bilo protuustavno i da je moguće hakirati glasačke strojeve pa rezultat izbora 2005. godine nije bio valjan. Tužba je tad usvojena te je Ustavni sud proglasio korištenje *NEDAP* strojeva **protuustavnim**. Ova odluka prethodila je potpunom zaustavljanju korištenja elektroničkog glasanja u Njemačkoj 2009. godine. [5]

## Indija

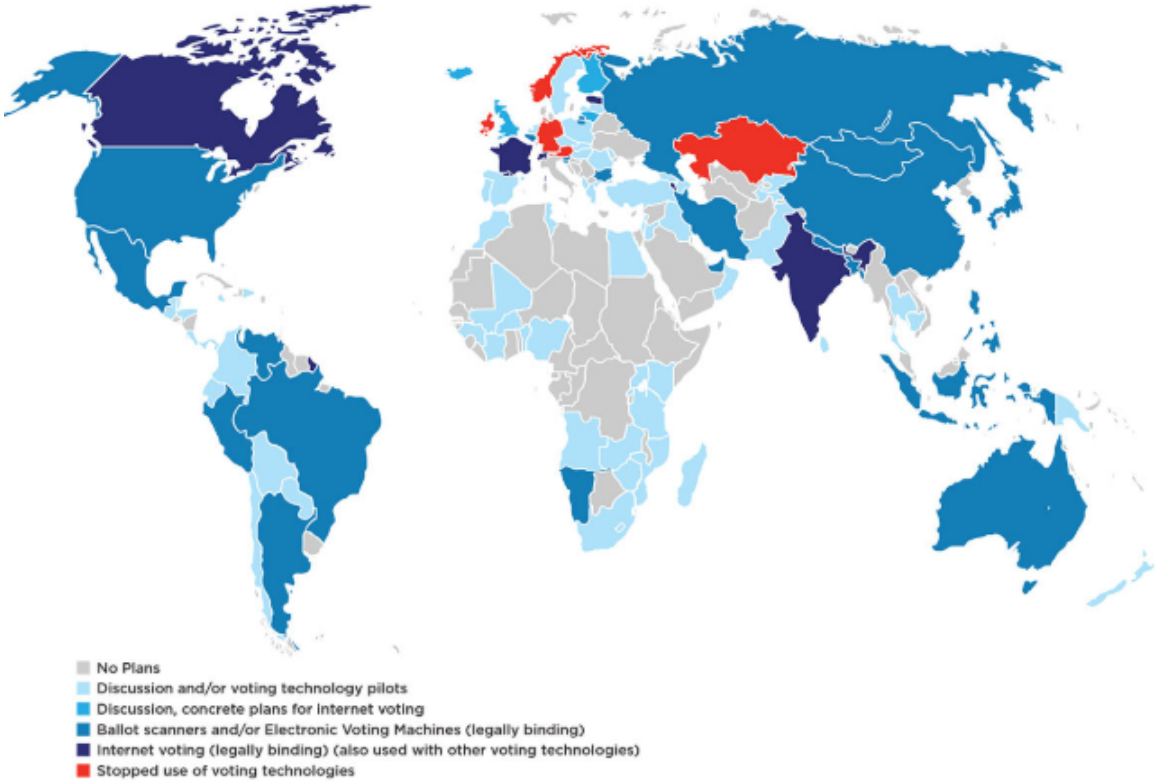
S više od milijardu stanovnika, Indija je najveća demokracija na svijetu. Biračko tijelo sastoji se od više od 668 milijuna ljudi i obuhvaća 543 parlamentarnih izbornih jedinica te zahtijeva više od milijun elektroničkih glasačkih strojeva (EVM-a). Pravno odobrenje EVM-a odobreno je 1989. godine, korišteni su na mnogim državnim izborima, ali nikada nisu korišteni na općim izborima. EVM obuhvaća dvije jedinice, jednu za kontrolu od strane biračkog tijela, a drugu za korištenje birača. Jedinica za glasanje zahtijeva da birači pritisnu gumb pored imena i simbola kandidata, a kontrolna jedinica bilježi glasanje. Svjetlo pored gumba svijetli te slijedi kratki zvučni signal koji označava da je glas zabilježen. Zatim, glasački nadzornik pritisne prekidač kojim omogućava daljnju upotrebu stroja za sljedećeg glasača. Prva upotreba elektroničkog glasanja u ovoj državi dogodila se 2004. godine. [40]
Sudeći po [9], u travnju 2011. godine indijska država Gujarat je prva počela eksperimentirati s **elektroničkim glasanjem**.

## Problemi s elektroničkim glasanjem u svijetu

Prema članku [2], navodimo najvažnije probleme vezane za elektroničko glasanje. Nažalost, neke države svijeta imaju **društveno - ekonomske probleme** koji stvaraju sveukupan problem prilikom glasanja. Primjerice, u **Meksiku** su glasači bili sumnjičavi u vezi vjerodostojnosti izbora zbog elektroničke prijevare koju su počinile stranke. Ta prijevara uključivala je: popunjavanje listića od strane izbornih dužnosnika, krađu glasačkih kutija, zastrašivanje birača, promatrača i stranačkih dužnosnika te manipuliranje popisima birača. U **Tajvanu** je za 10 dolara bilo moguće kupiti glas, a slična stvar se dogodila čak i **SAD-u** 2004. godine gdje su petorica članova stranke nudili siromašnim ljudima cigarete, lijekove, pivo i 5-10 dolara za njihov glas. Na izborima u **Gani** 2012. godine zabilježeni su slučajevi duplog glasanja, glasanja malodobnika i glasanja neprihvatljivih pojedinaca. Ovakvi slučajevi su mogući zbog upetljanosti državnih službenika u prijevaru. Takav problem još se naziva i

"*Insider-prijetnja*", jer službenici koji bi trebali biti ljudi u koje se može pouzdati imaju pristup sigurnosnom sustavu.
Još jedan veliki problem je tzv. **Cyber - prijetnja**, tj. prijetnja koja dolazi od strane računala, informacijske tehnologije ili virtualne stvarnosti. U **Ukrajini** se tijekom predsjedničkih izbora 2014. godine u Središnjem izbornom povjerenstvu pojavio virus kojim se se pokušali izbrisati glasovi. U spomenutom internetskom glasanju u **Estoniji** pronađen je put preko kojeg bi se mogao izvršiti Cyber- napad. Najpoznatiji slučaj je vjerojatno ruski Cyber-napad kojim je utjecano na predsjedničke izbore u **SAD-u** 2016. godine.

U članku [8] mogu se pronaći detaljniji opisi elektroničkog glasanja još nekoliko država. Na slici 1.3 nalazi se karta svijeta iz 2015. godine s označenim državama koje koriste neke vrste elektroničkog glasanja, one koje su prestale s korištenjem elektroničkog glasanja te koje nemaju planove uvesti elektroničko glasanje.




Slika 1.3: Elektroničko glasanje u svijetu 2015. godine

## 1.3 Elektroničko glasanje u Republici Hrvatskoj

Kao što smo vidjeli u prijašnjem odjeljku, mnoge države svijeta koriste *dopisno* i *elektroničko* glasanje. U ovom odjeljku detaljnije ćemo opisati koji su bili planovi za elektroničko glasanje u Republici Hrvatskoj i hoće li se oni ostvariti u skorije vrijeme.

### Opći uvjeti glasanja

Svaki punoljetni državljanin Republike Hrvatske, a i državljanin Europske unije koji ima prebivalište, boravište i/ili se trenutno zatekao u Republici Hrvatskoj ima biračko pravo. U sklopu projekta **e-Hrvatska** građani su dobili svoj pretinac u kojem mogu dobiti sve dokumente i informacije iz područja državne uprave. Svi hrvatski državljani mogu i *online* provjeriti svoje podatke na internetskim stranicama Ministarstva uprave. Na istoj stranici moguće je provjeriti koliko je birača prijavljeno na njihovoj adresi ili na bilo kojoj drugoj adresi u Republici Hrvatskoj. Ukoliko u vrijeme izbora neće biti u svom mjestu prebivališta i žele glasovati u nekom drugom mjestu u Republici Hrvatskoj, odnosno inozemstvu, birači koji imaju vjerodajnice i pristup aplikaciji *e- Građani* mogu prije održavanja izbora podnijeti elektroničkim putem zahtjev za privremeni upis, prethodnu i aktivnu registraciju. [23]

Prema [22], hrvatski državljani bez prebivališta u Republici Hrvatskoj - birači s e-osobnim iskaznicama ne moraju se aktivno registrirati za izbore. Birači bez prebivališta u Republici Hrvatskoj, koji su podnijeli zahtjev za e-osobnom iskaznicom, po službenoj dužnosti će se aktivno registrirati i uključiti u popis birača (prema adresi prijavljenog prebivališta u inozemstvu) za predstojeće izbore.

### Dopisno glasanje

Prema članku [24], u ovom je trenutku u Republici Hrvatskoj **zakonski moguće glasovanje u odsutnosti**, a dio toga je i dopisno glasanje za birače koji na dan izbora ne mogu izaći na biračko mjesto zbog opravdanih razloga: ne borave u tom trenutku u zemlji ili u svojem izbornom okrugu, bolesni su i nemoćni, nalaze se u zatvorima, na brodovima, u vojnim postrojbama, u diplomatskim misijama itd.

Tri su oblika glasanja u odsutnosti:

- prethodno glasanje, koje omogućuje biračima koji ne mogu glasovati na dan izbora da to učine dan ili nekoliko dana prije;
- poštansko glasanje, koje omogućuje osobama koje na dan izbora nisu u zemlji ili zbog nekih drugih razloga ne mogu izaći na biračko mjesto da glasački listić pošalju poštom;
- zamjensko glasanje, kojim se omogućuje da umjesto slijepih i, općenito, invalidnih osoba glasa druga, opunomoćena osoba ili da te osobe pošalju svoj glasački listić biračkom odboru po drugoj osobi.

Glasovi dani u odsutnosti pribrajaju se glasovima na glasačkim mjestima i izbornim okruzima u kojima su trebali glasati da nisu bili spriječeni u tome. Iako Ustav Republike Hrvatske i pravne stečevine EU zahtijevaju jednaku dostupnost glasanja svim biračima, tome nije tako. Više od 400 000 državljana koji prebivaju izvan Republike Hrvatske ne može glasati dopisnim ili elektroničkim putem, a neki glasači koji prebivaju u Republici Hrvatskoj moraju putovati na veću udaljenost kako bi došli do biračkih mjesta.

## Aplikacija za elektroničko glasanje

Tvrtka **Mobility** 2014. godine u samo tri mjeseca razvila je aplikaciju *e-vote*. Prema [36], direktor Nino Strmo ističe: „E-vote je vrlo jednostavan i pregledan za korištenje, a dostupan je na PC, Mac, iOS, Android te Windows Phone platformama. Prije glasovanja svaki je birač dobio mail s jedinstvenim ključem pomoću kojeg se sigurno uključio u sustav i obavio svoju dužnost.“ Ti ključevi se distribuiraju prema računalnom algoritmu neovisno o ljudskom faktoru kako bi se osigurala tajnost glasanja i privatnost izbora svakog glasača.

Platforma *e-vote* pruža i dodatne mogućnosti poput definiranja početka i kraja glasovanja, podršku za upis dopisnih birača tj. onih koji nemaju pristup internetu, te izradu hijerarhije izbornih listi i glasačkih ”listića” prema regijama, županijama, gradovima te na državnoj razini. Navedena aplikacija koristila se 2014. godine na **unutarstranačkim izborima** u stranci *OraH - Održivi Razvoj*.

Članak [35] prenosi riječi Nenada Strma - sustav je napravljen tako da se popis birača prvo anonimizira kako se ne bi znalo tko je kako glasao i tada slaže bazu koja ide na internet i šalje pozive na glasanje. Dodatno, redoslijed primljenih glasova miješa se kako se ne bi znalo ni po redoslijedu tko je kako glasao. Još se navodi da jedna politička stranka iz Slovenije i jedna velika hrvatska organizacija pregovaraju o kupnji navedenog sustava.

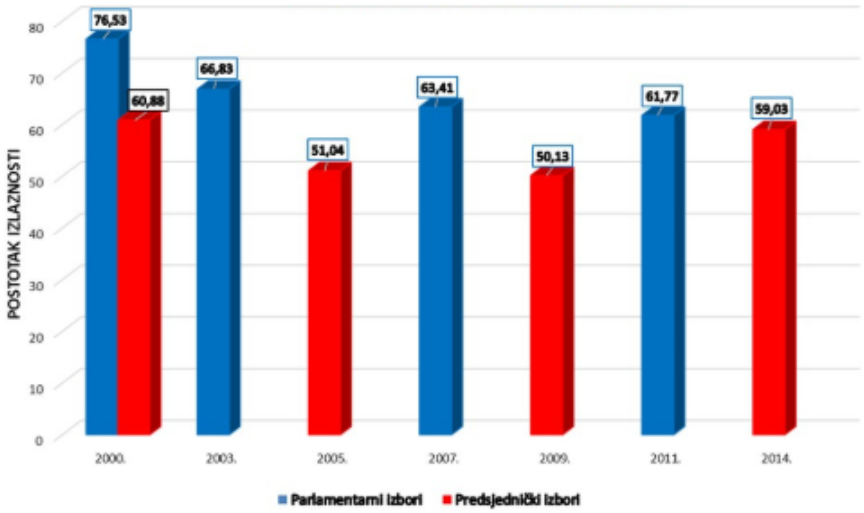
## Referendum 2018. godine

Građanska inicijativa *Narod odlučuje* odlučila je prikupljati potpise za **referendum za promjenu izbornog sustava** tvrdeći da bi tako sebi i drugima olakšati sudjelovanje u odabiru svojih političkih predstavnika. [11]

Jedan od glavnih ciljeva građanske inicijative *Narod odlučuje* za promjenu izbornoga sustava je **omogućivanje dopisnog i elektroničkog glasanja** svim hrvatskim državljanima, biračima u Republici Hrvatskoj i izvan Republike Hrvatske. Time se omogućuje da svi državljani Republike Hrvatske koji imaju pravo glasa mogu sudjelovati u glasanju. Uz to, referendum bi sadržavao pitanja o promjeni broja pojedinih zastupnika u Hrvatskom saboru.

Potpisi su se skupljali od 13. do 27. svibnja 2018. godine. Prema [18], 31. svibnja inicijativa *Narod odlučuje* je ispred Hrvatskog sabora objavila kako su prikupili dovoljno potpisa za referendum o dva pitanja: promjenama izbornog sustava koje uključuju smanjivanje broja zastupnika nacionalnih manjina u Hrvatskom saboru te isključivanje zastupnika nacionalnih manjina iz odlučivanja o povjerenju Vladi, kao i o državnom proračunu. Sudeći po [17], 13. lipnja spomenuta inicijativa predala je potpise za referendum u Saboru.

Politička stranka *Most* zatražila je 27. srpnja 2018. godine da se uvede dopisno i elektroničko glasanje već na idućim izborima, onima za Europski parlament. Tvrde da bi tada više građana izašlo na izbore i legitimnost građana bi bila veća. Na slici 1.4 iz grafa se da iščitati relativno mala izlaznost na parlamentarne i predsjedničke izbore od 2000. do 2014. godine.




Slika 1.4: Izlaznost na izbore 2000. - 2014. godine

Ministarstvo uprave navodi kako je iz sigurnosnih razloga za elektroničko glasanje potreban internet 5. generacije. S druge strane, ministar uprave Lovro Kuščević tvrdi da **tehnološki uvjeti ne zadovoljavaju kriterije da bi se moglo osigurati elektroničko glasanje** te da je tako nešto moguće osigurati tek za dvije godine, jer 5G mreža u ovom trenutku u Republici Hrvatskoj uopće ne postoji. Plan je da se uvede do 2020. Ipak, Krešimir Mazor iz *Hrvatske regulatorne agencije za mrežne djelatnosti* tvrdi da je elektroničko glasanje trenutno moguće uvesti, no pitanje je koliko je sredstava za to potrebno izdvojiti. [31]

# Poglavlje 2

# Upotreba kriptografije u elektroničkom glasanju

Kriptografija je znanstvena disciplina koja se bavi analizom i proučavanjem metoda koje osiguravaju sigurnu komunikaciju [1] između dvije strane - *pošiljalaca* i *primaoca*.

Začeci kriptografije pojavili su se još u antičkom dobu u civilizacijama poput Grčke, Egipta, Indije i Perzije. Tradicionalno, kriptografija se koristila za prijenos informacija između dvoje ljudi koji su koristili unaprijed dogovoren *ključ* poznat samo njima. Tijekom vremena ova disciplina se razvila, pa moderna kriptografija sadrži elemente **matematike**, **računarstva**, **električnog inženjeringa**, **komunikologije** i **fizike**.

## 2.1 Kriptografske funkcije korištene u elektroničkom glasanju

### Šifriranje i dešifriranje

Kako bismo objasnili ove pojmove, za početak pretpostavimo da imamo dvije osobe koje žele komunicirati - pošiljalaca kojeg ćemo zvati *Alice* i primaoca kojeg ćemo zvati *Bob*. Treću osobu, koja želi presresti njihove poruke, zvat ćemo *Eva*. Kao što smo već naveli, Alice šalje poruku Bobu. Tu poruku ćemo zvati *otvoreni tekst*, a ona može sadržavati slova, brojeve ili bilo što drugo. Alice transformira otvoreni tekst pomoću unaprijed dogovorenog *ključa*. Taj postupak zovemo *šifriranje*, a dobiveni rezultat *šifrat*. Poruka putuje kroz komunikacijski kanal, Eva može doznati sadržaj šifrata, ali ne i otvoreni tekst. Nakon što

[1] Komunikacija se smatra sigurnom ukoliko dvije strane komuniciraju, a treća neželjena strana ne može saznati o čemu komuniciraju.

prima poruku, Bob pomoću ključa može saznati kako je glasio otvoreni tekst, a taj postupak zovemo *dešifriranje*.

U najstarijoj i najjednostavnijoj klasičnoj kriptografiji postojala dva su glavna tipa šifara: **transpozicijske šifre** i **supstitucijske šifre**. U transpozicijskoj šifri šifrat je nastao promjenom redoslijeda slova, npr. riječ "pozdrav" bi bila šifrirana u "zvradop". Što se tiče supstitucijske šifre, ugrubo rečeno jedna grupa slova bi zamijenila drugu grupu slova. Najpoznatija supstitucijska šifra se zove *Cezarova šifra*. U njoj se svako slovo zamjenjuje sa slovom koje je za neki fiksni broj $k$ udaljeno za $k$ pozicija u alfabetu. Tako bi riječ "pozdrav", uz npr. k = 4, bila šifrirana kao "tsdhvez".[2]

Matematički gledano, Dujella daje sljedeću definiciju: [32]

**Definicija 2.1.1.** *Kriptosustav je uređena petorka (*$\mathrm{P}$, $\mathrm{C}$, $\mathrm{K}$, $\mathrm{E}$, $\mathrm{D}$*) za koju vrijedi:*
*1)* $\mathrm{P}$ *je konačan skup svih mogućih osnovnih elementa otvorenog teksta;*
*2)* $\mathrm{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
*3)* $\mathrm{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva;*
*4) Za svaki* $K \in \mathrm{K}$ *postoji funkcija šifriranja* $e_K \in \mathrm{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathrm{D}$.
*Pritom su* $e_K : \mathrm{P} \to \mathrm{C}$ *i* $d_K : \mathrm{C} \to \mathrm{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathrm{P}$.

Sada ćemo objasniti kako se koriste šifriranje i dešifriranje u izbornom sustavu. Ukoliko glasač glasa preko elektroničkog uređaja za glasanje, njegov rezultat se šifrira i sprema u taj uređaj. Isto tako, kada glasač pošalje svoj glasački listić u digitalnom obliku preko komunikacijske mreže, sadržaj poslanog listića se šifrira. Ključ koji se koristi za šifriranje određuje *Electoral Management Body* (EMB). [3] Ta organizacija je jedina koja zna ključ potreban da bi se dešifrirali šifrirani podaci. [14] Kasnije ćemo malo detaljnije opisati kako se generiraju takvi ključevi.

## Hash funkcije

Prema definiciji 2.1.1. vidjeli smo da postoje funkcije šifriranja i dešifriranja. U ovom odjeljku opisujemo drugu vrstu kriptografske funkcije - **hash funkciju**. Općenito, hash funkcija $H$ preslikava vrijednost iz nekog skupa (konačnog ili beskonačnog) u skup sa fiksnim brojem članova.

[2] Pretpostavljamo da koristimo engleski alfabet te da kad dođemo do kraja alfabeta nastavljamo brojati ispočetka.

[3] Organizacija kojoj su ciljevi određivanje tko smije glasati, primanje i validiranje nominacija za kandidaturu stranaka, priprema glasačkih listića te brojanje i tabeliranje glasova.

Hash funkcija se, između ostalog, može koristiti za mehanizam kontrolnog zbroja (za objašnjenje pogledati [33], str. 22) ili pronalaženje određene vrijednosti u bazi podataka. [12] Posebna vrsta hash funkcije je **kriptografska hash funkcija**.

Poželjno je da kriptografske hash funkcije ispunjavaju sljedeća tri svojstva: [7]

- funkcija je injekcija, tj. niti jedna dva različita ulazna podatka (input) se ne smiju preslikati u istu vrijednost (output);
- funkcija može biti skrivena, tj. trebalo bi biti teško pogoditi input hash funkcije ako znamo output;
- funkcija je takva da se iz odabranog inputa teško može pogoditi kako bi izgledao output (preslikavanjem je dobiven tzv. *random* output).

Kao što smo rekli, ova tri svojstva su poželjna, ali ih nije uvijek moguće implementirati. Na primjer, disparitet bitova (za objašnjenje pogledati [25]) u razmacima koji se nalaze u inputu i outputu može utjecati na to da funkcija više ne bude injekcija. Treća strana bi to mogla upotrijebiti te napasti, tj. proizvesti tzv. *Collision attack*.

Najpoznatije kriptografske hash funkcije pripadaju skupinama **MD** (Message Digest Algorithm) i **SHA** (Secure Hash Algorithm). Već 2004. godine Xiaoyun Wang i ko-autori su demonstrirali *Collision attack* na najnoviju seriju MD algoritama, MD5. S druge strane, 2017. godine CWI Amsterdam i Google Research su predstavili *SHAttered attack*, koji također krši prvo svojstvo kriptografskih hash funkcija, na seriju SHA-1. [15] Unatoč tome, takvi algoritmi se još uvijek koriste npr. pri spremanju lozinki u baze podataka. Najpoznatiji digitalni novac na svijetu, *Bitcoin*, za hashiranje koristi SHA-256 algoritam, iz serije SHA-2. [26]

Da bismo ilustrirali kako hash funkcije preslikavaju određene riječi, koristimo alat [19]. Služit ćemo se SHA256 algoritmom. Taj algoritam ulaznu riječ ”pozdrav” pretvara u šifrat ”7622AAE9EA1F27C663653DFA5C521CF549BFE24F2FE7081709B04F03602A5C46”. Ako bismo htjeli pretvoriti riječ ”pozdravi”, dobivamo šifrat ”9401BDA4617CF807DF7141263C43903C91749CC5299C656983FF44DBBD6E0C8F”. Iz ovog primjera se sada vidi da iako su riječi slične, njihovi šifrati se jako razlikuju, što nije bio slučaj sa spomenutim transpozicijskim i supstitucijskim šiframa.

Puno je primjena korištenja hash funkcija u glasanju. U SAD-u, javni repozitorij poznat kao *National Software Reference Library* (NSRL) pohranjuje hash-eve izvornog koda glasanja i kompilirane verzije softvera koji se koriste pri glasanju i brojanju glasova. Neki EMB-ovi provjeravaju softver prije instaliranja na glasačke strojeve tako da primjenjuju

hash funkcije u softveru i uspoređuju rezultate s pohranjenima u NSRL-u. Taj postupak pomaže u prepoznavanju zlonamjernih promjena softvera, a mnogi izborni dužnosnici također navode kako taj postupak pomaže prepoznati kada će biti instalirane netočne verzije ili kada je softver pokvaren. [14]

## Digitalni potpisi

Još jedne matematičke funkcije koje rade na sličan način kao kriptografske hash funkcije su **digitalni potpisi**. Za opisivanje digitalnih potpisa koristimo [30]. Digitalni potpisi su kriptografska zamjena za fizičke potpise ili žigove. Ako znamo kako izgleda nečiji potpis i vjerujemo da bi bilo teško za bilo koga osim vlasnika da proizvode takav potpis, prisutnost takvog potpisa na dokumentu potvrđuje da ga je vlasnik vidio i potpisao. Slično tome, otisak pečata na dokumentu potvrđuje da je netko s odgovarajućim pečatom ovjerio dokument, iako to ne mora značiti da je vlasnik pečata vidio dokument.

Digitalni potpis se razlikuje od fizičkih potpisa u tome što se oni ne nalaze na originalnom dokumentu, nego su zasebni objekti koji dolaze uz dokument. Kako bi se spriječio prijenos potpisa s jednog dokumenta na drugi, digitalni potpisi za drugačije dokumente bit će drugačiji objekti.
Da bi se mogao stvoriti digitalni potpis, potpisnik mora najprije stvoriti par ključeva koji se zovu *potpisni ključ* (ili tajni ključ) i *ključ za potvrdu* (ili javni ključ). Ključevi se stvaraju pomoću *algoritma za generiranje ključeva* (engl. key generation algorithm). Potpisni ključ je kao žig kojeg potpisnik može staviti na dokument. Takav žig na dokumentu sam po sebi ne znači puno jer svatko može kreirati svoj vlastiti žig, ali ako se zna kako izgleda žig određene osobe ili organizacije, usporedbom žiga na dokumentu i žiga sa kojeg se zna da je njihov može se potvrditi da je dokument originalan. Ključ za potvrdu ima sličnu ulogu u digitalnom potpisu.

Shema digitalnog potpisa dolazi s još dva algoritma. *Algoritam za potpisivanje* (engl. signing algorithm) kao ulazni podatak prima potpisni ključ, a kao izlazni podatak vraća potpis za dokument. *Algoritam za provjeru* (engl. verification algorithm) za ulazni podatak prima dokument, potpis i ključ za potvrdu, a vraća ”1” ako je za dani ključ i dokument potpis valjan, inače vraća ”0”.

Odgovornost je potpisnika da svi glasači imaju autentičnu kopiju ključa za potvrdu. Kao što smo već naveli, u nekim državama, svaki građanin dobiva inteligentnu karticu koja sadrži ključ za potpisivanje, a vlada objavljuje javnu baza podataka ključeva za potvrdu. Za digitalne izbore, ako izborne vlasti trebaju potpisati glasačke listiće, mogu objaviti svoj ključ za potvrdu u sklopu izborne odredbe.

Formalno, dajemo sljedeću definiciju:

**Definicija 2.1.2.** *Digitalna potpisna shema* $\Sigma$ *je uređena trojka algoritama*

$$\Sigma = (\mathrm{KeyGen},\ \mathrm{Sign},\ \mathrm{Verify})$$

*poznatih kao algoritmi za generiranje ključeva, potpisivanje i provjeru, a koji zadovoljavaju uvjet korektnosti naveden ispod.*

*Algoritam za generiranje ključeva ne prima ulazni podatak, a generira par ključeva (sk,vk)* $\leftarrow \mathrm{KeyGen}()$*, poznatih kao potpisni ključ i ključ za potvrdu. Algoritam za potpisivanje prima potpisni ključ sk i poruku m kao ulazne podatke, a generira potpis* $\sigma \leftarrow \mathrm{Sign}(sk,m)$*. Algoritam za provjeru mora biti deterministički. On prima ključ za potvrdu vk, poruku m i potpis* $\sigma$ *kao ulazne podatke, a vraća 0 ili 1 kao izlazni podatak. Kažemo da je* $\sigma$ *(valjan) potpis za m pod ključem vk ako* $\mathrm{Verify}(vk,m,\sigma) = 1$*.*

*Digitalna potpisna shema mora zadovoljavati sljedeći uvjet korektnosti koji znači da su korektno generirani potpisi uvijek valjani. Za proizvoljnu poruku m, za pokretanje sljedećeg niza algoritam dobiven je b = 1:*

$$(sk,vk) \leftarrow \mathrm{KeyGen}();\ \sigma \leftarrow \mathrm{Sign}(sk,m);\ b \leftarrow \mathrm{Verify}(vk,m,\sigma)$$

**Napomena 2.1.3.** *Deterministički algoritmi su algoritmi koji će pri svakom izvršavanju u bilo kojim uvjetima za iste ulazne podatke dati iste rezultate.*

U prethodnoj definiciji, u algoritmu za generiranje ključeva za isti ulaz možemo dobiti različite potpisne ključeve. Isto tako, algoritam za potpisivanje može prozvesti različit potpis za iste ulazne podatke. Zbog toga su ti algoritmi probabilistički.

Sada kada smo opisali na koji način rade digitalni potpisi, navodimo njihovu primjenu u glasanju. Na izborima se koriste za ”potpisivanje” sadržaja digitalne glasačke kutije ili izbora birača, čime se osigurava da glasačka kutija ili glasovi nisu promijenjeni. Ako je došlo do neovlaštenog korištenja i digitalni potpis je krivotvoren, napadač bi trebao znati tajni ključ napadnute osobe ili EMB-a. [14]

## 2.2 Metode osiguravanja elektroničkog glasanja

U ovom odjeljku razmotrit ćemo sljedeće metode: *prikriveni potpisi*, *kriptografski brojači* i *Mix nets*.
Cilj je napraviti sustav koristeći navedene metode, a koji će zadovoljavati sljedeće uvjete:

1. korektnost:
    - samo autorizirani korisnici smiju glasati
    - nijedan glasač ne glasa više od jednom
    - nijedan glasač ne smije zamijeniti glasove
    - odbor zadužen za tabeliranje glasova ne može promijeniti rezultate
2. povjerljivost
3. anonimnost korisnika
4. nemogućnost komuniciranja dviju ili više osoba tijekom glasanja

U ovom odjeljku koristimo informacije iz [42].

### Prikriveni potpisi

Prikriveni potpis (engl. blind signature) je metoda slična digitalnom potpisu. Da bismo pokazali razliku, na jednostavnom primjeru ilustrirat ćemo kako funkcionira. Pretpostavimo da Alice želi Bobu poslati poruku $m$, ali ne želi da Bob sazna sadržaj poruke. Ova situacija na prvi pogled ne izgleda logično - zašto bi Bob htio potpisati neki dokument kojem ne zna sadržaj? Odgovor je očit - ovakav slučaj osigurao bi anonimnost, pa je jasno da bi metoda bila korisna u elektroničkom glasanju, ali i u slučaju slanja digitalnog novca. Dakle, ovako bi izgledalo slanje poruka:

1. Reći ćemo da Alice "prikriva" poruku $m$ s nekim naizmjeničnim brojem $b$ (tzv. faktor za prikrivanje). Rezultat toga je blind(m,b).
2. Bob potpisuje poruku pa je rezultat toga sign(blind(m,b),d), gdje je $d$ Bobov privatni ključ.
3. Alice otkriva poruku koju je primila od Boba, koristeći $b$, a dobiveni rezultat je unblind(sign(blind(m,b),d),b).

Koncept prikrivenih potpisa i njihovu implementaciju u RSA kriptosustavu osmislio je David Chaum 1982. godine. [4]

U prethodnoj rečenici spomenuli smo RSA kriptosustav. To je najpopularniji i najkorišteniji kriptosustav s javnim ključem.[4] Dajemo definiciju RSA kriptosustava. [21]

**Definicija 2.2.1.** *Neka je $n = p * q$, gdje su $p$ i $q$ prosti brojevi. Neka je $\mathrm{P} = \mathrm{C} = \mathbb{Z}_n$, te*

$$K = \{\, (n, p, q, d, e) : n = pq,\ p, q\ prosti,\ de \equiv 1\ (mod\ \varphi(n)) \,\}.$$

*Za $K = (n, p, q, d, e) \in K$ definiramo*

$$e_K(x) = x^e\ mod n \quad i \quad d_K(x) = y^d\ mod n, \quad x,y \in \mathbb{Z}_n.$$

*Vrijednosti $n$ i $e$ su javne, a vrijednosti $p$, $q$ i $d$ su tajne.*

**Napomena 2.2.2.** *U prethodnoj definiciji $\varphi(n)$ je tzv. Eulerova funkcija, tj. broj brojeva u nizu 1,2, ..., n koji su relativno prosti s n.*

U elektroničkom glasanju, sadržaj glasačkog listića je prikriven da bi se osigurala povjerljivost. Za mogući prototip ovog modela, koristimo [27].

Za početak, glasač šalje svoje ime i prezime te osobni identifikacijski broj *registracijskom tijelu*. Te poruke su šifrirane. Ukoliko registracijsko tijelo[5] zaključi da glasač ispunjava uvjete za glasanje, poslat će glasaču listić s jedinstvenim ID-om. Označimo taj listić slovom **B**. Također, generirat će javni i tajni ključ. Koristeći RSA kriptosustav, pokazujemo kako generirati javni i tajni ključ. Za početak, izabrat ćemo dva velika prosta broja, $p$ i $q$, tako da je n = pq. Izaberemo broj $e$ relativno prost sa (p-1)(q-1). Sada nađemo $d$ tako da je ed = 1 mod (p-1)(q-1). Neka je (n,e) javni ključ registracijskog tijela te (n,d) njihov tajni ključ. Glasač nasumično generira broj $r$ tako da je nzd(r,n) = 1 [6] i šalje sljedeću vrijednost registracijskom tijelu:

$$B' = r^e\, B\, mod\, n.$$

Nasumično izabran broj $r$ skriva sadržaj glasačkog listića, stoga registracijsko tijelo ne zna što piše na njemu. Sljedeće, registracijsko tijelo potpisuje prikriveni listić. Ovako izgleda potpisna vrijednost:

$$S' = (B')^d = r\, B^d\, mod\, n.$$

[4] U kriptosustavu s javnim ključem, zbog činjenice da je iz funkcije šifriranja gotovo nemoguće izračunati funkciju dešifriranja, funkcija šifriranja je javna.

[5] Pretpostavit ćemo da je registracijsko tijelo skupina ljudi zadužena za sigurnost i verifikaciju glasača.

[6] nzd(x,y) je kratica od najvećeg zajedničkog djelitelja brojeva $x$ i $y$.

Nakon primanja potvrđenog listića, glasač otkriva sadržaj listića da bi ga mogao usporediti sa svojim prvotno poslanim listićem, a pravi potpis $S$ od registracijskog tijela dobiva računajući

$$S = S' r^{-1} \bmod n = B^d.$$

Opišimo sada ukratko proces glasanja. Najprije glasač šalje svoje ime i broj osobne iskaznice registracijskom tijelu. Registracijsko tijelo provjerava ispunjava li glasač uvjete za glasanje i je li glasao/glasala prije. Ako glasač ispunjava tražene uvjete te nije glasao/glasala prije, registracijsko tijelo šalje glasaču glasački listić. Svaki glasački listić ima svoj jedinstveni ID. Glasač ispunjava svoj glasački listić koji je prije slanja prikriven, potpisan i šifriran. Taj listić šalje se registracijskom tijelu na provjeru. Nakon provjere, registracijsko tijelo šalje potpisani listić glasaču. Glasač provjerava integritet glasačkog listića tako da "otkrije" glasački listić i uspoređuje ga s originalnim listićem. Nakon toga, provjereni listić i originalni listić se šalju *odboru za provjeru rezultata*, koji je zadužen za provjeru listića, brojanje glasova i tabeliranje rezultata. Odbor za provjeru rezultata provjerava glasački listić koristeći javni ključ. Provjereni listić se tada sprema u bazu podataka u kojoj se nalaze svi podaci vezani za glasanje. Na kraju, odbor za provjeru rezultata obavještava glasača da je primio njegov glasački listić tako da mu šalje ID glasačkog listića, vrijeme i datum glasanja te svoj privatni ključ - *td*.

## Kriptografski brojači

Neformalno, *kriptografski brojač* je niz znakova (tzv. string) koji predstavlja šifrirani tekst. Taj string je javan, ali otvoreni tekst je poznat samo registracijskom tijelu (koje posjeduje tajni ključ). Samo registracijsko tijelo može dešifrirati taj string i tako saznati vrijednost brojača, ali svi sudionici smiju povećati ili smanjiti brojač za proizvoljnu vrijednost. Informacije o promjeni vrijednosti brojača skrivene su od svih ostalih sudionika.
Kako bismo lakše definirali kriptografski brojač, dajemo definiciju brojača.

**Definicija 2.2.3.** N-brojač *se sastoji od skupa S i para algoritama (D,T) gdje su:*

- $S = \{s_1, ...\}$ *je* skup stanja *brojača.*
- algoritam dekodiranja *D je deterministički algoritam koji prima stanje $s \in S$ kao ulazni podatak, a vraća broj $i \in \mathbb{Z}_n$. Ovime je definirano preslikavanje iz skupa stanja S u skup* $[0,n\text{-}1] \subset \mathbb{Z}$.
- algoritam tranzicije *T je probabilistički algoritam koji prima stanje $s \in S$ i cijeli broj $i \in \mathbb{Z}_n$ kao ulazne podatke, a vraća stanje $s' \in S$.*

*Zahtijevamo da za svaki $s \in S$ te $i \in \mathbb{Z}_n$, ako $s' \leftarrow T(s,i)$, onda $D(s') = D(s) + i \bmod n$.*

Sada dajemo definiciju kriptografskog brojača.

**Definicija 2.2.4.** Kriptografski n-brojač *je uređena trojka algoritama (G,D,T), gdje su:*

- Algoritam za generiranje ključeva *G je probabilistički algoritam koji za ulaz* $1^k$ *vraća par javnog ključa i tajnog ključa (pk,sk) i string* $s_0$*. Tajni ključ zauzvrat implicitno definira povezani skup stanja* $S_{sk}$*. U ovom slučaju je* $s_0 \in S_{sk}$*.*
- Algoritam za dešifriranje *je deterministički algoritam koji za ulaz prima tajni ključ sk i string s. Ako je* $s \in S_{sk}$*, onda D vraća cijeli broj* $i \in \mathbb{Z}_n$*, inače vraća* $\perp$*.*
- Algoritam za tranziciju *T je probabilistički algoritam koji za ulaz prima javni ključ pk , string s i cijeli broj* $i \in \mathbb{Z}_n$*, a vraća string* $s'$*.*

*Za proizvoljan uređeni par (pk,sk), dobiven računanjem* $G(1^k)$*, definiramo* $D' = D(sk, \cdot)$ *i* $T' = T(pk, \cdot, \cdot)$*. Zatim zahtijevamo da skup* $S_{sk}$ *zajedno sa algoritmima (D' , T') definira n-brojač. Nadalje, zahtijevamo da vrijedi* $D'(s_0) = 0$ *(ovo predstavlja inicijalizaciju brojača na 0).*

Nadalje, dajemo definicije kriptografskog brojača sigurnog od zlonamjernog protivnika i provjerljivog kriptografskog brojača te ukratko opisujemo ograničene brojače.

**Definicija 2.2.5.** *Kažemo da je kriptografski n-brojač (G, D, T)* siguran od zlonamjernog protivnika*, ako je za bilo koju polinomno izračunljivu funkciju A (koja predstavlja protivnika) sljedeća vrijednost zanemariva:*

$$\left\| Pr\left[ \begin{array}{ll} (pk, sk, s_0) \leftarrow G(1^k) & \\ (s, x_0, x_1) \leftarrow A(1^k, pk, s_0) & \\ b \leftarrow \{0,1\} & : b' = b \\ s^* \leftarrow T(pk, s, x_b) & \\ b' \leftarrow A(s^*) & \end{array} \right] - 1/2 \right\|$$

Za bolje razumijevanje, dat ćemo kratko objašnjenje pojmova iz prethodne formule, tj. pokušaj napada. Protivniku A je dan javni ključ i početno stanje $s_0$. Protivnik tada generira stanje s te brojeve $x_0$, $x_1 \in \mathbb{Z}_n$. Bit b je odabran na slučajan način, a brojač je povećan za $x_b$ te funkcija T daje stanje $s^*$. Kada je protivniku A dano stanje $s^*$, on pogađa vrijednost b. "Pr" u prethodnoj formuli je oznaka za vjerojatnost.

**Definicija 2.2.6.** Provjerljivi kriptografski n-brojač *je uređena četvorka (G,D,T,V) tako da vrijedi:*

- *(G,D,T) je kriptografski n-brojač.*
- Verifikacijski algoritam *V je probabilistički algoritam koji zadovoljava potpunost i ispravnost za sve (pk,sk) (izlazne podatke od G), gdje su:*

  1. *(Potpunost) Za sve* $s \in S_{sk}$*, ako je* $s' \leftarrow T(pk,s,i)$ *za neki* $i \in \mathbb{Z}_n$*, tada:*

     $$V(pk,s,s') = 1 \ .$$

  2. *(Ispravnost) Za sve s i sve stringove* $s'$ *tako da za sve i,* $s'$ *nije u slici funkcije T(pk,s,i) , sljedeća vjerojatnost je zanemariva:*

     $$\Pr[\ V(pk,s,s') = 1\ ].$$

Definicije 2.2.3, 2.2.4 i 2.2.6 mogu se modificirati tako da dopuste mogućnost da, iako brojač može spremati vrijednosti u $\mathbb{Z}_n$, operacije povećavanja i smanjenja su ograničene na neki podskup skupa $\mathbb{Z}_n$. Brojače s ovakvim svojstvom zovemo *ograničeni brojači*. Primjer korištenja ovakog brojača je u procesu glasanja. Iako brojač mora pamtiti vrijednosti sve do L (broj glasača), može biti zahtijevano da se povećanje ili smanjenje brojača ograniči na skup {0,1}, što bi odgovaralo glasu da/ne.

Prije uvođenja modela, objasnimo neke pojmove koji će nam biti od koristi kasnije.

*Robusnost*, svojstvo koje osigurava da je konačan rezultat glasanja korektno dobiven, čak i u slučaju da je došlo do neispravnog ponašanja glasača tijekom glasanja, s obzirom na registracijsko tijelo može biti postignuta preko distribuiranog generiranja tajnog ključa skupa sa "treshold dešifriranjem" posljednjeg brojača. Pod pojmom *treshold dešifriranje* podrazumijevamo proces kada više grupa ljudi moraju zajedno surađivati u procesu šifriranja, dešifriranja ili potpisivanja poruka. Dakle, ako dođe do neispravnog ponašanja glasača, zbog činjenice da za navedene procese nije odgovoran jedan čovjek ili grupa ljudi, možemo reći da će konačan ishod glasanja biti korektno dobiven. Za poseban slučaj kada je šifriranje napravljeno korištenjem kvadratnih ostataka, možemo postići efikasno distribuirano generanje ključa i "treshold dešifiriranje". U algoritamskoj teoriji brojeva, *problem kvadratnog ostatka* glasi: ako su dani cijeli brojevi *a* i *N*, odrediti postoji li cijeli broj x tako da vrijedi $x^2 \equiv a \pmod{N}$, tj. odrediti je li *a* kvadratni ostatak modulo *N*. S obzirom na to da takvo šifriranje nije svrha ovog poglavlja, detaljniji opis ćemo izostaviti. Detalji se mogu naći u [39].

Sada ćemo predstaviti model koji je uveo Josh Benaloh. U proces glasanja uključeni su skup glasača $V_1$,...,$V_L$ i skup ljudi nadležnih za izbore (odbor nadležan za izbore) $A_1$,..., $A_M$. Dozvoljavamo da glasač može biti nadležan za izbore i obrnuto, tj. presjek ovih dvaju skupova ne mora biti prazan. Pretpostavljamo da bilo tko uključen u proces glasanja ima pristup *oglasnoj ploči* gdje svi glasači objavljuju svoje poruke. Poruke su autentične i identitet glasača koji je postavio poruku ne može biti krivotvoren niti poruke ne mogu biti neovlaštene. Poruke su poredane po redoslijedu dolaska (ili, ekvivalentno, svaka poruka sadrži vrijeme kada je poslana) i jednom kad se poruka postavi, nitko je može izbrisati s oglasne ploče. Napomenimo da ne pretpostavljamo da postoje privatni kanali između glasača i nadležnih osoba.

Opisat ćemo protokol za glasanje koji koristi kriptografske brojače, a dokazuje sljedeći teorem:

**Teorem 2.2.7.** *Shema elektroničkog glasanja koja zadovoljava provjerljivost, privatnost i robusnost može biti efikasno konstruirana iz proizvoljnog provjerljivog, ograničenog kriptografskog brojača sigurnog od zlonamjernog protivnika (gdje su glasovi ograničeni na skup {0,1}).*

*Skica dokaza.* Opisat ćemo protokol glasanja uz pretpostavku da postoji provjerljivi, ograničeni kriptografski $n$-brojač (gdje su glasovi ograničeni na skup {0,1}) siguran od zlonamjernog protivnika. Robusnost (s obzirom na odbor nadležan za izbore) slijedi ako je sam brojač robustan.

**POSTAVLJANJE SUSTAVA.** Odbor nadležan za izbore pokreće algoritam za generiranje ključeva za kriptografski $n$-brojač. Ovdje je $n$ izabran da bude jednak ukupnom broju glasača (ili gornjoj granici broja glasača ako je točan broj nepoznat). Ako želimo robusnost i/ili su neki glasači istovremeno osobe nadležne za izbore, ključevi se mogu generirati na način opisan prije iskaza teorema. Javni ključ $pk$ i početno stanje $s_0$ objavljeni su svim glasačima. Generiranje ključeva bi mogao biti najskuplji dio cijelog protokola, ali ta se operacija radi samo jednom i može biti obavljena mjesecima prije održavanja izbora.

**GLASANJE.** Brojač uvijek pamti ukupan broj glasova do sada. Vrijednost trenutnog brojača je uvijek definirana kao najnovija postavljena vrijednost brojača. Označimo brojač nakon $i$-tog glasa sa $s_i$. Tada $(i+1)$.-vi glas bilježi ovako: glasač pogleda stanje trenutnog brojača i računa novo stanje $s_{i+1}$ koristeći tranzicijsku funkciju, prijašnje stanje $s_i$, svoj odabir glasa $v \in \{0,1\}$ i javni ključ $pk$. Glasač objavljuje ažurirano stanje $s_{i+1}$ koje tada postaje trenutno stanje (jer je to sada najnoviji postavljeni brojač). Ovaj postupak se ponavlja $L$ rundi sve dok svaki glasač nije glasao jednom. Univerzalna provjerljivost (pa tako i korektnost glasova) slijedi iz provjerljivosti brojača, a privatnost glasača slijedi iz

definicije 2.2.5. Robusnost slijedi iz distribuiranog generiranja ključeva i dešifriranja.

**EVIDENTIRANJE.** Kada je glasanje završeno, osoba nadležna za izbore utvrđuje konačan ishod tako da dešifrira posljednji (validni) brojač. Ako postoji više osoba nadležnih za izbore, potrebno je koristiti "treshold dešifriranje". Možda bi bilo poželjno da odbor nadležan za izbore dokaže korektnost dešifiranja; primijetimo da nije prihvatljivo samo objaviti tajni ključ, jer bi to omogućilo retroaktivno određivanje glasova svakog birača. U slučaju kada se šifriranje provodi pomoću kvadratnih ostataka, odbor može lako dokazati da je dešifriranje korektno tako da objavi $x$ za svaku šifriranu vrijednost $y$ tako da vrijedi
$y = \pm\, x^2$.

□

Za ovu metodu korištene su informacije iz [38]. Također, tamo se mogu naći detaljni opis konstrukcije kriptografskih brojača, analiza složenosti korištenih funkcija te detaljan opis efikasnog kriptografskog brojača.

## Mix mreže

U ovom odjeljku ukratko ćemo opisati tzv. *mix mreže*, metodu kojom se osigurava privatnost i provjerljivost u elektroničkom glasanju.
Za početak ćemo definirati ElGamalov kriptosustav. [20]

**Definicija 2.2.8.** *(ElGamalov kriptosustav)*
*Neka je* $\mathrm{p}$ *prost broj i* $\alpha \in \mathbb{Z}_p^*$ *primitivni korijen modulo* $\mathrm{p}$. *Neka je* $\mathrm{P} = \mathbb{Z}_p^*$, $\mathrm{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ *i*

$$\mathrm{K} = \{(\, p,\, \alpha,\, a,\, \beta\,) : \beta \equiv \alpha^a \pmod{\mathrm{p}}\}\,.$$

*Vrijednosti* $\mathrm{p}$, $\alpha$ *i* $\beta$ *su javne, a vrijednost* $a$ *je tajna. Za* $\mathrm{K} = (\, p,\, \alpha,\, a,\, \beta\,) \in \mathrm{K}$ *i tajni slučajni broj* $\mathrm{k} \in \mathbb{Z}_{p-1}$ *definiramo:*

$$e_K(x, k) = (y_1, y_2),$$

*gdje je* $y_1 = \alpha^k \bmod p$ *i* $y_2 = x\beta^k \bmod p$. *Za* $y_1,\, y_2 \in \mathbb{Z}_p^*$ *definiramo:*

$$d_K(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p.$$

**Napomena 2.2.9.** *Od sada ćemo sve aritmetičke operacije računati modulo p, osim ako drugačije ne istaknemo.*

ElGamal ima multiplikativno homomorfno svojstvo. To znači da za dva dana ElGamalova šifrata (nad istim javnim ključem $\beta$) $(y_1,y_2) = (\alpha^{k_1}, x_1\beta^{k_1})$ i $(y_3,y_4) = (\alpha^{k_2}, x_2\beta^{k_2})$, gdje su $x_1$ i $x_2$ otvoreni tekstovi, tada je produkt $(y_1,y_2) \cdot (y_3,y_4) = (y_1,y_3) \cdot (y_2,y_4) = (\alpha^{k_1+k_2}, x_1 \cdot x_2\beta^{k_1+k_2})$ šifrat od $x_1 \cdot x_2$.

Ako je poznat ElGamalov šifrat od $x$ uz javni ključ $\beta$, $(y_1,y_2) = (\alpha^k, x\beta^k)$, može se transformirati u drugačiji šifrat tako da se slučajno izabere $k' \in \mathbb{Z}_p$ i izračuna $(y_1',y_2') = (y_1 \cdot \alpha^k, y_2 \cdot \beta^{k'})$ te tako dešifrira isti otvoreni tekst $x$. Koristeći *odlučivu Diffie-Hellmanovu* (DDH) [7] pretpostavku , treća strana ne može utvrditi jesu li otvoreni tekstovi $(y_1,y_2)$ i $(y_1',y_2')$ jednaki, to jest ElGamal kriptosustav je semantički siguran (jedino se zanemarive informacije o otvorenom tekstu mogu izvući iz šifrata). Drugim riječima, šifrati izgledaju potpuno drugačije, a ne može se utvrditi je li njihov otvoreni tekst jednak ili različit.

Koncept mix mreža uveo je David Chaum 1981. godine. Mix mreža je kriptografska metoda koja omogućuje jednom ili više mix servera da uzmu niz šifriranih primljenih poruka, ponovno ih šifriraju ili ih dešifriraju te ih iznesu u neobjavljenom, nasumično permutiranom poretku. U teoriji, ako postoji jedna poštena mix mreža, permutacijske veze su sigurne. Mix mreže mogu se podijeliti na *ponovno šifrirajuće* mix mreže i *dešifrirajuće* mix mreže. Chaum je predložio dešifrirajuće mix mreže, gdje su ulazni podaci u mix mrežu glasački listići šifrirani uz javni ključ svakog mix servera, od zadnjeg mix servera prema prvom. Pri dešifriranju, svaki mix server će prvo dešifrirati ulazni glasački listić pomoću svog tajnog ključa, zatim će izbaciti slučajnu vrijednost te će kao izlazni podatak dati sve nastale poruke u permutiranom poretku.

Ponovno šifrirajuće mix mreže predstavljene su u [34]. U ponovno šifrirajućim mix mrežama originalni glasački listići šifrirani su uz isti ElGamalov javni ključ $\beta$, a odgovarajući tajni ključ je distribuiran povjerenicima u "treshold shemi". U ponovno šifrirajućim mix mrežama procesi ponovnog šifriranja i dešifriranje su odvojeni. Svaki mix server prvo ponovno šifrira listu ElGamalovih šifrata $\{e_1, e_2, ..., e_N\}$ i za rezultat daje šifrate u slučajno permutiranom poretku kao još jednu listu ElGamalovih šifrata $\{e_1', e_2', ..., e_N'\}$, nakon čega sljedeća mreža ili dešifriranje može početi. Kad završi faza ponovnog šifriranja, povjerenici za dešifriranje zajednički dešifriraju sve glasačke listiće pomoću tajnog ključa $a$.
Na kraju cjelokupnog procesa povjerenici mogu vidjeti za koga je određen broj ljudi glasao, ali kako je poredak glasačkih listića promijenjen, ne može se utvrditi za koga je pojedina osoba glasala.

[7] Pretpostavimo da nam je dana ciklička grupa $G$ reda $q$ s generatorom $g$. DDH pretpostavka kaže da za dane $g^a$ i $g^b$, gdje su $a, b \in \mathbb{Z}_q$ slučajno izabrani, vrijednost $g^{ab}$ "izgleda" kao slučajan element grupe $G$.

Sada ćemo opisati postupak glasanja. Radi jednostavnosti, pretpostavimo da postoji samo jedno biračko mjesto, koje ćemo označiti sa BM te jedan glasački stroj koji može biti maliciozan. Kada izbori počnu, BM prikupi sve glasove i objavi ih na oglasnu ploču. Pristup oglasnoj ploči, na kojoj se nalaze objavljeni podaci, imaju autorizirani korisnici i bilo koji promatrači. Autorizirani korisnici imaju pravo pisati po ploči dok promatrači smiju čitati sadržaj ploče. U procesu glasanja postoji *povjerenstvo za dešifiriranje*. U njemu se nalazi $K$ ljudi koji posjeduju ključeve za dešifriranje koji se koriste pri dešifriranju glasačkih listića. Član povjerenstva smije postaviti podatke na oglasnu ploču. Još jedna pretpostavka vezana za glasanje je da samo zakoniti glasači smiju glasati te da će oni moći glasati samo jednom. Glasači glasaju koristeći vlastiti digitalni potpis te ih ukupno ima $N$.

**POSTAVLJANJE SUSTAVA.** U ovoj fazi BM inicijalizira oglasnu ploču te objavljuje sve poznate podatke (iz definicije 2.2.8), gdje su definirani svi javni ključevi koji se koriste tijekom izbora te opis hash funkcije $H$. Svi serveri za dekriptiranje i BM objavljuju svoje potvrđene javne ključeve. Također, imena kandidata su kodirana i objavljena svima koji sudjeluju u glasanju.

**GLASANJE.** U ovoj fazi BM potvrđuje identitet svakog glasača i provjerava je li on/ona već glasao/glasala. Ako nije, glasač glasa koristeći glasački stroj prema fiksiranom protokolu i dobiva posebnu priznanicu potpisanu od strane BM, nakon čega će njegov/njezin glasački listić biti objavljen na oglasnoj ploči.

**MIJEŠANJE GLASOVA.** Pretpostavit ćemo da postoji *odbor za miješanje glasova*. Posao tog odbora je da promiješa šifrirane glasove. Član tog odbora može biti bilo koji potvrđeni sudionik i članova smije biti proizvoljno mnogo. Mi ćemo pretpostaviti da je barem jedan član odbora pošten. Svaki član odbora uzima šifirirane listiće s oglasne ploče, promiješa ih i tako promiješane postavi ponovno na oglasnu ploču. Nakon toga sljedeći član ponavlja isti postupak ili povjerenstvo za dešifiranje obavlja svoj posao.

**DEŠIFRIRANJE GLASOVA.** U ovoj fazi povjerenstvo za dešifriranje proučava glasačke listiće. Osim dešifriranja, otkrivaju se neki dodatni podaci vezani za provjerljivosti njihovih akcija. Konačan rezultat je anonimna lista glasačkih listića.

Koristeći [37], ukratko smo opisali način na koji se mix mreže koriste u elektroničkom glasanju. U tom članku mogu se naći detaljnije opisane prethodne faze glasanja.

# Poglavlje 3

# Sigurnosni protokoli

Do sada smo opisali nekoliko metoda koje se mogu koristiti pri elektroničkom glasanju, ali i u neke druge svrhe. Vidjeli smo da zadovoljavaju osnovna svojstva navedena u prošlom poglavlju, od kojih su glavna bila da ni glasači ni povjerenici za glasanje ne varaju te da se osigura privatnost i anonimnost glasača. Postavljaju se pitanja: Što ako se u proces glasanja umiješa treća strana koja može promijeniti ishod glasanja? Možemo li neke alate koje smo spominjali upotrijebiti kako bismo osigurali sigurnu komunikaciju? U ovom poglavlju, koristeći [45], opisat ćemo neke sigurnosne protokole koji se mogu upotrijebiti u elektroničkom glasanju.

## 3.1 Uljezi u sredini i varalice

Izraz uljez u sredini (engl. *Intruder-in-the-middle*) koristi se kada se dogodi neautorizirano presretanje informacija. Za primjer uzmimo Alice i Boba koji razmjenjuju poruke. Oni žele utvrditi zajednički ključ za komunikaciju koristeći tzv. Diffie - Hellmanovu shemu, koja ovako izgleda:

1. Ili Alice ili Bob bira veliki, prosti broj $p$ i primitivni korijen $\alpha$ (mod $p$). $p$ i $\alpha$ mogu biti i javno objavljeni.

2. Alice odabire tajni slučajni broj $x$ za koji vrijedi $1 \leqslant x \leqslant p$ - 2, a Bob bira slučajni broj $y$ za koji vrijedi $1 \leqslant y \leqslant p$ - 2.

3. Alice šalje $\alpha^x$ (mod $p$) Bobu, a Bob šalje $\alpha^y$ (mod $p$) Alice.

4. Koristeći poruke koje su primili, svatko od njih dvoje može izračunati ključ $K$. Alice računa $K$ kao $K \equiv (\alpha^y)^x \bmod p$, a Bob računa $K$ kao $K \equiv (\alpha^x)^y \bmod p$.

Sada ćemo opisati kako izgleda napad uljeza u sredini.

1. Eva odabire eksponent $z$.
2. Eva saznaje vrijednosti $\alpha^x$ i $\alpha^y$.
3. Eva šalje $\alpha^z$ Alice i Bobu. (Alice misli da je dobila $\alpha^y$, a Bob misli da je dobio $\alpha^x$).
4. Eva računa $K_{AE} \equiv (\alpha^x)^z \pmod{p}$ i $K_{EB} \equiv (\alpha^y)^z \pmod{p}$. Alice, koja ne zna da se Eva nalazi u sredini, računa $K_{AE}$, a Bob računa $K_{EB}$.
5. Kada Alice šalje poruku Bobu, šifriranu s $K_{AE}$, Eva je presretne, dešifrira, šifrira s $K_{EB}$ i šalje Bobu. Bob tu poruku dešifrira sa $K_{EB}$ i otkriva sadržaj poruke. Bob nema razloga vjerovati da je komunikacija bila nesigurna, a s druge strane Eva također otkriva sadržaj poruke.

Kako bi se izbjegao napad uljeza u sredini, poželjno je imati postupak gdje Alice i Bob provjeravaju identitete međusobno, dok se ključ formira. Protokol koji to može učiniti poznat je kao *dogovor pomoću autentičnog ključa*.

Standardni način za zaustavljanje uljeza u sredini je *stanica prema stanici* (STS) protokol koji koristi digitalne potpise. Svaki korisnik $U$ ima funkciju $sig_U$ digitalnog potpisa skupa s algoritmom za provjeru $ver_U$. Na primjer, $sig_U$ može proizvesti RSA ili ElGamalov potpis, a $ver_U$ provjerava validnost potpisa za korisnika $U$. Algoritami za provjeru su kompilirani i objavljeni javno od strane povjerenika kojeg ćemo nazvati *Trent*. Trent potvrđuje da je $ver_U$ algoritam za provjeru za korisnika $U$, a ne za Evu.

Pretpostavimo sada da Alice i Bob žele uspostaviti ključ koji će se koristiti u funkciji šifriranja $E_K$. Komunikacija se odvija pomoću Diffie - Hellmanove razmjene ključeva, ali su dodani digitalni potpisi:

1. Alice i Bob odabiru veliki, prosti broj $p$ i primitivni korijen $a$.
2. Alice nasumično odabire $x$, a Bob nasumično odabire $y$.
3. Alice računa $\alpha^x \pmod{p}$, a Bob računa $\alpha^y \pmod{p}$.
4. Alice šalje $\alpha^x$ Bobu.
5. Bob računa $K \equiv (\alpha^x)^y \pmod{p}$.
6. Bob šalje $\alpha^y$ i $E_K(sig_B(\alpha^y, \alpha^x))$ Alice.
7. Alice računa $K \equiv (\alpha^y)^x \pmod{p}$.
8. Alice dešifrira $E_K(sig_B(\alpha^y, \alpha^x))$ da bi saznala $sig_B(\alpha^y, \alpha^x)$.

9. Alice moli Trenta da provjeri je li $ver_B$ Bobov algoritam za provjeru.
10. Alice koristi $ver_B$ da potvrdi Bobov potpis.
11. Alice šalje $E_K(sig_A(\alpha^x, \alpha^y))$ Bobu.
12. Bob dešifrira, moli Trenta da provjeri je li $ver_A$ Alicein algoritam za provjeru i onda koristi $ver_A$ da potvrdi Alicein potpis.

Primijetimo da su Alice i Bob sigurni da koriste isti ključ $K$, jer je malo vjerojatno da bi netočan ključ dao validan potpis. Također, u ovom protokolu je važno povjerenje. Ako žele razmjenjivati poruke preko sigurnog kanala, Alice i Bob moraju vjerovati Trentovoj provjeri. U ovom poglavlju, povjerenici kao Trent će biti važni sudionici u protokolima.

## 3.2 Kerberos

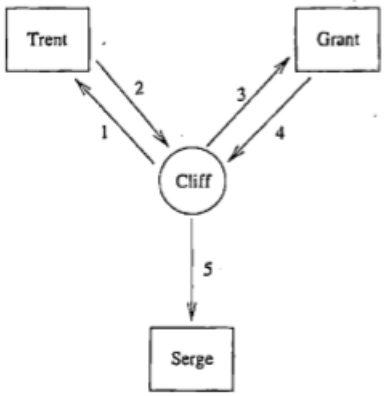
U grčkoj mitologiji **Kerberos** je bio troglavi pas koji je čuvao ulaz u podzemlje (Had). Isti naziv koristi se za implementaciju simetričnog kriptografskog protokola čija je namjena omogućiti ovjeravanje autentičnosti i sigurnost u razmjeni ključeva između korisnika u mreži. Pod pojmom *korisnik* podrazumijevamo osobu ili program koji želi komunicirati s drugim programom. Kerberos je nastao iz velikog projekta na MIT-u, poznatog kao *Project Athena*. Svrha Athene bila je omogućiti veliku mrežu računala za studente MIT-a, dopuštajući tako studentima jednostavan pristup njihovim datotekama.
Kod ovakvog okruženja postavljaju se pitanja oko sigurnosti mreže. U principu, komunikacije preko javne mreže kao što je Athena je jako nesigurna. Lako je moguće vidjeti podatke koji putuju kroz mrežu kao što su lozinke i ostali privatni podaci. Kerberos je razvijen zato da bi riješio takve sigurnosne probleme. U nastavku ćemo dati osnovni Kerberos - model i opisati što je to te što se njime pokušava postići.

Kerberos se bazira na arhitekturi klijent/poslužitelj. Klijent je korisnik ili neki softver koji ima zadatak koji želi izvršiti. Poslužitelj služi da bi omogućio usluge koje klijent traži.

Osnovni Kerberos - model ima sljedeće sudionike:

- Cliff predstavlja klijenta;
- Serge predstavlja poslužitelja;
- Trent predstavlja povjerenika;
- Grant predstavlja poslužitelja za izdavanje ulaznica.

Povjerenik je poznat i kao poslužitelj za provjeru autentičnosti. Također, možemo reći da je Cliff sada ono što je Alice bila, a Serge ono što je Bob bio u prijašnjim modelima. Na početku, Cliff i Serge nemaju nikakvu informaciju o tajnom ključu, a svrha Kerberosa je da svakom od njih da tu informaciju na siguran način. Rezultat Kerberos protokola je taj da će Serge imati provjereni Cliffov identitet te će tajni ključ biti uspostavljen.




Slika 3.1: Kerberos

Ovaj protokol, opisan na slici 3.1, počinje tako da Cliff zatraži ulaznicu od Trenta. Trent ima pristup bazi podataka u kojoj se nalaze informacije o lozinkama za sve klijente (zato se Trent ponekad naziva "Kerberosov server"). Trent vraća ulaznicu koja je šifrirana s klijentovom informacijom o tajnoj lozinci. Cliff sada želi koristiti uslugu koju Serge pruža, ali prije nego to uspije, mora mu biti dozvoljena komunikacija sa Sergeom. Cliff daje svoju ulaznicu Grantu. Grant uzima njegovu ulaznicu i ako je sve u redu (sjetimo se da ulaznica sadrži neke informacije koje identificiraju Cliffa), onda Grant daje Cliffu novu ulaznicu koja će omogućiti Cliffu da koristi Sergeove usluge (i samo Sergeove; ova ulaznica neće biti upotrebljiva ako želi komunicirati s drugim serverom, npr. Sarom). Cliff sada ima poslužiteljsku ulaznicu, koju sada može prikazati Sergeu. Cliff šalje Sergeu poslužiteljsku

ulaznicu skupa s uvjerenjem o autentičnosti. Serge provjerava ulaznicu s uvjerenjem o autentičnosti da se uvjeri da je važeća. Ako je tada sve u redu, Serge će pružiti uslugu Cliffu.

Sada ćemo pogledati Kerberos malo detaljnije, tj. opisat ćemo kako se šalju poruke između sudionika.

1. C → T: Cliff šalje poruku Trentu, a poruka sadrži njegovo ime i ime poslužitelja za izdavanje ulaznica (u ovom slučaju to je Grant).

2. T → C: Trent traži Cliffovo ime u bazi podataka. Ako ga nađe, on generira tajni ključ $K_{CG}$ koji će biti korišten između Cliffa i Granta. Trent također ima tajni ključ $K_C$ pomoću kojeg može komunicirati s Cliffom pa ga on koristi da bi mogao šifrirati Cliff-Grantov tajni ključ:

   $$T = e_{K_C}(K_{CG}).$$

   Dodatno, Trent kreira *ulaznicu za odobravanje* (TGT), koja će koristiti Cliffu da potvrdi svoju autentičnost Grantu. Ulaznica je šifrirana koristeći Grantov tajni ključ, kojeg Trent također posjeduje:

   $TGT$ = Grantovo ime$\|e_{K_G}$(Cliffovo ime, Cliffova adresa, VremenskaOznaka1, $K_{CG}$).

   Ovdje || označava konkatenaciju. Ulaznica koju Cliff dobiva je konkatenacija sljedeće dvije ulaznice:

   $$Ticket = T\|TGT$$

3. C → G: Cliff može saznati $K_{CG}$ pomoću ključa $K_C$, kojeg dijeli s Trentom. Koristeći $K_{CG}$, Cliff sada može sigurno komunicirati s Grantom. Cliff sada generira *provjeritelja*, koji će se sastojati od njegovog imena, njegove adrese i vremenske oznake. To će šifrirati koristeći $K_{CG}$ da bi dobio:

   $$Auth_{CG} = e_{K_{CG}}(\text{Cliffovo ime, Cliffova adresa, VremenskaOznaka2}).$$

   Cliff sada šalje $Auth_{CG}$ i $TGT$ Grantu tako da Grant može izdati *poslužiteljsku ulaznicu*.

4. G → C: Grant sada posjeduje $Auth_{CG}$ i $TGT$. Dio $TGT$-a je šifriran koristeći Grantov tajni ključ pa Grant može izvući taj dio i dešifrirati ga. Dakle, Grant može saznati Cliffovo ime, Cliffovu adresu, VremenskuOznaku1 te $K_{CG}$. Grant sada može koristiti $K_{CG}$ za dešifriranje $Auth_{CG}$ da bi provjerio autentičnost Cliffovog zahtijeva. To jest, $d_{K_{CG}}(Auth_{CG})$ će dati još jednu kopiju Cliffovog imena, Cliffove adrese i drugačiju vremensku oznaku. Ukoliko se dvije verzije Cliffovog imena i adrese podudaraju te su VremenskaOznaka1 i VremenskaOznaka2 dovoljno blizu jedna drugoj, onda će Grant proglasiti Cliffa validnim. Sada kad je Cliff odobren od strane Granta, Grant će generirati ključ $K_{CS}$ da bi Cliff mogao komunicirati sa Sergeom i također će vratiti Cliffu poslužiteljsku ulaznicu. Grant posjeduje tajni ključ $K_S$ kojeg dijeli sa Sergeom. Poslužiteljska ulaznica je:

$$ServTicket = e_{K_S}(\text{Cliffovo ime, Cliffova adresa, VremenskaOznaka3, VrijemeIsteka}, K_{CS}).$$

Ovdje VrijemeIsteka označava vrijeme valjanosti za tu poslužiteljsku ulaznicu. Ključ se šifrira koristeći ključ korišten između Cliffa i Granta:

$$e_{K_{CG}}(K_{CS}).$$

Grant šalje *ServTicket* i $e_{K_{CG}}(K_{CS})$ Cliffu.

5. C → S: Cliff je sada spreman koristiti Sergeove usluge. On počinje sa dešifriranjem $e_{K_{CG}}(K_{CS})$ kako bi saznao ključ $K_{CS}$ kojeg će koristiti za komunikaciju sa Sergeom. Cliff kreira provjeritelja:

$$Auth_{CS} = e_{K_{CS}}(\text{Cliffovo ime, Cliffova adresa, VremenskaOznaka4}).$$

Cliff sada šalje Sergeu $Auth_{CS}$ skupa sa *ServTicket*. Serge može dešifrirati *ServTicket* i iz toga izvući ključ $K_{CS}$ kojeg će moći koristiti. Koristeći taj ključ, on može dešifrirati $Auth_{CS}$ i provjeriti da je Cliff osoba koja se tako predstavila i nalazi li se VremenskaOznaka4 u intervalu između VrijemeIsteka i VremenskaOznaka3. Ako ne, Cliffova ulaznica nije upotrebljiva te će Serge odbaciti Cliffov zahtjev za uslugom. Inače, Cliff i Serge mogu koristiti zajednički ključ $K_{CS}$ da bi mogli obaviti svoju razmjenu.

## 3.3 Infrastrukture javnog ključa

Vidjeli smo da je kriptografija javnog ključa moćan alat koji omogućuje provjeru autentičnosti, razmjenu ključeva i zaštitu osobnih podataka. U navedenim primjenama, ključ je objavljen javno, ali kada pristupimo javnom ključu, kako znamo da Alicein javni ključ pripada Alice? Možda je Eva postavila svoj javni ključ tamo gdje je trebao biti Alicein. Ako ne postoji povjerenje u način na koji su ključevi generirani, koristi kriptografije javnog ključa su minimalne.

Da bi kriptografija javnog ključa bila upotrebljiva u aplikacijama, posebno u elektroničkom glasanju, potrebno je imati infrastrukturu koja vodi računa o javnim ključevima. **Infrastruktura javnog ključa** (skraćeno PKI) je struktura gdje su definirana pravila pod kojima funkcioniraju kriptografski sustavi i postupci za generiranje i objavljivanje ključeva i certifikata. Sve PKI sastoje se od procesa potvrde i provjere valjanosti. Proces potvrde povezuje javni ključ s entitetom kao što je korisnik ili dio informacija. Provjera valjanosti jamči da su potvrde (certifikati) valjane.

*Certifikat* je količina informacija koju je potpisao njegov izdavač koji se obično naziva *certifikacijskim tijelom* (CA). Postoje mnoge vrste certifikata. Dva najpopularnija su certifikati o identitetima i certifikati o vjerodostojnosti. Certifikati o identitetu sadrže podatke o identitetu entiteta, kao što su adresa e-pošte i popis javnih ključeva entiteta. Certifikati vjerodajnica sadrže podatke koji opisuju prava pristupa. U oba slučaja, podaci se obično šifriraju pomoću privatnog ključa od CA-a.

Pretpostavimo da imamo PKI, a CA objavljuje certifikate o identitetima za Alice i Bob. Ako Alice zna javni ključ od CA-a, onda može preuzeti objavljeni šifrirani certifikat o identitetu za Boba te izvući Bobove informacije o identitetu, kao i popis javnih ključeva potrebnih za sigurnu komunikaciju s Bobom. Razlika između ovog scenarija i konvencionalnog scenarija javnog ključa jest da Bob ne objavljuje ključeve, ali umjesto toga, odnos povjerenja nalazi se između Alice i izdavača. Alice možda ne bi vjerovala Bobu onoliko koliko bi mogla vjerovati CA-u, kao što je vlada ili telefonska tvrtka. *Koncept povjerenja* ključan je za PKI i možda je jedno od najvažnijih svojstava PKI-a.

Malo je vjerojatno da bi jedan entitet mogao voditi računa o javnim ključevima svakog korisnika interneta i izdavati ih. Umjesto toga, PKI-ovi se često sastoje od više CA-a kojima je dopušteno međusobno potvrđivanje s potvrdama koje izdaju. Dakle, Bob bi mogao biti povezan s drugim CA-om nego Alice, a kada bi zatražila Bobov certifikat o identitetu, Alice bi se mogla pouzdati samo ako njezin CA ima povjerenje u Bobov CA. Na velikim mrežama poput interneta, između Alice i Boba mogu postojati mnogi CA, a postaje neop-

hodno da za svaki od CA koji se nalazi između nje i Boba postoji međusobno povjerenje. Osim toga, većina PKI-ova ima različite razine povjerenja, omogućujući nekim CA-ima da potvrde druge CA-e s različitim stupnjevima povjerenja. Moguće je da CA može vjerovati samo drugim CA-ima za obavljanje određenih zadataka. Na primjer, Alicein CA može vjerovati samo Bobovom CA-u da bi dobila certifikat o Bobu, a ne vjerovati drugim CA-ovima, dok Alicein CA može vjerovati Daveovom CA-u da bi dobila certifikat o nekom drugom. Povezani odnosi mogu postati vrlo razrađeni i budući da ti odnosi postaju složeniji, postaje sve teže utvrditi u kojoj mjeri Alice vjeruje certifikatu koji prima.
U sljedećem potpoglavlju ćemo raspravljati o primjeru PKI-ja koji se koristi u praksi.

## 3.4 Pretty Good Privacy

**Pretty Good Privacy** (PGP) je infrastruktura javnog ključa koju je razvio Phil Zimmerman kasnih 1980-ih i ranih 1990-ih. PGP je prilično decentralizirani sustav koji ne koristi CA. Svaki korisnik ima certifikat, ali povjerenje u taj certifikat je ovjereno različitim stupnjevima od strane drugih korisnika. To stvara mrežu povjerenja.
Da bismo malo bolje objasnili posljednje dvije rečenice, dajemo primjer. Ako Alice poznaje Boba i može izravno potvrditi da je njegov certifikat valjan, onda ona potpiše njegov certifikat svojim javnim ključem. Charles se pouzdaje u Alice i ima svoj javni ključ, stoga može provjeriti je li Alicein potpis na Bobovom certifikatu valjan. Charles tada vjeruje u Bobov certifikat. Međutim, to ne znači da Charles vjeruje certifikatima koje Bob potpisuje - on vjeruje Bobovom javnom ključu. Bob bi mogao biti lakovjeran i potpisati svaki certifikat koji susreće. Njegov će potpis biti valjan, ali to ne znači da je certifikat valjan.

Svaki korisnik, na primjer Alice, održava datoteku s ključevima koja sadrži razine povjerenja koje Alice ima u potpisima različitih ljudi. Razine povjerenja koje netko može dodijeliti su: nema podataka, nema povjerenja, djelomično povjerenje i potpuno povjerenje. Kada se ocjenjuje valjanost certifikata, PGP program prihvaća certifikate koje su potpisali ljudi u koje Alice ima povjerenja ili dovoljnu kombinaciju djelomičnih povjerenja, inače će program upozoriti Alice i ona mora odabrati hoće li nastaviti.

PGP se primarno upotrebljava za provjeru autentičnosti i šifriranje poruka. U elektroničkom glasanju, povjerenik mora provjeriti autentičnost glasača prije nego što bi glasač mogao glasati. Nakon toga, sve poruke koje se šalju između glasača i povjerenika moraju biti šifrirane da treća strana ne bi mogla presresti poruku i napraviti nešto zlonamjerno. U nekim slučajevima poželjno je da se pri slanju poruke istovremeno provjeravaju autentičnost i šifrira poruka. Pokazat ćemo kako se PCP ponaša u slučaju provjere autentičnosti, u slučaju šifriranja poruka i u slučaju istovremene provjere autentičnosti i šifriranja poruka. Nadalje, pretpostavit ćemo da Alice uvijek šalje poruke Bobu.

## Provjera autentičnosti

1. Alice obično koristi hash funkciju SHA-1 da bi dobila hash vrijednost poruke.
2. Alice potpisuje hash tako da ju podiže na svoj tajni eksponent $d$ mod $n$. Rezultat toga (hash kod) se stavlja na početak poruke koja se šalje Bobu.
3. Bob podiže hash kod na eksponent $e$, koji se nalazi u javnom RSA od Alice. Dobiveni rezultat se uspoređuje s hash-om ostatka poruke.
4. Ako se rezultat slaže s hash-om i ako Alice vjeruje u Bobov javni ključ, poruka je prihvaćena i smatra se da dolazi od Boba.

Primijetimo da povjerenje ima važnu ulogu u procesu provjere autentičnosti. Ako Bob ne vjeruje u Alicein javni ključ, ne može biti siguran dolazi li poruka od Alice ili Eve.

## Šifriranje

1. Aliceino računalo generira slučajni broj, obično 128 bita, koji će se koristiti kao ključ za algoritam šifriranja privatnih ključeva, npr. 3DES, IDEA ili CAST-128. Taj ključ, koji se koristi više puta u razmjeni poruka, zvat ćemo ključ sesije.
2. Alice koristi algoritam s ključem sesije kako bi šifrirala svoju poruku.
3. Alice šifrira ključ sesije pomoću Bobovog javnog ključa.
4. Šifrirani ključ i šifrirana poruka šalju se Bobu.
5. Bob koristi svoj privatni RSA ključ za dešifriranje ključa sesije. Zatim koristi ključ sesije za dešifriranje Aliceine poruke.

Primijetimo da povjerenje nije potrebno ako je poželjno samo šifriranje poruka.

## Provjera autentičnosti i šifriranje

1. Alice hashira svoju poruku i potpisuje hash kako bi stvorila hash kod, kao u drugom koraku prethodno opisane provjere autentičnosti. Taj se hash kod stavlja na početak poruke.
2. Alice proizvodi slučajni 128-bitni ključ sesije i koristi algoritam s ovim ključem sesije kako bi šifrirala hash kod zajedno s porukom, kao u prije opisanom postupku šifriranja.
3. Alice koristi Bobov javni ključ za šifriranje ključa sesije.

4. Šifrirani ključ sesije i šifrirani hash kod i poruka šalju se Bobu.
5. Bob koristi svoj privatni ključ za dešifriranje ključa sesije.
6. Bob koristi ključ sesije kako bi dobio hash kod i poruku.
7. Bob provjerava potpis pomoću Aliceinog javnog ključa, kao u prethodno opisanom postupku provjere autentičnosti.

Naravno, ovaj postupak zahtijeva da Bob vjeruje Aliceinom certifikatu javnog ključa. Također, razlog potpisa prije šifriranja je taj da Bob nakon dešifriranja može pohraniti poruku koja sadrži otvoreni tekst s potpisom.

Podsjetimo se što znače brojevi $n$, $d$ i $e$ te usput ukratko opišimo kako postaviti PGP certifikat. Aliceino računalo koristi slučajni unos dobiven od pritisaka na tipke, pokreta miša i sl. kako bi pronašlo proste brojeve $p$ i $q$ i zatim izračunalo $n = pq$ i eksponente $e$ i $d$ koji se koriste u šifriranju i dešifriranju u RSA kriptosustavu. Brojevi $n$ i $e$ su tada Aliceini javni ključevi. Alice također odabire tajnu zaporku. Tajni ključ $d$ sigurno je pohranjen u njenom računalu. Kad računalo treba koristiti njezin privatni ključ, pita je za njezinu zaporku kako bi bilo sigurno da je to Alice. Ovo sprječava Evu da koristi Aliceino računalo i pretvara se da je Alice. Prednost ove lozinke je da Alice ne mora zapamtiti ili upisati eksponent dekriptiranja $d$ koji vjerojatno sadrži više od stotinu znamenki. Opisan je postupak gdje se koristio RSA kriptosustav za potpise, ali naravno da se ne mora isključivo on koristiti.

# Bibliografija


[1] *The Age of the Votomatic*, https://www.nytimes.com/2000/12/04/opinion/the-age-of-the-votomatic.html, posjećena srpanj, 2018.

[2] *Analysis of Electronic Voting schemes in the real world*, https://www.ukais.org/resources/Documents/ukais%202018%20proceedings%20papers/paper_17.pdf, posjećena srpanj, 2018.

[3] *Astronauts To Vote From Space*, https://www.nasa.gov/mission_pages/station/expeditions/expedition18/vote.html, posjećena srpanj, 2018.

[4] *Blind signatures*, https://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/blind_sigs.html, posjećena kolovoz, 2018.

[5] *The Constitutionality of Electronic Voting in Germany*, https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany, posjećena kolovoz, 2018.

[6] *Countries with e-voting projects*, http://www.aceproject.org/ace-en/focus/e-voting/countries, posjećena srpanj, 2018.

[7] *Cryptographic Hash Functions Definition*, https://www.investopedia.com/news/cryptographic-hash-functions/, posjećena kolovoz, 2018.

[8] *Democracy Rebooted: The Future of Technology in Elections*, http://publications.atlanticcouncil.org/election-tech/index.php, posjećena srpanj, 2018.

[9] *E-voting for IT land*, https://www.business-standard.com/article/beyond-business/e-voting-for-it-land-111072300044_1.html, posjećena kolovoz, 2018.

[10] *Expert Visit on New Voting Technologies*, https://www.osce.org/odihr/elections/22450?download=true, posjećena srpanj, 2018.

[11] *GI Narod odlučuje: Referendum za dopisno i elektroničko glasovanje za sve birače – u Hrvatskoj i izvan nje*, https://narod.hr/hrvatska/gi-narod-odlucuje-referendum-dopisno-elektronicko-glasovanje-birace-hrvatskoj-nje, posjećena srpanj, 2018.

[12] *Hash Function*, http://mathworld.wolfram.com/HashFunction.html, posjećena kolovoz, 2018.

[13] *i-Voting*, https://e-estonia.com/solutions/e-governance/i-voting/, posjećena kolovoz, 2018.

[14] *The Important Uses of Cryptography in Electronic Voting and Counting*, https://www.ndi.org/e-voting-guide/examples/cryptography-in-e-voting, posjećena srpanj, 2018.

[15] *MD5 Collision Attack Lab*, http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Crypto/Crypto_MD5_Collision/, posjećena kolovoz, 2018.

[16] *Minister says no to voting online in next election*, https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=6387118, posjećena kolovoz, 2018.

[17] *'Narod odlučuje' predao potpise za referendum u Saboru*, https://www.tportal.hr/vijesti/clanak/narod-odlucuje-predaje-potpise-za-referendum-u-saboru-foto-20180613, posjećena kolovoz, 2018.

[18] *Narod odlučuje tvrdi: 'Prikupili smo potpise'; Referendum kojim se smanjuju prava manjina ili će reagirati Ustavni sud?*, https://net.hr/danas/hrvatska/narod-odlucuje-tvrdi-prikupili-smo-dovoljno-potpisa-idemo-na-referendum-kojim-se-smanjuju-prava-manjina-ili-ce-reagirati-ustavni-sud/, posjećena srpanj, 2018.

[19] *Online Hash Functions*, http://www.convertstring.com/Hash, posjećena kolovoz, 2018.

[20] *Ostali kriptosustavi s javnim ključem*, https://web.math.pmf.unizg.hr/~duje/kript/josjavni.html, posjećena kolovoz, 2018.

[21] *RSA kriptosustav*, https://web.math.pmf.unizg.hr/~duje/kript/rsa.html, posjećena kolovoz, 2018.

[22] *Središnji državni portal - Glasovanje u inozemstvu*, https://gov.hr/moja-uprava/aktivno-gradjanstvo-i-slobodno-vrijeme/gradjani-u-

politickom-zivotu/glasovanje-u-inozemstvu/1736, posjećena kolovoz, 2018.

[23] *Središnji državni portal - Izbori*, https://gov.hr/moja-uprava/aktivno-gradjanstvo-i-slobodno-vrijeme/gradjani-u-politickom-zivotu/izbori/1580, posjećena kolovoz, 2018.

[24] *Sve što možda ne znate, a trebate znati o dopisnom i elektroničkom glasovanju*, https://narod.hr/hrvatska/sve-sto-mozda-ne-znate-trebate-znati-o-dopisnom-elektronickom-glasovanju, posjećena kolovoz, 2018.

[25] *What is running disparity (RD)?*, https://searchnetworking.techtarget.com/definition/running-disparity, posjećena kolovoz, 2018.

[26] B. Asolo, *What Is SHA-256 And How Is It Related to Bitcoin?*, https://www.mycryptopedia.com/sha-256-related-bitcoin/, posjećena kolovoz, 2018.

[27] S.R.A. Aziz, S. Ibrahim, M. Kamat i M. Salleh, *Secure E-voting with Blind Signature*, https://ieeexplore.ieee.org/document/1188334/, posjećena kolovoz, 2018.

[28] L. Barlow, *An Introduction to Electronic Voting*, https://pdfs.semanticscholar.org/87e0/50a900fce2fbc373fa3e5f33ac7f80ed4032.pdf, posjećena srpanj, 2018.

[29] B. Bergin, *All Your Lever Voting Machine Questions Answered (Admit It - You Have Them)*, https://www.wnyc.org/story/300838-your-lever-voting-machines-questions-answered-you-have-them-admit-it/, posjećena srpanj, 2018.

[30] D. Bernhard i B. Warinschi, *Cryptographic Voting — A Gentle Introduction*, https://eprint.iacr.org/2016/765.pdf, posjećena kolovoz, 2018.

[31] K. Brečić, *Elektroničko glasovanje u Hrvatskoj još nije moguće*, http://hr.n1info.com/a320317/Vijesti/Elektronicko-glasovanje-u-Hrvatskoj-jos-nije-moguce.html, posjećena kolovoz, 2018.

[32] A. Dujella, *Klasična kriptografija - Osnovni pojmovi*, https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html, posjećena kolovoz, 2018.

[33] L. Grubišić i R. Manger, *Mreže računala*, http://web.studenti.math.pmf.unizg.hr/~manger/mr/MR-skripta.pdf, posjećena kolovoz, 2018.

[34] K. Itoh, K. Kurosawa i C. Park, *Efficient Anonymous Channel and All/Nothing Election Scheme*, https://link.springer.com/content/pdf/10.1007%2F3-540-48285-7_21.pdf, posjećena kolovoz, 2018.

[35] B. Ivezić, *I Slovenci žele naš sustav za elektroničko glasovanje*, http://www.poslovni.hr/tehnologija/i-slovenci-zele-nas-sustav-za-elektronicko-glasovanje-283327, posjećena kolovoz, 2018.

[36] A. Jastrić, *Zagrebački Mobility uspješno podržao prve on-line izbore u Hrvatskoj*, https://www.ictbusiness.info/internet/zagrebacki-mobility-uspjesno-podrzao-prve-on-line-izbore-u-hrvatskoj, posjećena kolovoz, 2018.

[37] A. Jivanyan i G. Khachatryan, *New Receipt-Free E-Voting Scheme and Self-Proving Mix Net as New Paradigm*, https://eprint.iacr.org/2011/325.pdf, posjećena kolovoz, 2018.

[38] J. Katz, S. Myers i R. Ostrovsky, *Cryptographic Counters and Applications to Electronic Voting*, https://link.springer.com/content/pdf/10.1007/3-540-44987-6_6.pdf, posjećena kolovoz, 2018.

[39] J. Katz i M. Yung, *Threshold Cryptosystems Based on Factoring*, https://eprint.iacr.org/2001/093.pdf, posjećena kolovoz, 2018.

[40] S. Kumar i E. Walia, *Analysis of Electronic Voting system in various countries*, International Journal on Computer Science and Engineering **3** (2011), br. 5, 2, https://www.researchgate.net/publication/267235287_ANALYSIS_OF_ELECTRONIC_VOTING_SYSTEM_IN_VARIOUS_COUNTRIES.

[41] G. Lin i N. Espinoza, *Electronic Voting - Case Study: France*, https://cs.stanford.edu/people/eroberts/cs201/projects/2006-07/electronic-voting/index_files/page0005.html, posjećena kolovoz, 2018.

[42] B. Lynn, *Cryptography - Electronic Voting*, f, posjećena srpanj, 2018.

[43] R. Sietmann, *Aus für den digitalen Wahlstift*, https://www.heise.de/newsticker/meldung/Aus-fuer-den-digitalen-Wahlstift-196394.html, posjećena srpanj, 2018.

[44] L. Thomas, *France drops electronic voting for citizens abroad over cybersecurity fears*, https://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233, posjećena kolovoz, 2018.

[45] W. Trappe i L.C. Washington, *Introduction to Cryptography with Coding Theory, second edition*, Pearson, New Jersey, 2006.

# Sažetak

Ukratko, u ovom radu općenito smo opisali načine na koje se odvija elektroničko glasanje te kako se koriste elektronički sustavi za glasanje. U uvodu smo naveli prednosti koje ističu zagovornici te nedostatke na koje ukazuju protivnici elektroničkog glasanja. Nakon toga smo opisali kako su se razne tehnike koje se koriste u elektroničkom glasanju razvijale kroz povijest te zatim na koji način se određeni sustav koristi u nekim državama svijeta i u Republici Hrvatskoj.
U nastavku smo pokazali primjenu matematike i kriptografije u elektroničkom glasanju. Osnovni cilj kriptografije je osiguravanje sigurne komunikacije između dvije strane, što se postiže tako da se tekst koji se šalje transformira u neki drugi tekst. Prvo smo naveli koje matematičke funkcije se koriste za preslikavanje određenih riječi, tj. transformaciju teksta. Zatim smo opisali neke metode elektroničkog glasanja kojima je cilj osigurati korektnost, povjerljivost, anonimnost korisnika i nemogućnost komuniciranja više osoba tijekom glasanja. U svakoj od tih metoda opisan je proces glasanja.
U zadnjem poglavlju smo opisali tri sigurnosna protokola koja se mogu upotrijebiti u elektroničkom glasanju. U svakom od tih protokola opisan je način razmjene poruka sudionika te objašnjenje na koji način su sudionici sigurni da komuniciraju s pravom osobom. Poslije protokola ”Infrastrukture javnog ključa” opisan je primjer tog protokola koji se koristi u praksi.

# Summary

In this thesis, we have described the ways in which electronic voting is taking place and how electronic voting systems are used. In the introduction, we have highlighted the advantages pointed out by proponents and the disadvantages pointed out by opponents of electronic voting. After that, we have described how various techniques used in electronic voting have been developing through history, and then how a particular system is used in some countries of the world and in the Republic of Croatia.
After that we have demonstrated the use of mathematics and cryptography in electronic voting. The main purpose of cryptography is to ensure secure communication between the two sides, which is achieved so that the text being sent is transformed into another text. Firstly, we have identified which mathematical functions are used to map certain words, that is, text transformation. Then we have described some electronic voting methods that aim to ensure correctness, verifiability, user anonymity and the receipt-freeness. In each of these methods we have described the voting process.
In the last chapter, we have described three security protocols that can be used in electronic voting. Each of these protocols describes the way participants exchange their messages and explains how participants are sure to communicate with the right person. Following the ”Public Key Infrastructure” protocol, an example of this protocol used in practice is described.

# Životopis

Rođena sam 7. svibnja 1994. godine u Zagrebu, gdje sam završila osnovnu školu i X. gimnaziju "Ivan Supek". Internacionalni ispit za završetak srednjoškolskog obrazovanja (IGCSE) sam položila 2010. godine, iz predmeta matematika i engleski jezik. Državnu maturu položila sam 2012. godine, a iste godine upisala sam Preddiplomski sveučilišni studij matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Nakon završenog preddiplomskog studija 2016. godine, upisala sam Diplomski sveučilišni studij Računarstvo i matematika.