



УНИВЕРЗИТЕТ СИНГИДУНУМ
ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

**Могућности имплементације
електронског сервиса за гласање
преко Интернета у Србији**

- Дипломски рад -

Ментор:

Доц. др Саша Адамовић

Студент:

Марко Марковић

Бр. индекса: 2010200147

Београд, 2014.



ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

УНИВЕРЗИТЕТ СИНГИДУНУМ

ФАКУЛТЕТ ЗА ИНФОРМАТИКУ И РАЧУНАРСТВО

Београд, Данијелова 32

Кандидат: Марко Марковић

Број индекса: 2010200147

Смер: Информатика и рачунарство

Тема: Могућности имплементације гласања преко Интернета у Србији

Датум одобрења рада:
Београд, _____.____._____.

МЕНТОР

Доц. др Саша Адамовић

ДЕКАН

Проф. др Драган Цветковић

Могућности имплементације електронског сервиса за гласање преко Интернета у Србији

Сажетак:

У раду је анализирано тренутно стање развоја електронских сервиса у е-управи. Сервис који ћемо детаљно да разматрамо је сервис који би грађанству омогућио електронско гласање преко Интернета. Гласање преко Интернета понудило би низ погодности за обе стране. Међутим, сервис који би омогућио ову услугу, изграђен је на стандардним безбедносним протоколима који се користе и у другим протоколима у којима је неопходно обезбедити сервис аутентификације, интегритета и непорецивости. Обзиром да су постојећи сервиси за електронску трговину достигли висок ниво практичне безбедности, ту чињеницу узимамо као основу за могућности разматрања увођења сервиса за гласање преко Интернета у Србији. Размотрићемо све критичне тачке ових крипто система. Као највећи проблем намеће се аспект друштвене прихватљивости, а то подразумева поверилачки однос између грађана и сервиса, проблем анонимности, пребројавања и других важних активности који постоје унутар овог сервиса, а који се до сада у нашој земљи обавља на врло примитиван начин. Увођењем овог сервиса, трошкови читаве организације избора би били смањени, резултати би били обрађени у реалном времену са високом прецизношћу и поузданошћу, а са друге стране ергономичне особине би утицале на повећање излазности на изборе, а то би значило и доношење квалитетнијих одлука на нивоу целе земље.

Кључне речи: Интернет гласање, електронско гласање.

Possibilities of implementation of electronic services for voting over the Internet in Serbia

Abstract:

In this paper we address the current state of development of electronic services in e-government. The service that we will be discussing in detail is the service that would allow citizens electronic voting over the Internet. Internet voting would offer a number of benefits for both sides. However, a service that would provide this favor, is built on standard security protocol used in other protocols in which it is necessary to provide the service authentication, integrity and non-repudiation. Considering that existing services for e-commerce reached a high level of practical security, we take this fact as a basis for considering the possibilities of introducing the service to vote over the Internet in Serbia. We will consider all the critical points of the encryption system. The biggest problem arises aspect of social acceptance, and that includes creditor relationship between citizens and services, the problem of anonymity, counting and other important activities that exist within the service, which is so far in the country performs in a very primitive way. The introduction of this service, the cost of the entire election would be reduced, the results would be processed in real time with high accuracy and reliability, and on the other ergonomic features that affect the increase turnout in elections, and that would mean making better decisions at the national level. **Keywords:** Online voting, e-voting, remote voting.

САДРЖАЈ

1	Увод	5 -
1.1	Предмет истраживања.....	5 -
1.2	Структура рада.....	6 -
2	Преглед у области истраживања	7 -
2.1	Систем за гласање и доношење одлука	7 -
2.1.1	Кратка историја гласања	7 -
2.1.2	Интернет гласање	11 -
2.2	Преглед електронских система за гласање	13 -
2.2.1	Бушене картице за гласање.....	13 -
2.2.2	Оптички скенери за гласање.....	16 -
2.2.3	DRE (Direct recording electronic system)	17 -
2.3	Преглед система у е-управи	20 -
2.3.1	Појам е-управе	20 -
2.3.2	Основни системи е-управе.....	21 -
2.4	Истакнути системи за Интернет гласање у неким земљама ЕУ	22 -
2.4.1	Швајцарска.....	22 -
2.4.2	Естонија.....	24 -
3	Теоријске основе истраживања	27 -
3.1	Mixnet.....	27 -
3.2	Хомоморфна енкрипција	29 -
3.3	Дељење тајни (Secret sharing)	31 -
3.4	End-to-end	33 -
3.5	SSH.....	34 -
3.6	SSL (Secure Socket Layer).....	36 -
3.6.1	SSL i MITM	38 -
3.7	Хеш	38 -

3.8	ECC (<i>Elliptic curve cryptography</i>).....	- 40 -
3.9	Доказ нултог знања (Zero proof knowledge)	- 41 -
3.10	Верификација гласова	- 44 -
3.11	Аутентификација	- 45 -
3.12	Шема дупле коверте	- 46 -
4	Преглед предложеног решења	- 47 -
4.1	Генеричка шема	- 47 -
4.2	Поставка и објашњење експерименталног решења	- 48 -
4.3	Хомоморфност – Паилиеров алгоритам [5]	- 50 -
5	Закључак	- 55 -
5.1	Сумирани циљеви рада и остварени доприноси	- 55 -
5.2	Предлог за будући рад	- 55 -
	Литература.....	- 56 -

Слика 1. Римски новчић из 63. године п.н.е. на којем је представљен гласач који убацује свој глас у гласачку кутију.	- 7 -
Слика 2. Куглица и плочице од бронзе коришћене за различите врсте гласања у старој Грчкој.	- 8 -
Слика 3. Употребљене гласачке кутије.	- 8 -
Слика 4. Пример гласачког листића коришћен на општинским изборима у Ајови 1893. године.	- 9 -
Слика 5. Нацрт система за гласање који је предложен од стране Чариста.	- 10 -
Слика 6. Машина за гласање која користи полугу за одабир кандидата.	- 11 -
Слика 7. Један од првих типова бушених картица.	- 14 -
Слика 8. <i>Votomatic</i> уређај за бушење гласачких картица.	- 14 -
Слика 9. Проблем који се понекад јављао, делимично или случајно избушена рупа. ...	- 15 -
Слика 10. Тип гласачког листића коришћеног за оптички скенер.	- 16 -
Слика 11. Важеће ознаке које се броје.	- 16 -
Слика 12. Важеће које се не броје.	- 17 -
Слика 13. Не важеће ознаке.	- 17 -
Слика 14. Ознаке које се не могу прочитати из првог пута.	- 17 -
Слика 15. <i>Dre (Direct recording electronic system)</i>	- 18 -
Слика 16. Извештај у облику QR кода који се добија после одабира кандидата. ...	- 19 -
Слика 17. Животни век гласачког листића [7].	- 23 -
Слика 18. Естонска лична карта.	- 25 -
Слика 19. Систем преношења гласа у Естонији [8].	- 25 -
Слика 20. Систем мешања гласова (<i>Mixnets</i>) [11].	- 28 -
Слика 21. Хомоморфно додавање гласова [11].	- 31 -
Слика 22. Линија чији је полином степена 1, на којој су две тачке.	- 32 -
Слика 23. Линија чији је полином степена 1, на којој су три тачке.	- 32 -
Слика 24. Линија чији је полином степена 2, на којој су три тачке.	- 33 -
Слика 25. <i>SSH</i> протокол.	- 35 -
Слика 26. <i>SSL</i> протокол на ОСИ моделу.	- 36 -
Слика 27. Једноставан <i>SSL</i> протокол.	- 37 -
Слика 28. <i>SSL</i> протокол.	- 37 -
Слика 29. Пример хеш функције над различитим текстом.	- 39 -
Слика 30. Елиптична крива.	- 40 -
Слика 31. <i>Fiat-Shamir</i> протокол.	- 42 -
Слика 32. <i>Fiat-Shamir</i> протокол када је $e = 1$	- 42 -
Слика 33. <i>Fiat-Shamir</i> протокол када је $e = 0$	- 43 -
Слика 34. Шифрован глас се шаље изборном серверу, сервер генерише сесијски код “44570” који враћа корисничкој апликацији.	- 44 -
Слика 35. Случајан број “9821490817408174” и сесијски код “44570” су преко изборне апликације приказани у облику QR кода, који се може прочитати помоћу мобилног уређаја. Идеја овога је да гласач може помоћу кода односно хеш вредности поруке утврди интегритет гласа.	- 44 -

Слика 36. Изборна апликација шаље сесијски код “44570” изборном серверу. Сервер идентификује гласача, и враћа дигитално потписан глас и листу гласача на корисников рачунар или мобилни уређај, како би изборна апликација могла да провери интегритет гласа.	- 45 -
Слика 37. Генеричка шема.....	- 47 -
Слика 38. Резултат на предложеној шеми је 3, што значи да су сва три гласача гласала „за”.....	- 49 -
Слика 39. Резултат на предложеној шеми је 2, што значи да су два гласача гласала „за” и један „против”.....	- 49 -
Слика 40. Резултат на предложеној шеми је 0, што значи да су сва три гласача гласала „против”.....	- 50 -
Слика 41. Листа кандидата, гласача и забележених гласова.....	- 53 -
Слика 42. Представљене вредности шифрованих гласова.	- 54 -

1 Увод

1.1 Предмет истраживања

Право на бирање представника је основни концепт демократије, то је политички систем у коме један народ својом слободном вољом бира свог вођу. Постоје два основна типа гласања: јавно и тајно. Метод који ће бити разматран је метод који обезбеђује тајно гласање и уједно дизајн и имплементација овог метода биће анализирани и разматрани у овом раду. Тајно гласање је облик гласања у коме избор гласача остаје поверљив. Главна сврха овог метода је да избор гласача буде аутентичан, односно да се онемогуће спољни утицаји као што су застрашивање и подмићивање. Најједноставнији облик тајног гласања се састоји у томе да гласач свој глас напише на комаду папира који потом убацује у кутију, из које се касније пребројавају гласови.

Један од циљева е-управе је дизајнирање система Интернет гласања, првенствено да буде безбедан, што је и један од најзахтевнијих задатака. Услов безбедности овог система рашчланићемо на више комплементарних сервиса преко којих је могуће задовољити све критеријуме и тако дизајнирати један безбедан систем за ову намену.

Организовање и спровођење Интернет гласања је један веома одговоран задатак. Потребно је истовремено обезбедити употребљив и веома безбедан сервис аутентификације, интегритета и непорецивости. Интернет гласање има добру основу и шансу да уђе у неку озбиљнију употребу у Србији, јер би било изграђено на стандардним безбедносним протоколима који се већ широко користе у разним гранама трансакција на Интернету, банкарства и осталих врста продаја. Гласање преко Интернета има низ могућности од којих су, гласање са удаљених локација, већа излазност млађе генерације, особа са посебним потребама и смањење трошкова саме организације. Неки од главних циљева овог протокола јесте да се спроведе гласање на такав начин да се заштити гласачева приватност, омогући корисницима да провере свој глас и да се на безбедан начин обави бројање гласова. У изборној процедури сваки гласач се може сматрати као потенцијални злонамерни учесник, у тој мери безбедносни протоколи морају бити отпорни према великом броју злонамерних актера, који имају за циљ разне врсте превара, првенствено вишеструко гласање, утицај на гласача, мењање и куповину гласова.

Е-управа је термин који се односи на употребу информационих и комуникационих технологија у размени информација, пружању сервиса и пословању државних органа и институција са физичким и правним лицима, као и међу гранама саме управе. Увођење е-управе има за циљ смањење административних трошкова, већу брзину, ефикасност и доступност јавних сервиса, као и побољшан квалитет рада који се односи на аутоматизацију и оптимизацију сервиса чији су корисници физичка или правна лица [10].

Део рада ће се бавити и условима у земљи Србији, који се односе на стање компјутерске писмености становништва и другим ограничавајућим факторима примене овог сервиса. Према најновијим истраживањима [13], компјутерска писменост за 2011. Годину, на основу урађеног пописа становништва износи 48,99%, а од те суме је 14,78% делимично компјутерски писмено. Према том резултату

можемо да закључимо да постоје проблеми и на овом пољу (више од 50% људи у Србији није компјутерски писмено), и поред проблема који се односе на саму технологију која треба да обезбеди један такав сервис.

1.2 Структура рада

У овом раду размотрићемо предности и недостатке система за гласање преко Интернета, са освртом на безбедносне слабости. На бази истраживања теоријских основа биће представљени протоколи који су важни и неопходни како би дизајнирали почетни модел система за гласање преко Интернета.

Рад је подељен у 5 целина:

1. Увод
2. Преглед у области истраживања
3. Теоријске основе истраживања
4. Преглед предложеног решења
5. Закључак

У првом делу рада је дат је увод у проблематику и доприносе које добијамо имплементацијом гласања преко Интернета.

У другом делу приказани су класични системи за гласање који сви заједно чине основу модерних система, представљена је кратка историја гласања у циљу лакшег разумевања система за доношење одлука и упознавања са основним безбедносним проблемима. Такође, представљен је дизајн два веома успешна система Интернет гласања, чије су основе веома битне за наш рад.

У трећем делу на основу истраживања постојећих радова на ову тему, представљене су теоријске основе које су нам неопходне како би реализовали основни дизајн система за гласање преко Интернета.

У четвртом делу представљена је генеричка шема нашег система, опис и поставка окружења у којем смо приказали основни модел за гласање. У Cryptool-у предложили смо једноставну демонстрацију за гласање, помоћу *Paillier* алгоритма за генерисање кључева, шифровање и дешифровање. Такође, на крају је ради бољег разумевања алгоритма детаљно објашњен *Paillier* протокол који смо користили за демонстрацију.

На крају, у последњем поглављу дат је закључак са свим оствареним претходно постављеним циљевима као и предлогом за будући рад.

2 Преглед у области истраживања

2.1 Систем за гласање и доношење одлука

Механичке а касније електронске машине за гласање уведене су да би се смањили трошкови и време. Електронско гласање се односи на било који вид гласања који користи електронска средства у том систему. Користећи се овом дефиницијом већина гласачких система у свету припадају електронском систему гласања. Електронско гласање омогућава бржи приказ коначног збира гласова, бржи изборни процес, мање трошкове и грешке. Људи праве грешке, правилно имплементирани системи, не! [11].

У овој области представимо постојеће електронске системе за гласање и њихов настанак. Ово укључује технологије папирних система где се електронска средства користе за бројање гласачких листића, неке од поменутих технологија су старије, а неке су још у фази развоја.

2.1.1 Кратка историја гласања

Реч *ballot* односно гласачки листић, потиче од италијанске речи *ballota* што значи лопта, у старом Риму много раних гласачких листића су представљале лоптице.



Слика 1. Римски новчић из 63. године п.н.е. на којем је представљен гласач који убацује свој глас у гласачку кутију¹.

¹ <http://math.arizona.edu/~voting-theory/longinus.html>

Док су се у античкој Грчкој за овај процес користиле плочице од метала, или лоптице које су даване сваком гласачу (Слика 2), који их је потом убацивао у одговарајући земљани лонац односно гласачку кутију (Слика 3).



Слика 2. Куглица и плочице од бронзе коришћене за различите врсте гласања у старој Грчкој².



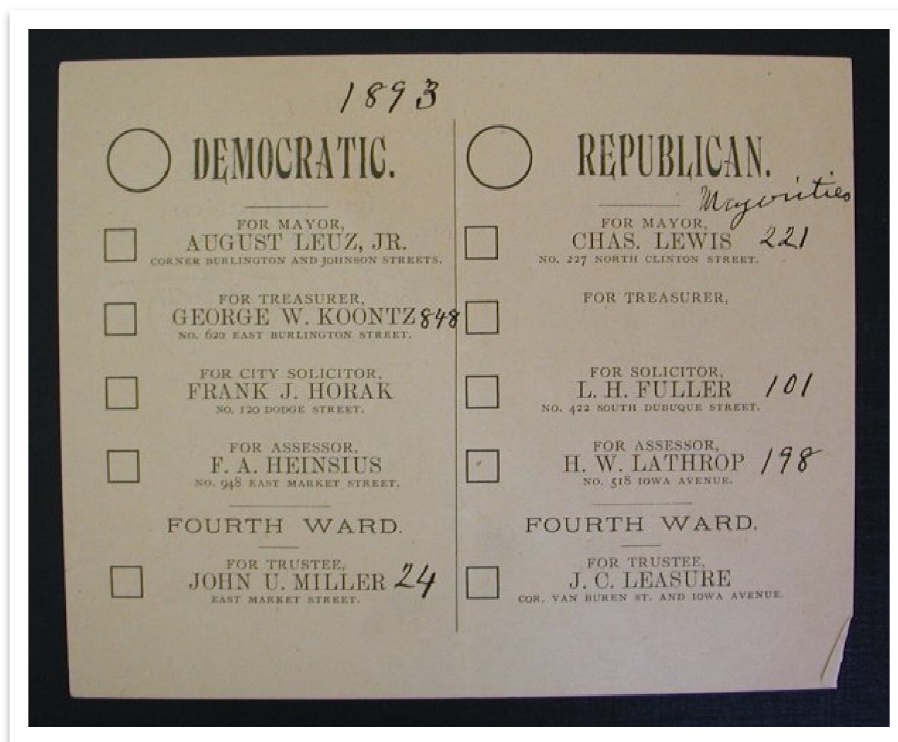
Слика 3. Употребљене гласачке кутије³.

Избори и изборни процес се одвија од настанка људске цивилизације. Када се помене гласање углавном се мисли на гласање преко папира. Први облик папирног гласачког листића употребљен у Риму 139. године пре нове ере. Овај рани гласачки листић нуди скромну приватност гласача и лака је мета за разне облике изборних превара.

² <http://www.pinterest.com/pin/27654985185261906/>.

³ http://en.wikipedia.org/wiki/File:0_-_Sto%C3%A0_of_Attalus_Museum_-_Ostraka_for_ostracism_-_Photo_by_Giovanni_Dall'Orto,_Nov_9_2009.jpg.

Модеран систем гласања користећи стандардизоване гласачке листиће први пут је реализован у Аустралији 1858. године [15]. Велика Аустралијска иновација била је, да се штампају стандардизовани гласачки листићи о државном трошку, и буду испоручени гласачима на гласачким местима. На крају гласања је захтевано да се гласачки листић врати. Правилно имплементиран, овај гласачки листић (Слика 4.) је поставио веома висок стандард, осигуравајући гласачеву приватност, спречавајући гласаче да открију како су гласали и уверавајући их у тачно и непристрасно бројање.

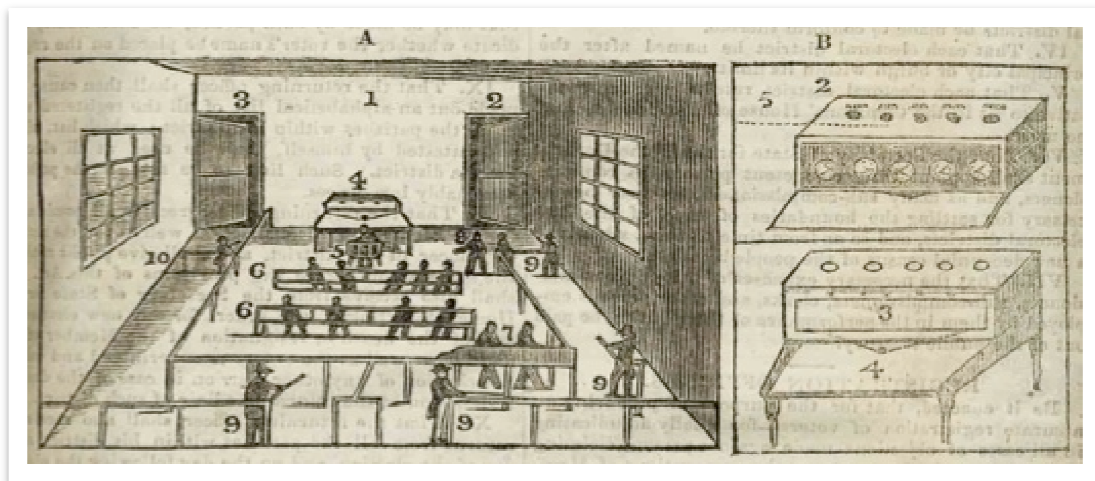


Слика 4. Пример гласачког листића коришћен на општинским изборима у Ајови 1893. године⁴.

Први велики предлог за коришћење машина за гласање долази од Чариста⁵ 1838. године. Они су захтевали да међу радикалним реформама буде и тајно гласање. То је захтевало велике промене у дотадашњем изборном процесу. Чаристи као одговорни реформатори не само да су затражили реформу већ су и описали како постићи задате захтеве, распоред на слици 5 представља: људе који воде изборе А (лева страна), распоред Б (десна страна) представља машину која треба да се користи.

⁴ <http://homepage.cs.uiowa.edu/~jones/voting/pictures/>.

⁵ Чаристи или чартизам су представљали радници и занатлије који су се удружили као покрет Енглеске радне класе која је захтевала масовне изборне реформе.



Слика 5. Нацрт система за гласање који је предложен од стране Чариста⁶.

За дизајнирање ове машине за гласање је заслужан *Benjamin Jolly*. Машина је одговарала захтевима Британских парламентарних избора. Сваки гласач је имао могућност да убади само једну месингану лоптицу у одговарајућу рупу на врху машине по имену кандидата. Лоптица је померала бројач за један и враћала се назад надлежнима који су ту исту лоптицу давали следећем гласачу.

Henry Spratt је 1875. године добио патент за машину која је представљала гласачки листић као низ тастера, за сваког кандидата је постојао посебан тастер. Његова машина је дозвољавала само један глас за сваког гласача.

Anthony Beranek је 1881. године патентирао своју машину која је имала један ред тастера за сваког кандидата а други ред за сваку партију и браве иза сваког реда ради спречавања гласање више пута. Механизам на вратима би поништавао механизам за следећег гласача.

Прва успешна механичка машина за гласање била је *Myers* кабина са полугом (Слика 6) која је први пут употребљена 1892. године у Њујорку, ова машина је дизајнирана да механички штити бирача од преваре, омогући приватност и направи бројање гласа чисто и сигурно. До 1930. године у суштини све више урбаних центара нације су усвојили овај начин гласања, 1944. године корпорација за оглашавање објавила је, да је те године 12 милиона гласача употребило ову машину, најчешће у местима где је до тада било највише изборних крађа.

Почетком 20. века користећи много покретних делова ова машина је представљала огромни помак у технологији, била је толико напредна као бушене картице 60тих и *DRE* машине 90тих. Метод је био такав да гласач уђе у кабину, за сваког изборног кандидата је постојала посебна полука, једну од којих је гласач повлачио и тиме бележио свој глас.

⁶ <http://homepage.cs.uiowa.edu/~jones/voting/pictures/>.



Слика 6. Машина за гласање која користи полугу за одабир кандидата⁷.

Постојао је механизам који није омогућавао да се полуга повуче више пута. Механизам за бројање је бележио глас за сваког кандидата. Први проблем је био поверење надлежних органа који одржавају и проверавају машину. Други проблем се јављао у механизму када је после броја 99 долазило до заглављивања или бележења вишеструког гласа.

2.1.2 Интернет гласање

“Они који гласају не одлучују ништа, они који броје гласове одлучују све” - *Joseph Stalin*.

Како је технологија напредовала у последњих неколико година, повећање и напредак електронских система се такође појавио. Овај вид гласања је једна од технологија која је још у фази развоја и има велики значај за будућност наше државе. Имплементација електронског гласања је термин који обухвата увођење посебног електронског система за бележење и бројање гласова. Са растом информационих технологија, гласање преко Интернета има добар основ и велике шансе да буде имплементиран као стандардан систем е-управе, јер би био изграђен на постојећим системима и безбедносним протоколима који се већ успешно користе. Постоји много безбедносних претњи и проблема који се односе на нападе преко мреже: преваре, корумпираност и слично. Због тога овај систем да би правилно и безбедно радио, захтева имплементацију постојећих криптографских протокола, који би обезбедили сигуран пренос кроз мрежу и правилно бројање гласова. Неке од традиционалних ствари које систем мора да поседује су: аутентификација, тајност, непорецивост, транспарентност и безбедност.

Када се мисли на гласање преко Интернета, подразумева се гласање са удаљених локација, што значи да корисник може са било које локације да гласа, све што му је потребно је неки вид идентификације и рачунар са стабилном Интернет конекцијом да би обавио гласање. Једноставна идеја је: да се гласач са својим дигиталним

⁷ <http://uspolitics.about.com/od/elections/ig/History-of-Voting-Systems/Mechanical-Count--Lever-Pull.htm>.

потписом односно посебним *PIN* кодом на смарт картици идентификује, и након тога добије приступ гласачком систему и обави гласање, гласачки листић се шифрује и преноси путем Интернета до сервера на коме се складиште и пребројавају гласови.

Омогућити људима да гласају од својих домова је велики корак напред, особе са посебним потребама би имали више могућности да гласају, они који су на путовањима, војници, студенти у страним државама и сл. Излазност би била већа, млађа генерација би била подстакнута да више учествује у стварању своје будућности, такође би свима пружили лакши начин гласања. Гласање преко Интернета се све више развија и напредује, овакви системи успешно функционишу у неким државама. Две државе чији системи имају добре основе за наш рад и имају веома успешан систем Интернет гласања, које ћемо у овом раду истражити су Естонија и Швајцарска.

Гласање преко Интернета има и својих лоших страна, уколико се изузме безбедност, дешавају се прекиди у вези, закрчења саобраћаја и сл. Електронски систем гласања би требало да има алтернативу у начину комуникације. Систем мора бити отпоран на нестанке електричне енергије. Гласање помоћу традиционалних гласачких листића у Србији је широко прихваћено и представља стандардан начин гласања, али и тај систем има својих мана, грешке су више него могуће ако се пребројавање врши ручно. Такође морамо да верујемо да сви који броје гласове и проверавају бројање истих нису корумпирани. Идеја Интернет гласања настоји да елиминира ове ствари, и створи аутоматски систем бројања гласова, који би био изграђен на криптолошким протоколима који би спречили различите врсте превара.

Основне особине система Интернет гласања су: безбедност, тајност и провера заједно са доступношћу и приступачношћу. Имплементација овог система подразумева увођење различитих механизма верификације, где гласач нема потребе да верује, изборним званичницима па чак ни компонентама система. Изборни модел треба да садржи: изборно подешавање, снимање гласова (са могућношћу провере), бројање гласова, проверу изборног интегритета.

- Квалификација и аутентификација - само регистровани гласачи са правом гласа имају право да гласају.
- Јединственост - квалификовани гласачи могу само једном да гласају, односно да имају само један важећи глас.
- Прецизност - да гласови буду правилно снимљени, у тој форми да обезбеде анонимност, а у исто време да могу да се преброје.
- Интегритет - гласови не могу обрисани и измењени.
- Верификација и одговорност - систем мора да има могућност провере односно да ли је глас правилно пребројан и записан.
- Поузданост - систем мора да ради без компромитовања гласова иако систем откаже.
- Тајност - глас може бити тајан али гласач не сме да поседује било какав доказ како је гласао.
- Флексибилност - систем мора да буде прилагодљив свим типовима гласача.
- Исправност - систем мора бити тестиран од стране изборних званичника, пре сваког изборног процеса.
- Транспарентност - гласачи морају да разумеју како систем ради, што доприноси стицању поверења друштва.

- Цена – почетна цена имплементације система је сигурно велика, док у неком даљем раду и до 85% уштеде по појединачном гласу.

Постоји доста истраживања на пољу развоја и имплементације система Интернет гласања, али само неколико држава је имало могућност и услове да развије овај систем и успешно га користи. Интернет гласање је критикована и веома комплексна тема и јасно је да постоје различити проблеми. Могућност гласања путем Интернета је пожељна функција у свакој држави, али са коришћењем такође долазе нови безбедносни проблеми. Потреба за побољшањем безбедносних механизма довела је развијања E2E гласачких система (приказан у области 3.4).

2.2 Преглед електронских система за гласање

Електронском систему гласања припадају: бушене картице, оптички скенери, ДРЕ гласачки системи, системи за електронско бројање гласова и остали. У електронском гласању базираном на папиру користе се екрани осетљиви на додир, који након што гласач забележи свој глас штампају гласачки листић који се убацује у гласачку кутију. Гласачки листићи се након тога броје помоћу оптичких скенера. Предност овог система је што увек постоји физички доказ гласачког листића. Ипак и тада може доћи до грешке у каснијем бројању гласова као и преносу до оптичких скенера уколико се налазе на централној локацији.

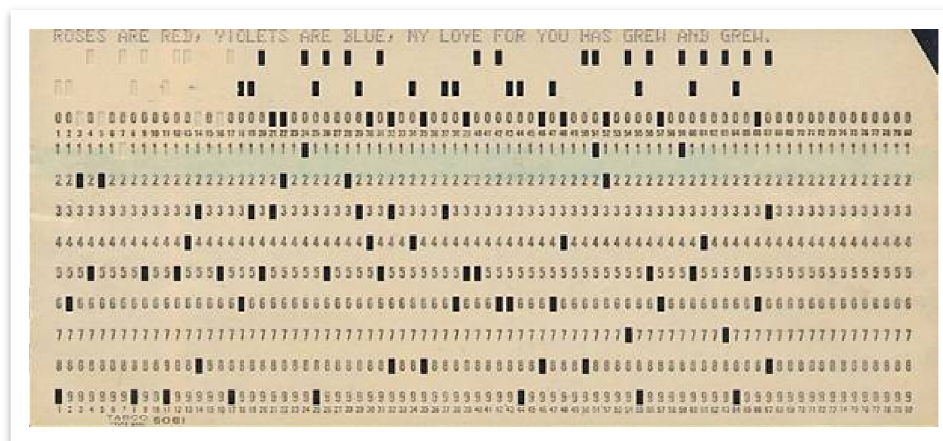
2.2.1 Бушене картице за гласање

Бушене картице представљају технологију која се користи од 19. века у различите сврхе. Овај тип бушених картица и табеларни приказ изумео је статистичар по имену *Herman Hollerith*.

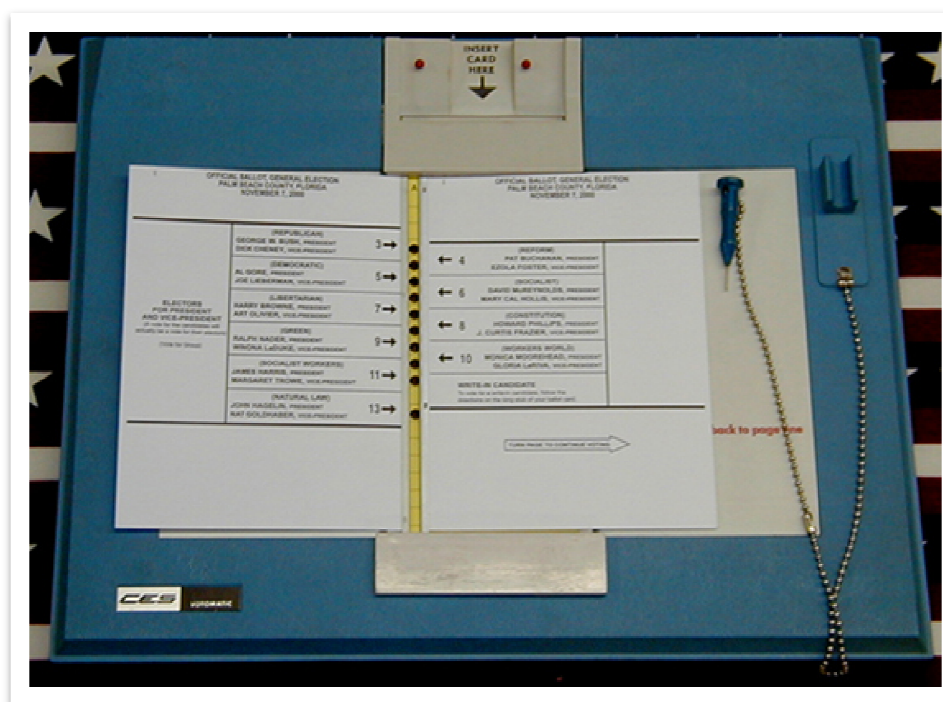
Бушена картица је комад крутог папира који се састоји од низа колона и редова који се према одређеном шаблону буше. Команде или информација на њима представљају присуство или одсуство рупа на дефинисаним позицијама. Бушене картице у 20. веку коришћене су у прерађивачкој индустрији, на системима за унос, обраду, складиштење података и сл. Рани рачунари су користили овај систем за унос података и програма.

Herman Hollerith, инспирисан картом за воз, развио је бушене картице које је 1889. године патентирао као медијум помоћу кога се могу снимати и читати подаци. Бушене картице су први пут коришћене за табеларни приказ Балтиморског одбора за здравство, касније за попис грађана 1890. године. Картице које су тада коришћене имале су округле рупице са 12 редова и 24 колоне. Такође је развио и уређај односно тастатуру са којом се картице буше, овим је елиминисано појединачно штампање сваке картице, идеја је била да се на уређају за бушење налази шаблон према коме се буши картица. *Herman* је 1896. године основао *Tabulating Machine Company* која је била једна од 4 компаније које су се спојиле у *Computing Tabulating Recording Company (CTR)*, које су касније постале познате као *IBM*.

IBM је производио и продавао низ машина за креирање, сортирање и снимање података. *IBM*-ов концепт дизајниран 1928. године имао је 80 колона са 12 места за бушење на свакој картици.

Слика 7. Један од првих типова бушених картица⁸.

Први велики напредак бушене картице су имале ране 1960. године, када је *Joseph P. Harris* заједно са *Wiliam Rouverol*-ом направио неколико побољшања *IBM*-ог система *Port-A-Punch*. Нови систем је патентиран и формиран је *Harris Votomatic inc*. После многобројних тестирања бушене картице су у сврху гласања први пут коришћене у Фултон и Декалб окрузима у Џорџији 1964. године. Због добрих резултата у новембру исте године коришћене су на председничким изборима у неколико округа у Калифорнији, где су резултати били одлични, због чега 1965. године *IBM* одлучује да купи компанију *Votomatic*.

Слика 8. *Votomatic* уређај за бушење гласачких картица⁹.

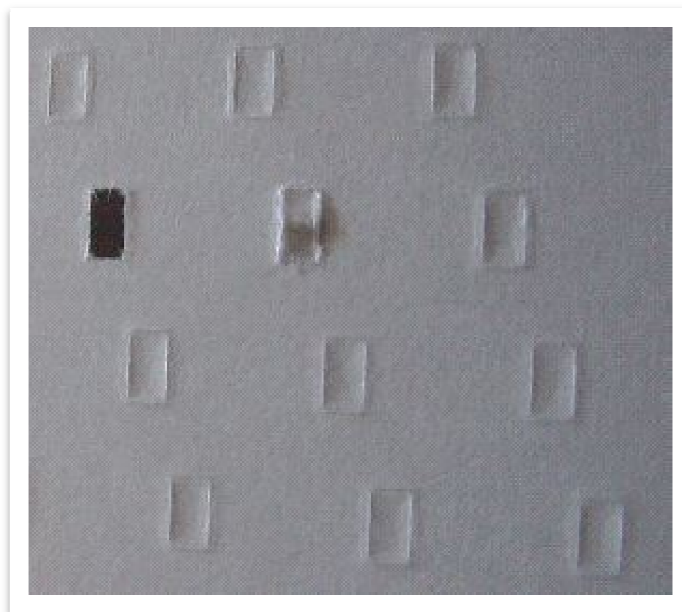
Систем ради тако што гласачи буше рупе на картици која се убацује у машину за бушење (Слика 8) на којој се налази одређени шаблон са изборним кандидатима. За

⁸ <http://wvegter.hivemind.net/abacus/CyberHeroes/Hollerith.htm>.

⁹ <http://www.sciencecases.org/election/official.asp>.

потребе гласања бушене картице су коришћене за бележење гласова и потом су убациване у машину или рачунар како би се гласови сортирали и пребројавали.

Проблеми са овим система били су познати од самог почетка, у зависности од материјала коју су били коришћени, дешавало се да рупа не буде лепо пробушена или рупа до ње буде делимично пробушена што се може тумачити као неважећи или глас за неког другог кандидата.



Слика 9. Проблем који се понекад јављао, делимично или случајно избушена рупа¹⁰.

Постоје више ових система неки од значајних су: *Votomatic* и *Datavote*.

Votomatic листић је у зависности од дизајна садржао од 228 до 235 распореда гласачких места, сама бушена картица нема информацију о именима кандидата и текста гласачких питања, та информација се налази на машини која утискује рупице по задатом шаблону. *Votomatic* систем је био веома успешан, до 1996 године овај систем је користило 37.3% америчких грађана.

Постоји још један успешан систем поред *Votomatic* система, који се у неким случајевима показао поузданијим, то је *Datavote* систем. Принцип овог система је исти само што за разлику од претходника, картице морају да се посебно штампају за сваке изборе са именима кандидата поред сваке позиције за бушење, где се између сваког имена оставља 2-3 празна места.

На председничким изборима у Америци овај систем у једном тренутку је стекао лошу репутацију, јер се сумња да је због техничке грешке на неким местима дошло до погрешног исхода гласања.

После ових проблема 2008. године убрзо већина округа на Флориди прешли су на систем гласања који користи папирне листиће који се броје помоћу оптичких скенера.

¹⁰ <http://homepage.cs.uiowa.edu/~jones/voting/pictures/>.

2.2.2 Оптички скенери за гласање

Оптички скенер за гласање представља електронски систем, који служи за читање означених места на гласачком листићу, најчешће квадрат, круг и слично приказано на Слици 10. Оптички скенери су првенствено развијени 1950-тих за школску употребу ради полагање тестова. Овај систем за снимање гласова није ушао у неку практичнију употребу све до 1960-тих када је развијен систем *Norden Electronic Vote Tallying System*. Систем је захтевао посебно мастило за препознавање ознака на гласачком листићу. *Votronic* 1965. године је развио први систем који је могао да препозна ознаке класичне графитне оловке.

OFFICIAL BALLOT
Random County, Somestate

INSTRUCTIONS: To vote for a candidate, make an X in the oval beside the name of the candidate you prefer.

PRESIDENT (vote for one) ☐ G. Washington ☐ A. Lincoln ☐ _____ (write in)	U.S. CONGRESS (vote for one) ☐ S. Rayburn ☐ J.G. Cannon ☐ N. Longworth ☐ _____ (write in)
---	---

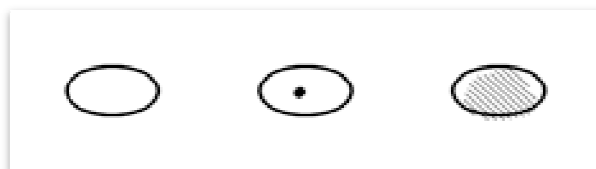
Слика 10. Тип гласачког листића коришћеног за оптички скенер¹¹.

Начин снимања је такав да постоји сензор за сваку колону, сензор снима све ознаке у боји или тамније области од постојећих. *Avante Vote-Tracker* бележи број тамних и светлих пиксела у свакој колони и на тај начин препознаје ознаке. Коришћење дигиталне фото технологије омогућило је мало напреднији приступ снимању, неки софистициранији алгоритми за препознавање имају могућност да препознају облик ручно забележене ознаке. Модернији дигитални системи за снимање гласова користе дигитални папир који препознаје мала камера која се налази на оловци. Листић може бити одмах проверен да би се утврдило да ли је важећи, да нема грешке као што су приказане на следећим сликама:



Слика 11. Важеће ознаке које се броје.

¹¹ <http://homepage.cs.uiowa.edu/~jones/voting/optical/>.



Слика 12. Важеће које се не броје.



Слика 13. Не важеће ознаке.



Слика 14. Ознаке које се не могу прочитати из првог пута.

Један могући напад на овај систем према *Douglas W. Jones*-у је да ако нападач дође у контакт са рачунаром или фајловима гласачког система, он би могао да припоји гласове једног кандидата другоме. *Douglas* је нашао те фајлове на једном рачунарском систему који је требао да буде коришћен за изборе. Ове фајлове је неко пребацио неким преносним медијумом. Ко год да је имао приступ овим фајловима је потенцијални нападач на систем. Други вид преваре је да ко год поседује гласачки листић пре избора има могућност да дели већ означене листиће, ово може да буде решено штампањем случајно генерисаних листића или таквог броја на листићу. Предности ових машина је да корисник не мора да учи како се машина користи, корисник може једноставно да употреби оловку да обележи своју изборну вољу. У случају да се скенер поквари гласач и даље може да попуни свој гласачки листић и скенира га на другом месту.

Софтвер може бити пројектован да дозволи само један глас по кандидату, препозна вишеструко гласање и да могућност одбацивања листића.

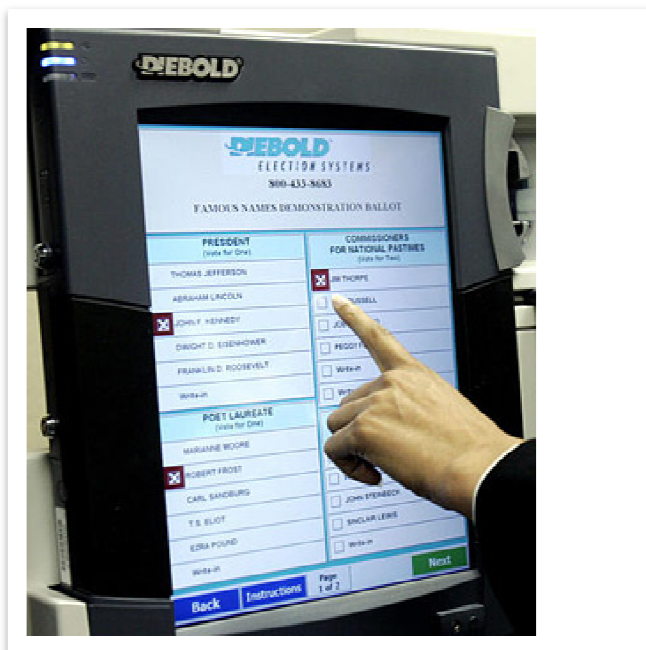
Неке предности коришћењем овог система су да означени листић јасно показује гласачеву вољу, нема проблема као што су били случај бушеним картицама.

2.2.3 DRE (Direct recording electronic system)

Direct recording electronic system је систем гласања у којем се користе електронски уређаји. Уведен је 1975. године, овај метод гласања се и даље користи на изборима у неким земљама [15]. То је концепт гласања који је заснован на систему гласања помоћу полуге, где бирачи гласају повлачењем полуге. Овај систем не користи гласачке листиће, сви кандидати и могућности гласачу су приказане на екрану осетљивом на додир или преко одређеног распореда тастера у зависности од модела уређаја. Забележени гласови се чувају на меморији уређаја и преносе се до централизоване станице у којој се броји. Глас се може пребацивати и пребројити у

тренутку гласања или на крају изборног процеса где се добија табеларни приказ снимљених гласова. Иако се глас може пребацити преко јавне мреже, ово се једино ради у случају убрзаног бројања.

Предност овог система је брзина којом се резултати избора могу знати, јер се резултати могу добити тренутно. У овом систему се такође умањује механичка грешка. Пошто се гласање одвија преко рачунара, кориснички интерфејс се може прилагодити потребама гласача. Ради веће безбедности могу се користити смарт картице. По завршетку гласања добија се папир односно извештај о успешно обављеном гласању.



Слика 15. *Dre (Direct recording electronic system)*¹².

Овај систем омогућава владама и организацијама да уштеде новац, јер се ангажује мање људи за надгледање, не штампају се гласачки листићи, а систем се уз мало промена може опет користити. Постоје и *DRE* системи који користе јавну мрежу за пренос електронских гласова са гласачког места на неку локацију путем јавне мреже, гласови се могу преносити појединачно, у повременим серијама или на крају цела серија одједном где се пребацују на централно место на којем се касније пребројавају [21].

2.2.3.1 Бразил

Електронско гласање у Бразилу је представљено 1996. године када су први тестови спроведени у Санта Катарини. Већ 2000. године сви системи за гласање у Бразилу су електронски. Од тада се користи више од 400.000 гласачких машина широм земље и резултати су спремни у неколико минута по затварању гласачких места. 2010. године

¹² <http://www.voterescue.org/NatNewsArticles/HR811.htm>

за председничке изборе на које је изашло 135 милиона грађана, резултат је био спреман за само 75 минута од завршетка гласања.

Бразил ће наставити да користи и развија овај систем гласања који је већ широко користи и у суседним земљама као сто су: Ел Салвадор, Еквадор, Колумбија, Панамама и Перу који полако усвајају овај веома успешан систем и раде на пилот пројектима заснованим на његовим побољшањима. У последњих неколико година земља полако развија биометријску гласачку кутију, која омогућава и гарантује идентитет гласача и елиминише грешке и преваре [20].

2.2.3.2 Белгија

Електронско гласање у Белгији је почело 1991. године и широко се користи за председничке и општинске изборе, 1999. године је уведен систем који је базиран на два система познатим као *Jites* и *Digivote*. Оба ова система су окарактерисана као индиректно евидентирање електронских система за гласање, јер машина не снима директно глас и уписује га у табелу, него уместо тога оба система врше запис на магнетним тракама.

Данас се користи систем *Smartmatic*, који ради на истом принципу као претходни систем само уместо магнетних трака гласач добија папир или извештај са QR кодом (приказан на слици 16.) који уместо убацивања у гласачку кутију се скенира и глас је тако забележен. Гласање у Белгији је обавезно за све грађане који су навршили 18 година. Постоје одређени пенали за оне који не излазе на гласање, што чини Белгију као једна од држава на чије изборе излази скоро 90% регистрованих корисника.



Слика 16. Извештај у облику QR кода који се добија после одабира кандидата¹³.

¹³ <http://elections.smartmatic.com/belgians-prepare-to-vote-for-three-elections-on-the-same-day>.

2.3 Преглед система у е-управи

Као и сваки аспект ИТ домена е-управа има своје предности и недостатке. Првобитна намера је позитивна и многи грађани су овај начин пословања е-управе оберучке прихватили, јер наручивање докумената и обављање одређених послова преко Интернета значи да без чекања у реду грађани могу да добију тражена документа, а да при том не изгубе читав дан на шалтерима. Осим уштеде времена, ово за грађане значи и уштеду новца, транспарентност и праведност функционисања јавне администрације и побољшање квалитета услуга. Са друге стране, за запослене увођење е-управе подразумева једноставнији и ефикаснији начин рада, док за привреду смањење трошкова комуникације и трансакција, и коначно за саму државну управу елиминисање корупције и злоупотребе у процесу јавних набавки. Неки од проблема који се јављају при увођењу е-управе су: у многим институцијама руководство не зна и не прихвата предности коришћења информационо комуникационих технологија, непостојање свести руководећег кадра о потенцијалном доприносу ИТ-а, многе општине и немају ИТ одељења, најчешће уколико постоји једна особа у ИТ сектору, она се бави одржавањем система.

Највећи проблеми са којима се грађани срећу при обављању неких административних послова су: гужве на шалтерима, долажење више пута ради обављања истог посла, посећивање више различитих објеката, обимни обрасци и формулари, нељубазност особља, радно време шалтера, неорганизованост, високи административни трошкови и остало [22]. Имплементацијом е-управе могу да се реше претходно наведени проблеми, чиме се омогућава ефикаснији сервис према становништву, једноставније обављање послова уз добру организацију, смањење административних трошкова, мање папирологије, као и лакша комуникација путем Интернета, мобилних телефона и слично. Такође, е-управа омогућава сузбијање корупције и ефикаснији однос са привредним субјектима.

2.3.1 Појам е-управе

Појам е-управе се односи на начин организовања јавног менаџмента у циљу повећања ефикасности, интензивним и стратешким коришћењем информационих и комуникационих технологија. Опште значење појма е-управе је доступност сервиса и услуга државних служби електронским путем. Оно што се код овог система подразумева је доступност клијентима 24 часа дневно, за разлику од класичног приступа где доступност зависи од гужве и радног времена шалтера. Данас је то највећим делом преко Интернета, мада постоје и други начини као што су путем телефона односно *Call* центра, факса и слично. Е-управу представљају онлајн сервиси, који су доступни преко владиних веб страница и најзаступљенији су на нивоу општина и градова. Е-управа је окренута и намењена пре свега грађанима, али и пословним субјектима и организацијама. Уместо одласка у владине одсеке и канцеларије ради попуњавања пријава, регистрације или овере неких формулара, сви послови могу да се обаве путем Интернета и попуњавањем формулара на службеној веб страници.

Један од најважнијих принципа у е-управи су поверење и приватност. Да би е-управа успешно функционисала мора да постоји поверење код грађана, приватност је такође веома важна и она подразумева тајност свих података, почев од личних до

пословних трансакција, па до неких владиних информација. Поред предности увођења базе података, отварају се могућности за кршење права на приватност и злоупотребе личних података. Ово може подразумевати надгледање и праћење понашања појединца, трговину или размену база са личним подацима, крађу идентитета, као и многе друге облике злоупотребе. Како би се то спречило разумљиво је да овај систем подразумева и специфичне мере заштите података, како би смањили могућност губитка информација или њихово неовлашћено мењање. Како у модерном друштву постоје озбиљне претње за приватност, потребно је да Република Србија обезбеди адекватне правне услове за развој и деловање националних капацитета за заштиту личних података. Употреба електронског потписа само је једно од начина утврђивања аутентичности. Ово је технологија е-пословања која служи као заштита интегритета преноса података и која потврђује непорецивост електронских порука. Електронски потпис има особину да штити интегритет електронски потписаних порука, што није могуће традиционалним потписом [14].

2.3.2 Основни системи е-управе

- *G2G – Government to Government*
- *G2B – Government to Business*
- *G2E – Government to Employee*
- *G2C – Government to Citizen*

G2G (Government to Government) је сервис који представља сарадњу између владиних служби. Омогућава унапређење сарадње органа различитих нивоа државне управе и стварање пуног партнерства између њих, у сврху бољег пружања сервиса грађанима и другим објектима. Овај систем укључује дељење података електронским путем између запослених у влади на националном и локалном нивоу.

Постоје две врсте: хоризонтални и вертикални *G2G*.

Хоризонтални *G2G* се односи на сарадњу и комуникацију структура власти на истом нивоу, на пример између општина.

Вертикални *G2G* представља комуникацију између хијерархијски различитих структура власти на пример између општинске и републичке владе[9].

G2E (Government to Employee) је сервис сарадње владе и запослених у владиним службама. Заснован на концепту Интранета и односи се на електронско управљање документацијом. Запослени су у могућности да ефикасније размењују информације, односно да имају бољу комуникацију и користе информациони систем. Ово омогућава лакши проток информација и података унутар владе, односно већу ефикасност рада.

G2B (Government to Business) је сервис за комуникацију јавне управе са пословним субјектима заснован на концепту Интернета и Екстранета. Основне компоненте су снабдевање, информације и сервиси. Представља однос између владе и привреде. Ово је потенцијално најперспективнији сегмент е-управе, првенствено због жеље и притиска пословног сектора за побољшање брзине обављања услуга и могућег смањења трошкова.

G2C (Government to Citizen) представља сарадњу владиних служби и грађана, односно комуникацију јавне управе са грађанима заснован на концепту Интернета. Овај део е-управе је најмасовнији и основне компоненте су посетиоци, информације, онлајн сервиси и дигитална демократија. Поменути сервиси подразумевају омогућавање трансакција као што су подношење захтева, обнове дозвола, плаћање пореза, издавање докумената (држављанства, извода из матичне књиге и слично). Већина влада данас у свету дистрибуирају информације путем интернета, изграђују своје дигиталне базе података и пружају одређени вид услуга онлајн путем.

2.4 Истакнути системи за Интернет гласање у неким земљама ЕУ

2.4.1 Швајцарска

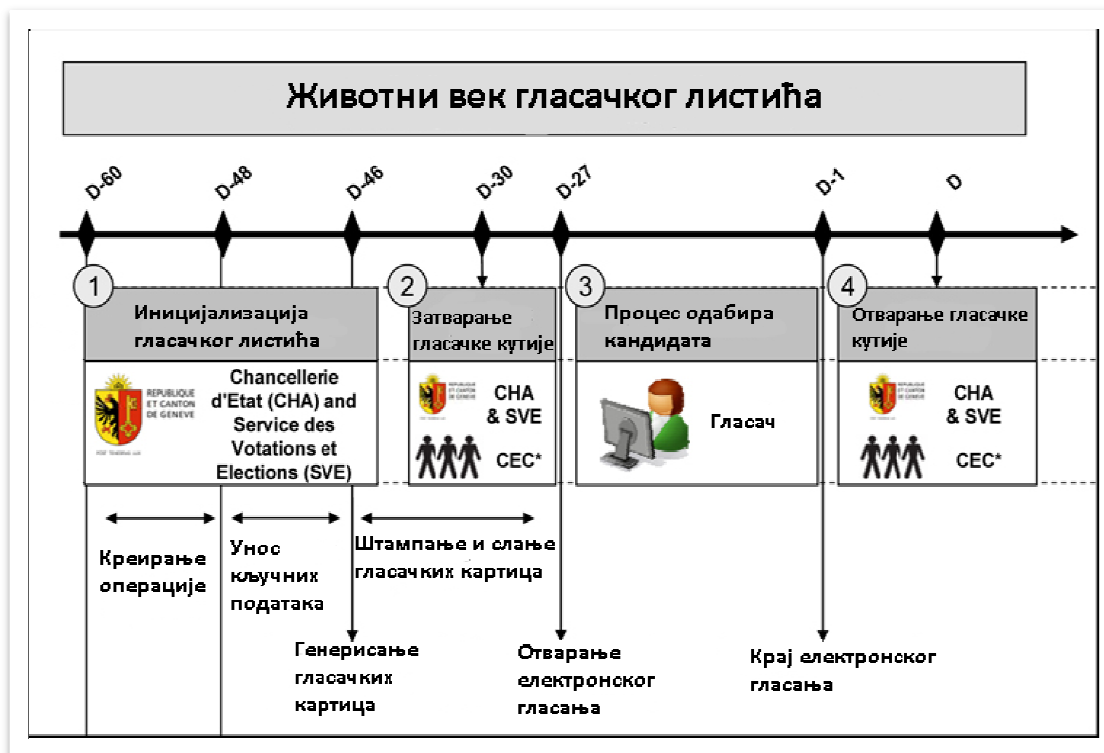
Швајцарски полу директни демократски систем омогућава грађанима да учествују у доношењу било ког закона предложеног од стране власти, односно предложеног од стране грађана уколико се за то прикупи довољан број потписа. Као резултат тога Швајцарци у просеку од 4 до 6 пута годишње излазе на гласање да прихвате или одбију одлуке своје владе, што значи да је добар гласачки систем неопходан за демократска права грађана у Швајцарској.

Central Electoral Commission (CEC) је централна изборна комисија која је оформљена 1. Јануара 2010. године, у исто време кад је представљен систем електронског гласања у Женевском кантону, док је први глас у тој области забележен 2003. године. Према закону *CEC* има приступ свим операцијама у изборном процесу, могућност провере одређених информација у било ком тренутку независно од изборних операција. Закон такође прописује да се систем Интернет гласања провери сваке три године и резултати тих истраживања буду јавно објављени. Прва провера система извршена је 2012. године.

Затварање гласачке кутије се врши за време састанка званичника *CEC*-а који припремају односно генеришу низ криптографских кључева. После овог стадијума криптографски механизми су постављени тако да обезбеде непробојност гласачке кутије, што значи да нико нема приступ гласовима пре бројања. Гласачка кутија је безбедна када се гласови не могу записати или прочитати а да систем то не примети. Приватни кључ познат је само систему и он је једини који може да запише гласове у гласачку кутију, валидан глас је само онај који се може дешифровати приватним кључем. Једном када је гласачка кутија запечаћена, сајт преко кога се врши гласање може бити отворен за коришћење.

Када гласач приступи сајту, пример: <http://www.geneve.ch/evoting/english/welcome.asp> користећи свој претраживач он остварује безбедну комуникацију. Да би приступио гласању корисник:

- На страници за идентификацију уписује број гласачке картице и остале личне податке.
- Прихватају се услови коришћења.
- Попуњава се гласачки листић.
- Проверавају се унети подаци и глас се шаље.



Слика 17. Животни век гласачког листића [7].

Пар питања која долазе у обзир, како бити сигуран да се приступа правом сајту, како је гласач идентификован и како избећи манипулације и малициозне гласове.

Када корисников претраживач оствари контакт са сајтом за гласање, *HTTPS* протокол генерише сигурну заједничку *SSL* комуникацију између њих.

Како би систем био што безбеднији и напади били што тежи, у систем је имплементиран концепт сигурног канала између претраживача и сервера. Овај канал је базиран на комбинацији више безбедносних метода: класични *SSL* протокол, заједнички *SSL* протокол и *Surencryption*.

Најједноставнији вид *SSL* протокола јесте аутентификација у једном смеру тј. сервер представља свој сертификат клијенту како би он могао да га аутентификује.

Заједнички *SSL* проток представља аутентификацију у оба смера, ово обезбеђује да клијент и сервер буду сигурни да комуницирају један с другим. Једном када је ова веза остварена, заједнички *SSL* протокол обезбеђује први ниво енкрипције и заштите за сав саобраћај што се оствари, што значи да је кориснику загарантовано да има приступ правом сајту за гласање и све следеће информације између њих ће бити шифроване.

Surencryption се састоји од шифровања података на нивоу апликације пре слања кроз заједнички *SSL* канал. Шифровање је базирано на симетричним кључевима, чији тајни кључ потиче од *UVN* броја, који је употребљен за добијање хеш вредности односно отиска који се користи за слање. Подаци се шифрују два пута на различите начине што ојачава јачину шифровања. По добијању шифроване поруке и отиска, систем користи јавни кључ за дешифровање отиска, потом систем рачуна отисак поруке, ако се добијени поклапа са оригиналним отиском, порука се дешифрује приватним кључем, и глас се записује.

Тренутни веб претраживачи немају функцију потребну за имплементацију сигурног канала какав је представљен овде, због чега систем захтева коришћење *Java* технологије, која ће радити са корисниковим претраживачем. У пракси корисник скида *Java* апликацију са официјалног сајта за гласање, где се идентификује гласач, док апликација обезбеђује сигурну конекцију.

Идентификација гласача

За сваки избор, гласачи путем поште добијају гласачку картицу. Посебно за сваког гласача постоји јединствени број са гласачке картице *UVN*, омогућавајући да се на систему изврши идентификација. Како овај број не би запао у погрешне руке, број се никада не шаље, уместо њега шаље се отисак тог броја, што представља дељену тајну између гласача и система. Отисак је хеш вредност *UVN* броја што значи да је веома тешко скоро немогуће доћи до оригиналног броја у оквиру задатог времена [7].

2.4.2 Естонија

Пилот пројекат започет 2002. године је био завршен и први пут тестиран 2005. године за локалне изборе савета, када је више од 9 хиљада људи свој глас забележило преко Интернета, то је први вид коришћења гласања путем Интернета у Естонији. Захваљујући томе у Естонији 2007. године је први пут у свету коришћено гласање преко Интернета за парламентарне изборе. Од тада овај систем се успешно користи. До данас је употребљен 5 пута на парламентарним изборима, 2007, Јун 2009, Октобар 2009, 2011 и 2013. године.

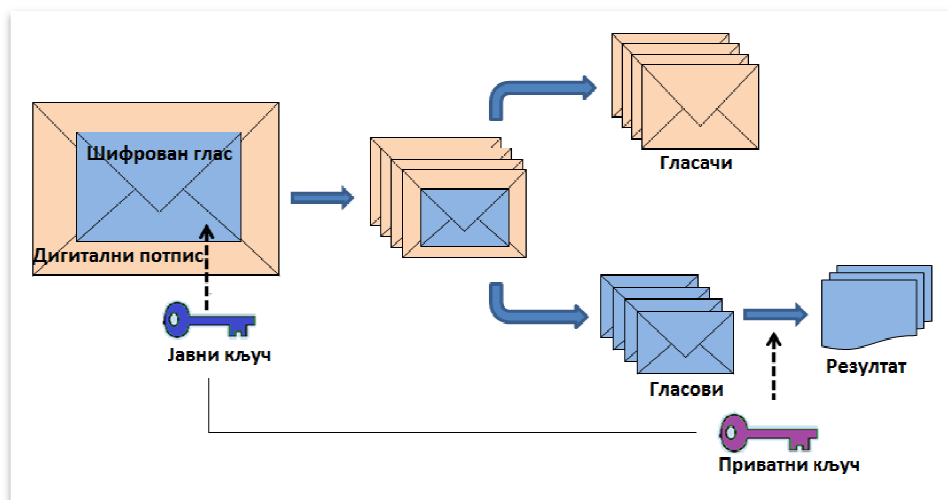
Груби концепт овог система је да се:

- Гласач идентификује неким документом (слика 18).
- Гласач добија гласачки листић и две коверте.
- Гласач испуњава свој листић и ставља је у прву коверту на којој нема било какве информације о гласачу.
- Након тога прва коверта се ставља у другу на којој има информација о гласачу.
- По доласку коверти на бирачко место и утврђеног права на гласање, на основу информације на спољној коверти, она се отвара и прва коверта односно унутрашња се ставља у гласачку кутију.

Овај систем обезбеђује да гласачев избор остане тајан а у исто време да се забележи да је он гласао. Гласање преко интернета у Естонији ради на том концепту, систем се може представити као систем са две коверте. Апликација коју корисник добија на свом рачунару, по завршетку гласања шифрује глас, што представља прву неозначену коверту, након тога гласач даје свој дигитални потпис, чиме обезбеђује информацију о себи док глас остаје тајан. Пре пребројавања сертификационо тело уклања дигитални потпис, личне податке и анонимно дешифрује унутрашњу коверту односно глас. Метод користи криптографску шему са јавним и приватним кључевима, где национални комитет за гласање поседује приватни кључ. Аутентификација гласача се врши личном картом.

Слика 18. Естонска лична карта¹⁴.

Сваки гласач мора да поседује своју идентификациону картицу са својим јединственим *PIN* кодом. То је уствари смарт картица која садржи микро чип који рачунар може да препозна, што значи да не служи само као документ, већ представља и дигитални идентитет. Све што је потребно гласачу да би обавио гласање је: лична карта, читач, рачунар и стабилна Интернет конекција.



Слика 19. Систем преношења гласа у Естонији [8].

Овај начин гласања у Естонији је могућ само 7 дана унапред у току изборног процеса, да би се обезбедило време како би се елиминисали дупли гласови до краја избора. Како би обезбедили да гласач изрази своју праву вољу, у случају ако се гласач предомисли, постоји могућност да се глас промени електронски или да се на гласачком месту физички забележи глас за време трајања избора. Пример, ако гласач оде на гласачко место и гласа, тиме се поништавају сви претходни електронски гласови, и тај последњи глас се уважава. Ако се деси да гласач гласа електронски и физички, та информација се прослеђује електронском одбору за гласање, и његов електронски глас се поништава. После овога његов глас је коначан. Верификација електронских система у Естонији ће бити могућа тек од 2015. године због даљег развоја система.

¹⁴ <http://ec.europa.eu/idabc/en/document/4487/5584.html>.

Верификацијом електронских система омогућава да се добије тачнија информација о рачунару који је коришћен за гласање. Верификацијом се детектује неки малициозни програм на том рачунару и помоћу тога онемогући гласање.

Висок степен компјутерске писмености, модерна инфраструктура комбинована са е-управом омогућавају Интернет гласање у Естонији могућим и широко прихваћеним.

3 Теоријске основе истраживања

3.1 Mixnet

Mixnet је систем базиран на шифровању са јавним кључевима. Ово је систем који је дизајниран с намером да комуникацију чини тешком за праћење, односно користи ланац сервера који мешају поруке од различитих пошалајоца и шаљу их на следећу дестинацију. Сврха мешања порука је да прекине везу улаза и излаза у циљу постизања анонимности. Овај начин мешања порука чини овај систем компликованијим за прислушкивање и праћење такозване *end-to-end* комуникације.

David Chaum је 1981. године представио „*Mixnet*” као алат који осигурава анонимност, користећи вишеслојно *RSA* шифровање (енгл. *RSA onions*¹⁵), у комбинацији са низом случајних битова. *Mixnet* систем који је базиран на овом концепту шифровања и једном слоју дешифровања на сваком серверу се зове *Chaumian mixnets*.

Идеја је следећа: скупљају се гласови од гласача, шаљу се на први део односно на случајну пермутацију *A*, где се гласови насумично изокрећу или мешају, и врши се шифровање, потом се садржај шаље на пермутацију *B*, која такође меша гласове и шифрује својим кључем, и на крају се (у случају да има три сервера) шаље у *C* која ради исто то. Неколико различитих сервера за мешање доприноси стицању поверења.

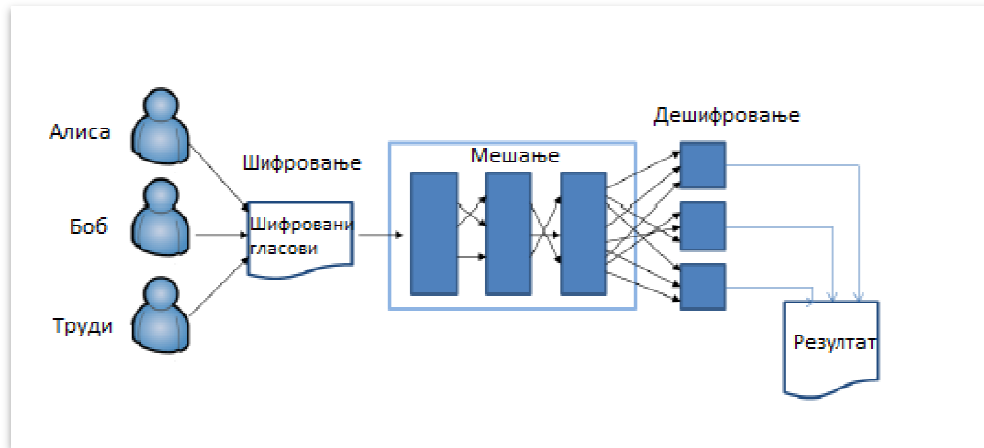
Један једноставан начин за шифровање је: $Eka(Ekb(Ekc(m)))$, јер морамо да дешифрујемо исправним редом.

Mixnets се састоји од низа секвенци $M_0, M_1, M_2, \dots, M_n$ који представљају сервере за мешање, сваки сервер генерише свој пар јавних и приватних кључева (pk, sk), и објављује свој јавни кључ pk . Кроз ове сервере шаље се неки текст m који представља изабраног кандидата. Сваки глас ће бити шифрован са јавним кључевима сваког сервера по задатом реду. $Epk_0(Epk_1(Epk_n(m)))$. Ово значи да први сервер M_0 дешифрује сав унет текст, меша резултат и шаље даље. Онда M_1 ради исто то са примљеним резултатом и тако за сваки следећи корак до последњег M_n . Циљ овог мешања је да излаз не може да се повеже са улазом, за систем Интернет гласања то је веома битно, како би се постигла гласачева анонимност. С обзиром да ће текст остати оригиналан, у шеми мешања постоји шанса да се дође до оригиналног пошалајоца. Да би систем радио без могућности да се дође до њега, ре-енкрипција је потребна.

Ре-енкрипција је друга форма овог система. Ово је систем у коме нема дешифровања у корацима, дешифровање се ради само у финалном кораку, што значи да се глас шаље и уместо да сваки сервер дешифрује вредности, сервери поново шифрују шифроване вредност.

¹⁵ Поруке се више пута шифрују и шаљу се кроз неколико мрежних чворова, како сваки рутер уклања слој енкрипције, тако се добијају инструкције за сваки следећи корак и на које се место шаљу.

За гласачеву верификацију у гласачком протоколу *Chaum* предлаже варијанту овог канала за гласачки протокол, у сврху да помогне гласачима да провере свој глас да је коректно забележен. Протокол захтева два круга кроз сервер за мешање. У првом кругу Алиса шаље свој јавни кључ pk за који поседује приватни кључ sk . Затим она проверава да ли је њен јавни кључ дошао до краја. У другом кругу Алиса шаље $(pk, Esk(m))$.



Слика 20. Систем мешања гласова (*Mixnets*) [11].

Алиса шаље поруку m Бобу, тако што шифрује Бобовим јавним кључем kb , пре слања она додаје његову адресу B и случајну вредност R поруци, шифрује јавним кључем сервера km $I = km(R1, Kb(R0, m)B)$ где је R_1 и R_0 случајни низ бита. Сервер затим дешифрује информацију својим приватним кључем, одбацује низ бита, где остаје $X = kb(R0, m)B$ и ову компоненту може да проследи Бобу коју он дешифрује такође својим приватним кључем.

R_0 је случајна вредност која спречава нападача да нагађа поруке, пошто се претпоставља да нападач може посматрати сав долазећи и одлазећи саобраћај, ако се случајна вредност не користи: шаље се $(kb(m)B)$ тако да нападач има добре шансе да погоди поруку m' , тако што може да тестира $kb(m') = kb(m)$ да ли се подударају, из које може да сазна садржај поруке. Додавањем случајне вредности R_0 нападач је онемогућен да обавља своју врсту напада, односно нападач може да тестира $m = m'$ али неће бити сигуран да ли је то тачно јер не зна случајну вредност R_0 .

Додатак томе Алиса добија потписану признаницу када шаље поруке серверу, она тако може да пружи значајне доказе ако сервер за мешање на излазу не добије исправну вредност. Тада Алиса може пружи:

$$Y = (ka - 1(C, ka(R1, kb(R0, m)B)))$$

где је $ka = 1$ приватни кључ Алисе, а C велика константа и представља опозив потписане поруке, она исто може да пружи вредности које на излазу недостају.

$$K = (kb(R0, m)B)$$

пошто се сваки пут шаље цела шифрована целина, ако X недостаје, оно се може извући из копије те целине.

Повратни саобраћај односно одговор са дестинације је могућ без жртвовања анонимности, све поруке које се враћају деле исту безбедност и перформансе као долазне поруке у другом смеру. За потребе Интернет гласања повратни систем није потребан.

У случају да је потребан повратни саобраћај, он се заснива на следећем концепту: Алиса ствара адресу којој се не може ући у траг $km(S_1, A)$ где је S_1 кључ који делује и као случајна вредност за потребу шифровања, kx је јавни кључ за једну употребу, Боб шаље $km(S_1, A)$, $kx(S_0, одговор)$ у сервер, на излазу се добија вредност A , $S_1(kx(S_0, одговор))$, само Алиса може да дешифрује резултат јер је она генерисала S_1 и kx – осигурава да се садржај поруке не може видети.

У сврху Интернет гласања круцијално је да се измене послатих вредност примете како би се елиминисале манипулације, ово може да се назове и верификација гласова.

Прве доказиве мреже за мешање (енгл. *Mixnet*) се зову *Sako-Kilian Mixnet*. У овом систему поруке се могу измешати пре дешифровања. Систем ради тако што узима вредности са улаза, дешифрује их користећи кључеве, затим сервер врши мешање на случајан начин. Да би постојала провера мешања сервер генерише додатни доказ *shadow mix*, који на неки начин представља отисак пермутације која је коришћена у сврху провере, сервер може да пружи доказ или да покаже разлику између два мешања¹⁶. Ако је сервер “искрен” одговориће на оба изазова, а ако није може да одговори на бар један изазов што значи да ће у 50% случајева погрешити.

3.2 Хомоморфна енкрипција

Хомоморфна енкрипција омогућава све потребне особине које су потребне за Интернет гласање.

Идеја која стоји иза овог система је довољно једноставна. Са стандардним шемама за шифровање, шифровани подаци морају прво да се дешифрују како би могли да се обраде. Хомоморфна енкрипција омогућава различите операције над шифрованим подацима, односно омогућава рад са шифрованим подацима а да пре тога нема потребе за дешифровањем. У преводу могуће је узети два дела шифрата и урадити одређену операцију над њима, и њихов резултат на крају дешифровати.

Пример функција шифровања који поседује мултипликативну хомоморфност је *El-Gamal*. Ако се шифрат поруке m_1 и шифрат поруке m_2 помноже, резултат је шифрат читаве поруке m .

$$E(m_1) * E(m_2) = E(m_1 * m_2)$$

Два примера хомоморфних крипто система су *RSA* и *El-Gamal*.

У *RSA* систему после шифровања отвореног текста P у шифрат C , можемо помножити C са 2 и онда дешифровати $2C$ и тако добити $2P$. Ово не би било могуће у неком симетричном систему, на пример ако би у *AES* шифрату помножили са 2 и онда дешифровали, као резултат би добили неку случајну вредност уместо P .

¹⁶ Разлика између два мешања значи да ако се понови мешање, постојеће излазе доказа ће трансформисати у првобитне излазе.

El-Gamal је криптолошки систем базиран на дискретним алгоритмима који је добио име по свом проналазачу *Taher El Gamal*-у. Ово је одличан систем јавних кључева који се користи за дигиталне потписе и је базиран на *Diffie-Hellman* протоколу. У случају *El-Gamal* протокола можемо узети шифрате гласова и на крају добити резултат.

Систем ради тако што:

- Боб генерише прост број P и број G који представља вредност између 1 и $(p - 1)$.
- Генерише се случајна вредност x која представља његов приватни кључ.
- Боб рачуна y , $y = g^x \bmod P$.
- Кључ који Боб шаље Алиси је p , g и y .
- Након свега овога Алиса по добијању вредности, узима вредности које је добила и поруку коју хоће да пошаље, генерише своју случајну вредност k .
- Рачуна своју вредност $a = g^k \bmod P$.
- Након тога израчунава $b = y^k \bmod P$.
- a и b као шифроване вредности шаље Бобу.
- Шифрат C представљају параметри (a, b) , а то значи $(g^k, M y^k) = C$

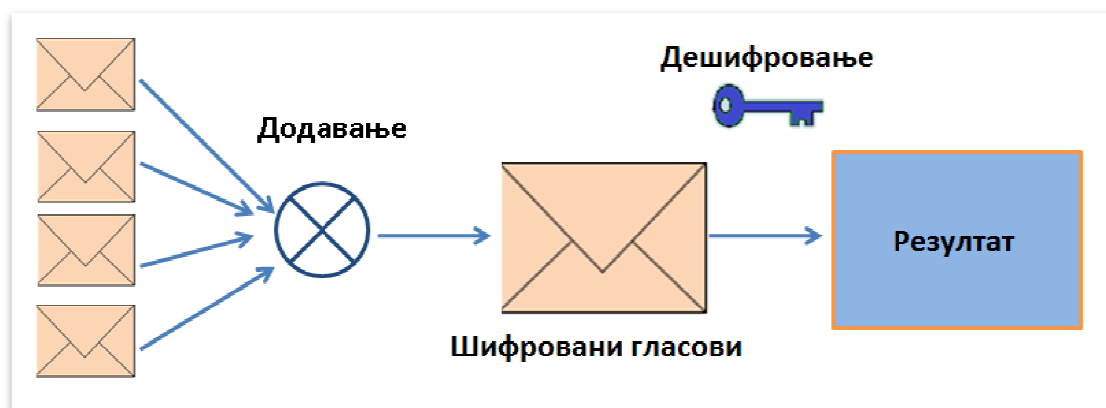
Дешифровање:

$$C = M y^k / (g^k)^x = M y^k / (g^x)^k = M y^k / y^k = M$$

Користећи x можемо извршити факторизацију другог дела шифрата и доћи до поруке.

У криптографском протоколу Интернет гласања, идентитет гласача може да се користи за шифровање, тако да гласач има могућност да провери тачност свог записаног гласа. У случају спајања гласова, оригиналан глас неће бити доступан као у случају кад се гласови шифрују одвојено, у гласачком систему множење гласова онемогућава проверу њиховог интегритета, решење би био неки протокол који сабира гласове и на крају приказује укупан збира гласова.

Главна предност хомоморфног сабирања гласова је у томе да није потребно дешифровање појединачних гласова, већ се приватни кључ користи само једном за дешифровање коначног збира за сваки изборни процес. На овај начин све време се чува тајност појединачних гласова. Пример протокола хомоморфног сабирања представљен је у области 4.3.



Слика 21. Хомоморфно додавање гласова [11].

Сваки од ових примера дозвољава операције над текстом само на један начин (или сабирање или множење). Криптолошки систем који у исто време подржава обе операције је познат као потпуна хомоморфна енкрипција. Постојање ефикасне и потпуне хомоморфности има велике практичне имплементације на пример у *cloud computing*-у.

3.3 Дељење тајни (Secret sharing)

Тајно дељење представља криптографски алгоритам који је креирао *Adi Shamir* 1979. године. То је форма дељења неке тајне на делове, и давање одређеним странама део те тајне, где су неки делови или сви потребни како би се дошло до тајне. Дељење информација на делове представља идеалну шему за складиштење података који су веома осетљиви и битни. Шема се подразумева у чувању криптолошких кључева, банковних рачуна, кодова за лансирање ракета и слично. Свака од ових информација мора бити безбедно чувана, свако најмање откривање може имати лоше последице.

Проблем са складиштењем кључева је: како у исто време постићи поверљивост и поузданост. Чување више копија на различитим местима повећава поузданост али исто тако негативно утиче да поверљивост, јер постоји већа вероватноћа да ће нека копија завршити у погрешним рукама, док поверљивост добијамо када чувамо само једну копију кључа на месту са високом безбедношћу.

Пример депоновање кључева: идеја је била уколико се нешто шифрује, кључ мора да се региструје, простије речено морамо наш кључ некеме дати. Било ко са судским налогом би могао легано да дође до тог кључа и наша информација не би била више тајна. Једноставно решење за овај случај је дељење тајни, односно уместо једној агенцији, кључ поделимо на више агенција тако да ниједна агенција не може сама да дође до наше информације [1].

Дељење тајни представља безбедносни механизам који обезбеђује да кључ у исто време буде поверљив и поуздан. У овој шеми постоји особа која дели тајну и они који добијају делове те тајне и само одређен број тих повереника заједно може да дешифрује тајну. А то значи да се тајни кључ K дели на мање делове и дели повереницима n , где важи да само одређен број повереника k од могућих n , а важи ($k \leq n$), је потребан како би се тајна реконструисала. Један начин је да делиоц генерише пар кључева и подели их на делове и затим дистрибуира те делове

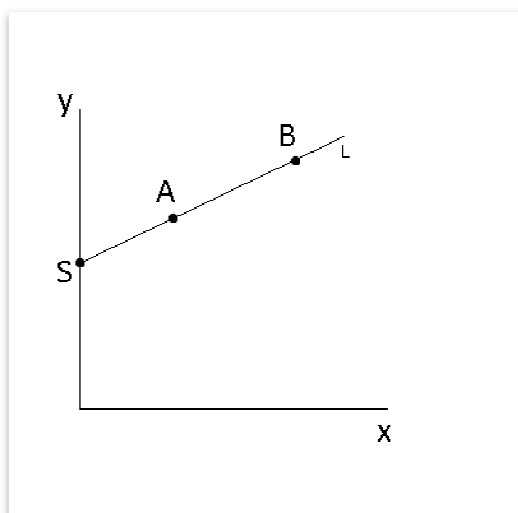
повереницима. Безбеднији приступ је имати поверенике који ће генерисати пар кључева заједно при чему ниједна страна неће знати читав K током процеса.

Пример: 11 научника ради на тајном пројекту и пожеље да закључају документ у сеф, тако да сеф може да се отвори, само ако је 6 или више научника присутно, то значи да од 11 научника који раде на проблему, најмање 6 научника је потребно да откључају сеф и разумеју тајни пројекат.

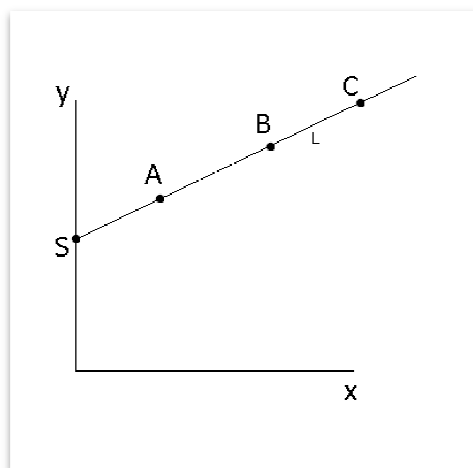
Претпоставимо да имамо тајну S и желимо да Алиса и Боб деле ту тајну тако да не могу сами да дођу до S , али док су заједно могу да дођу до S .

Mark Stamp је описао овај протокол као чињеницу да две тачке чине линију. Веома једноставан пример. Дата је тајна S и линија L , Алиси је дата тачка A , а Бобу тачка B . Нико од њих сам не може да зна тајну S али ако се удруже и споје своје знање дођи ће до тајне S .

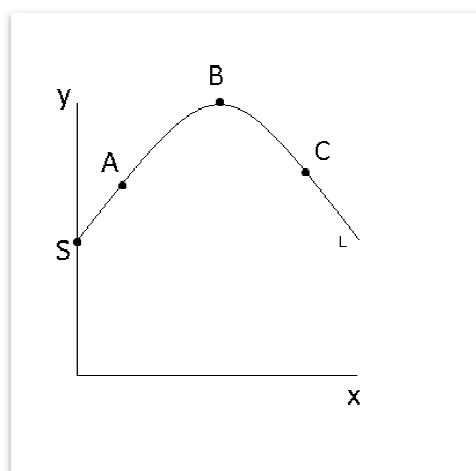
У случају дељења тајне на више делова када је $m \leq n$ где је n број корисника а m је минимални број корисника који могу да саставе тајну у приказаном случају потребно је само две тачке како би се дошло до тајне.



Слика 22. Линија чији је полином степена 1, на којој су две тачке.



Слика 23. Линија чији је полином степена 1, на којој су три тачке.



Слика 24. Линија чији је полином степена 2, на којој су три тачке.

Линија чији је полином степена 1 и одређује се са минимум две тачке, док је парабола чији је полином степена 2 одређује се са 3 тачке, у овом случају параболе, само две тачке нису довољне да би дошли до тајне *S*, што значи да је минимум 3 тачке довољно како би дошли до тајне.

3.4 End-to-end

У последњих пар година сведоци смо појаве све више оваквих система. Примарна сврха овог система настоји да побољша изборни интегритет кроз *E2E* верификацију. *E2E* систем представља комбинацију електронских и традиционалних метода гласања, како би постигао могућност верификације. Главни циљ овог система је да пружи сервис верификације а да исто време не угрози изборни интегритет.

Једноставно објашњење овог система заштите је: *E2E* систем представља метод заштите преноса неке информације кроз мрежу, тако да само почетна и крајња тачка могу да виде оригиналну поруку [12].

E2E систем је фантастичан у детектовању преваре, овакви системи могу да пруже сигурност да исход избора буде подједнако коректан као традиционалне методе гласања. *E2E* систем елиминише потребу за поверењем, односно корисник нема потребу да верује рачунару и изборним званичницима. Пре одабира кандидата, гласачки листић је шифрован. *E2E* систем даје гласачу могућност да верификује шифровање, да би верификовао да је глас снимљен као што је замишљено.

Са великим могућностима јављају се и велики проблеми, са представљањем *E2E* провере јављају се проблеми са приватношћу, комплексношћу и употребљивошћу. Систем Интернет гласања према садашњим истраживањима не може још да буде 100% отпоран на претње и принуде. На основу истраживања долазимо до закључка да ако омогућимо гласачу да верификује свој глас, онда се стварају могућности да гласач буде манипулисан на одређен начин, скоро је немогуће да систем поседује могућност провере а да буде отпоран на манипулације у исто време. Ако може да се

провери за кога је гласано, онда глас није тајан. Начин на који овај проблем може да се заобиђе је представљен у области 3.10.

Криптографски протоколи за гласање обећавају верификацију без потребе да верујемо интегритету било ког софтвера у гласачком систему. *E2E* важи за систем са јаким особинама интегритета и јаке отпорности.

Ови системи користе постојеће криптографске методе за генерисање извештаја и доказа, дајући гласачу могућност да провери свој глас, да није дошло до неких измена или мењања. Коришћењем других криптографских метода, верификација је могућа и без откривања било ког система за ког кандидата је гласано. *E2E* систем је најчешће комбинација папирног и електронског метода

Најједноставнији пример који користимо свакога дана је SSL протокол унутар веб претраживача. Пример када седимо за својим рачунаром и претражујемо своју омиљену онлајн продавницу, наш саобраћај може бити надгледан од стране треће особе, све док не кренемо да уносимо податке са своје картице где у врху странице ћемо угледати *HTTPS* у адреси или зелени квадратик. То за просечног корисника значи да је линија сигурна и лични подаци са картице су безбедни и не могу бити украдени у току преноса кроз мрежу [12].

Неко ко чита ово може сад да се запита, “Како можемо бити сигурни да хакери неће наћи неки други начин да дођу до мојих података” – Тачно. Драго ми је да размишљате тако, али *E2E* није једина солација која постоји, како се развија технологија бићемо сведоци настанка различитих решења за размену података, која за циљ имају постизање одређеног нивоа безбедности [12].

3.5 SSH

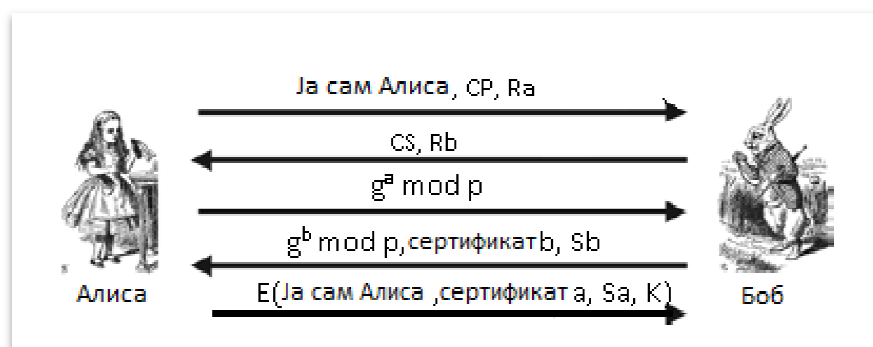
SSH је мрежни протокол који омогућава корисницима успостављање сигурног комуникационог канала између два рачунара путем несигурне рачунарске мреже. *SSH* пружа три битне особине, које отварају неке од креативних решења:

- *Secure command-shell*
- *Port forwarding*
- *Secure file transfer*

Secure command-shell се односи на то да све команде које могу да се извршавају помоћу командног прозора (енгл. *command prompt*), сада могу да се изврше са неке удаљење локације (са путовања, од куће и слично). Овај систем уствари представља даљинско управљање, односно систем или администратори могу даљински започети, видети или зауставити неки процес, креирати нове кориснике, мењати дозволе, фајлове, прегледати докуменате, приступ бази итд.

Port forwarding је моћан алат који пружа безбедан приступ *TCP/IP* апликацијама и уређајима, тако што на фајерволу отвара одређени порт. Овај термин се некад односи на тунеловање, што значи да се омогућава сигуран пренос информација које обично путују несигурним путем. После пуштања система у рад, саобраћај се преусмерава и шаље шифрованим тунелом и све апликације које се користе могу безбедно да функционишу.

Secure File Transfer (SFTP) представља под систем *SSH* протокола. У преводу то је један одвојен протокол који се бави преносом фајлова. *SFTP* има неколико предности од класичног *FTP*. *SFTP* пре слања шифрује корисничко име и лозинку, користи исти порт као *SSH* сервер, што елиминира потребу за отварањем посебног порта. Коришћење овог под-протокола се заобилази натовање¹⁷ које у класичном *FTP* систему може створити одређене грешке. *SFTP* креира безбедну линију за пренос фајлова и докумената



Слика 25. *SSH* протокол.

- *CP* – Предложени криптографски параметри.
- *CS* – Изабрани криптографски параметри.
- *Ra, Pb* – Случајно генериране вредности.
- Сертификат *a* – Алисин сертификат.
- Сертификат *b* – Бобов сертификат.
- *K* – кључ, $g^{ab} \bmod p$.

Фаза 1: Алиса шаље Бобу следеће: ја сам Алиса, предложене криптографске параметре, *Ra* изазов на основу кога аутентификује Боба.

Фаза 2: Боб шаље одабране параметре, и своју параметар изазова *Pb* (на основу кога аутентификује Алису).

Фаза 3: Алиса шаље вредност $g^a \bmod p$, односно *Diffie-Halman* протокол, (на основу кога ће Боб израчунати симетрични кључ *Kab*).

Фаза 4: Боб одговара са својом вредношћу $g^b \bmod p$ (на основу кога ће Алиса израчунати симетрични кључ *Kab*), свој сертификат *b*, и дигитално потписане све поруке *Sb* до тада послате.

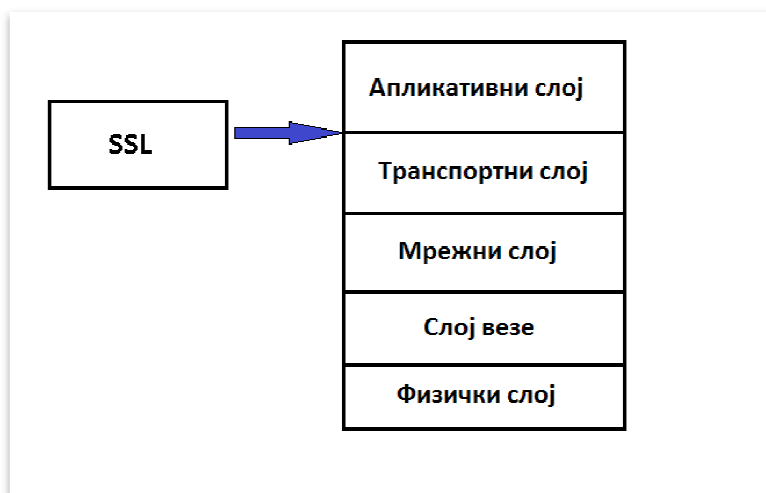
Фаза 5: Алиса шаље шифровану поруку која садржи: ја сам Алиса, свој сертификат *a*, дигитално потписане поруке *Sa*, и успостављен кључ *Kab*.

SSH и *MITM* напад неће успети из једноставног разлога. Аутентификација неће бити успешна јер све претходне поруке које су послате се неће поклапати, из разлога што Труди мора да пошаље, односно замени g^a или g^b са својим g^t , што значи да и Алиса и Боб ће приметити да је неко изменио информацију и угрозио комуникацију између њих.

¹⁷ Натовање је процес превођења IP адреса из локалне мреже у IP адресе јавне мреже.

3.6 SSL (Secure Socket Layer)

У савременом електронском пословању *SSL* протокол се користи за већину безбедних трансакција преко Интернета. *SSL* се налази између апликативног и транспортног слоја, на ОСИ моделу [2]. Имплементиран је у веб претраживач, где *HTTP* протокол представља слој апликације, а *TCP* протокол слој транспорта.



Слика 26. *SSL* протокол на ОСИ моделу.

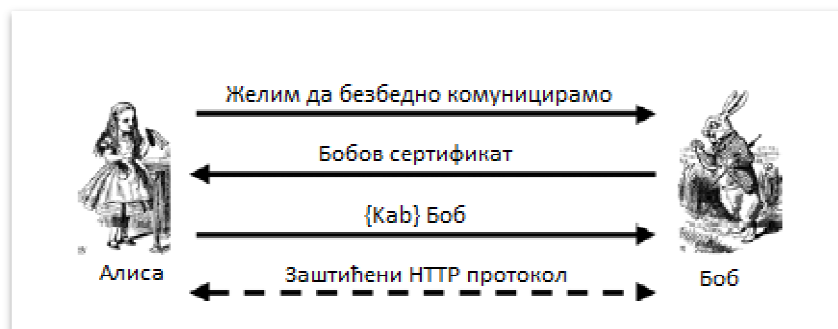
На пример ако хоћемо да обавимо неку куповину или трансакцију преко Интернета, пре него што унесемо потребне податке хоћемо да будемо сигурни да је сајт који користимо прави, када у то будемо сигурни уносимо све потребне приватне податке који су потребни. Принцип је да ми као корисник аутентификујемо сајт, док друга страна нема потребу да аутентификује нас, ово је један облик једностране аутентификације.

Задатак *SSL* протокола је да оствари заштићен пренос података кроз мрежу. *SSL* обезбеђује механизме за идентификацију сервера, идентификацију клијента и шифровану размену података између њих.

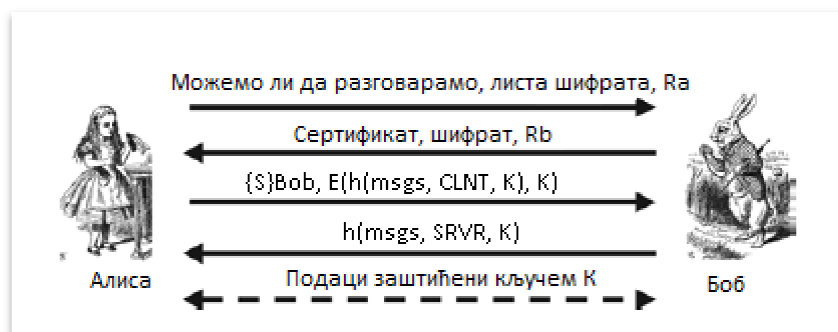
Идеја је следећа: клијент захтева безбедну везу са сервером, шаље своје криптолошке алгоритме за размену кључа и симетрични кључ.

Након успостављања безбедне *SSL* комуникације размена података између клијента и сервера може да започне.

Узећемо примере из [1] и [2] како би лакше приказали и разумели овај протокол. Пример 1: Алиса (клијент) и Боб (сервер). Алиса обавештава Боба да жели да оствари сигурну комуникацију, Боб одговара својим сертификатом, Алиса проверава потпис на сертификату. Када ће након провере Алиса бити сигурна да има Бобов сертификат, али није сигурна да комуницира са Бобом. Тада Алиса шифрује вредност Бобовим јавним кључем и шаље му кључ. Овај пример представља поједностављен *SSL* протокол. Проблем је што Боб није потпуно аутентификован и једини начин на који ће Алиса да зна да комуницира с њим је када се правилно дешифрује претходно шифрована вредност. Такође Алиса се није аутентификовала Бобу тако да ни он није сигуран с ким комуницира.



Слика 27. Једноставан SSL протокол.



Слика 28. SSL протокол.

- S – тајна пре главне вредности.
- K – је тајни кључ, $h(S, R_a, R_b)$, $h(хеш)$.
- $msgs$ – представља све претходне поруке.
- $CLNT$ – клијент константа.
- $SRVR$ – сервер константа .

Пример 2:

Фаза 1: Алиса обавештава Боба да жели да успостави SSL конекцију, и шаље листу шифрата које она подржава, и параметар изазова R_a .

Фаза 2: Боб одговара својим сертификатом, изабира један од шифрата, и шаље свој параметар R_b на основу кога жели да аутентификује Алису.

Фаза 3: Затим Алиса шаље S (тајна пре главне вредности) који је она генерисала и дигитално потписала, заједно са хеш вредношћу¹⁸ $h(msgs, CLNT, K)$ коју је шифровала својим кључем K , што не повећава сигурност, већ се и сматра да ово шифровање представља мању грешку у протоколу [1].

Фаза 4: Затим Боб одговара са својом хеш вредношћу, и тако Алиса има могућност да види све поруке које је Боб примио, и провери да су то оне које је она послала. $K = h(S, R_a, R_b)$ представља по два кључа за слање и пријем а они су: за шифровање, за

¹⁸ Хеш вредност се користи да би се проверила аутентичност порука.

заштиту интегритета и иницијализационе векторе. Различити кључеви у сваком смеру онемогућавају одређене типове напада.

У овом примеру нема узајамне аутентификације, у Примеру 2. Алиса је аутентификовала Боба, али не и обрнуто. Узајамна аутентификација је могућа ако Боб у фази два пошаље захтев за Алисин сертификат. Онда Алиса мора да поседује валидан сертификат како би наставио комуникацију, или уместо тога Боб може да затражи Алисину лозинку.

Ова ситуација се често дешава на сајтовима за куповину на пример, довољно је да знате с ким послујете и да имате новац, другу страну не занима ништа друго.

3.6.1 SSL i MITM

SSL је првенствено дизајниран да заштити MITM нападе. Да би спречили ову врсту напада, неопходно је прво да претпоставимо да сертификате издаје трећа страна од поверења. Бобов сертификат мора бити издат од треће стране која је од поверења. Труди може да пошаље Бобов сертификат Алиси, али онда Труди не може себе аутентификовати Бобу, ако Труди пошаље свој сертификат уместо Бобов, напад пропада када Алиса покуша да аутентификује сертификат, јер ће тако утврдити да то није Боб.

Пример: ако Алисин сертификат није валидан, веб претраживач ће је упозорити. Већина корисника ће занемарити ово упозорење и наставиће даље. Ако Алиса занемари упозорење, Труди ће имати отворена врата и напад ће бити успешан [1].

У реалном протоколу постоји могућност компресије, што значи да би компресијом отвореног текста пре слања добили већу тачку јединствености. Компресија заснована на ентропијском кодовању, уклонила би редувантне податке и тако појачала ентропију добијених шифрата. Увођење компресије представља скупу операцију која захтева много процесорске снаге. Недостатак компресије представља критичну безбедносну тачку у SSL протоколу. Разлог за компресију је и податак да симетрични алгоритми за шифровање, на улазу прихватају фиксне блокове отвореног текста (64, 128, 192 или 256 битова). Отворени текст се конвертује преко UTF8 стандарда. Труди би могла да са великом вероватноћом погоди до 50% битова шифроване поруке, под условом да је порука садржана од великих и малих слова [2].

3.7 Хеш

Хеш функција се користи у многим областима криптографије, постоји много типова ових функција са различитим безбедносним особинама. Хеш обично подразумева функцију компресовања, односно трансформацију неке поруке произвољне дужине у вредност фиксне дужине. Ова функција је такође веома пожељна када се ради о неком великом фајлу [17].

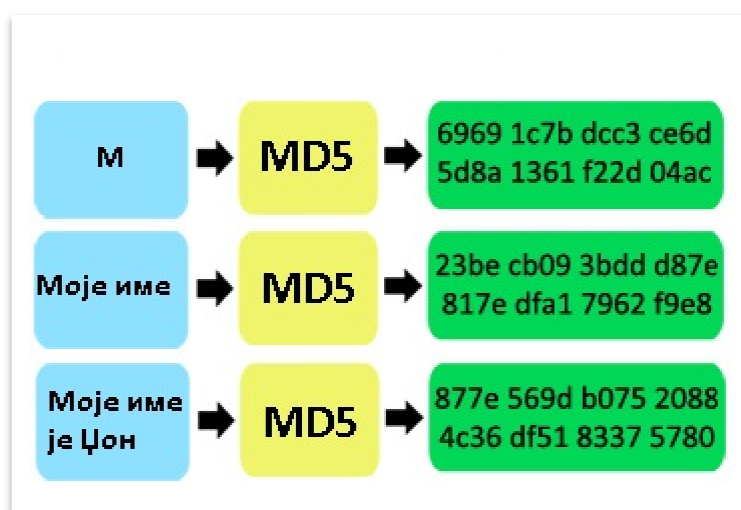
Код криптографије са јавним кључевима постоји проблем везан за веродостојност података које је на пример: Алиса послала Бобу. Наиме, користећи неки од алгоритама са јавним кључевима, шифровану поруку шаљемо Бобу, када Боб прими шифрат уз помоћ свог приватног кључа може да га дешифрује и дође до отвореног текста, али како би прималац био сигуран да је то порука баш од Алисе уводи се

појам дигиталног потписивања што условно значи шифровање поруке приватним кључем. Разлика је само што се у том случају не шифрује порука већ се шифрује отисак или хеш од послате поруке, а шифровање поруке се обавља опционо уколико је захтеван и сервис тајности [17].

Хеш функцију би могли једноставно да представимо као једносмерну функцију која обрађује неку поруку M и као резултат тога добијамо фиксну вредност $h(M)$. Хеш функција се може дефинисати као идентификатор или као људски отисак прста који је просто речено мали, а опет има моћ да идентификује људску особу. Ако Алиса потпише шифровану поруку и пошаље Бобу, он може израчунати хеш како би добио M али само ако важи $H(M) = H(M')$.

Пример: Алиса потписује поруку M својим приватним кључем и добија $S = [M]a$. Када пошаље то Бобу он може да верификује потпис тако да важи $M = \{S\}a$. У случају да је M велики податак, слање ће бити веома дуго и потребно је много ресурса да изврши операцију. Претпоставимо да Алиса користи хеш функцију у овом случају, јер тада $h(M)$ представља отисак поруке M , који је значајно мањи податак у односу на M , а опет довољан за идентификацију. Алиса може да потпише $S = [h(M)]a$ и тако пошаље Бобу M и S , онда би он верификовао да је $h(M) = \{S\}a$. Која је разлика? Овим поступком потписивања и слања $h(M)$ уместо M , стварамо већу ефикасност јер ће се операција само извршити над малим податком $h(M)$, а то значи већу брзину, коришћење мање ресурса и бољи проток. Такође значи да је ово безбедан начин провере да ли је дошло до било каквих промена у поруци.

Алиса може Бобу да пошаље поруку заједно са хеш вредношћу свих претходних порука. Боб тако једноставно има могућност да упореди са својим хешом од свих претходних порука и провери да ли се нешто променило. Проблем који се са коришћењем одређеног алгоритма јавља су колизије, што значи да постоји могућност да у две различите поруке добијемо исти хеш. Такође постоји ефекат лавине, односно ако се у хеш вредности промени и само један бит, хеш те исте поруке ће променити бар половину укупног броја бита у хеш вредности [18].



Слика 29. Пример хеш функције над различитим текстом¹⁹.

¹⁹ <http://www.gohacking.com/what-is-md5-hash/>.

Међу хеш функцијама које су нашле ширу примену издвајају се *MD5* и *SHA-1*, код којих су уочене одређене слабости. Напад на *MD5* је већ реализован у пракси и лако је изводљив и има пуно онлајн алата који могу да потпомогну нападу. Док се за *SHA-1* тврди напад могућ, што је ова функција доведена у питање, с обзиром да је заснована на истим принципима као *MD5*.

Постоји много врста хеш алгоритама *MD4*, *MD5*, *SHA-0*, *SHA-1*, *SHA-2*, *SHA-3*, *Tiger* итд.[17]

Један од напада на ове алгоритме се своди на проналажење колизије, односно проналажење неке вредности која ће имати исту вредност као и оригинална порука, ово се још назива и парадокс рођендана.

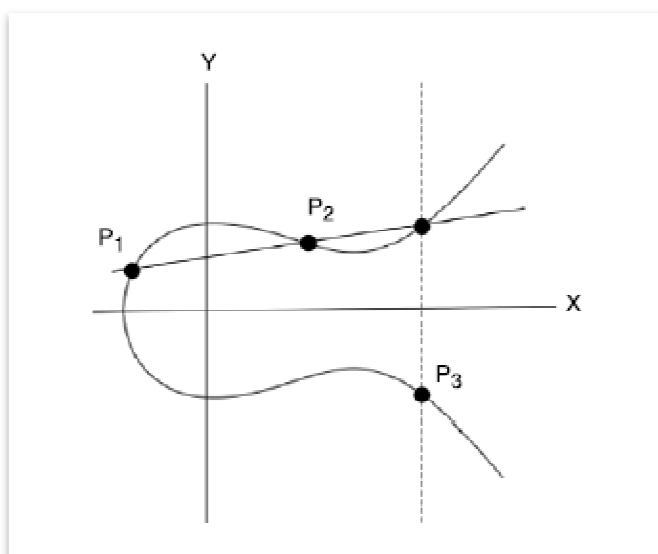
3.8 ECC (*Elliptic curve cryptography*)

Елиптичне криве не спадају под класични криптолошки систем, уместо тога овај систем само обезбеђује други начин за обављање комплексних математичких једначина које су подразумеване у криптолошким системима са јавним кључевима. Предност *ECC* је коришћење мање бита за исти ниво безбедности у случају класичних система. Лоша страна је што је *ECC* веома комплексан систем и као такав је скупљи за саму имплементацију. Зато овај систем је посебно популаран у неким системима који су ресурсима ограничени.

$$y^2 = x^3 + ax + b$$

Слика 30. приказује метод који се користи за налажење суме две тачке на криви. Како би израчунали *P1* и *P2*, повезују се линијом и обично пресеца криву у некој тачки у овом случају *P3* и важи:

$$P3 = P1 + P2$$



Слика 30. Елиптична крива.

једини додатак који је нама потребан у криптографији је $(mod\ p)$, који додајемо генеричкој једначини и важи:

$$y^2 = x^3 + C = x^3 + ax + b$$

$$y^2 = x^3 + ax + b \pmod{p}$$

ECCDH ради на принципу да Алиса и Боб генеришу пар кључева (d_a, Q_a) и (d_b, Q_b) . Од којих размењују Q_a и Q_b , тако да важи $P = daQb = dbQa$ [9].

3.9 Доказ нултог знања (Zero proof knowledge)

У криптологији овај метод подразумева, да Алиса као начин аутентификовања, може да докаже Бобу да је нека изјава истинита, без одавања било какве информације о њој, осим чињеница да је та изјава заиста истинита. Ако доказивање захтева да Алиса поседује знање неке тајне информације, Боб иако убеђен да је информација тачна он неће моћи да докаже то некоме, јер не поседује тајне информације о тој чињеници. Боб у процесу верификовања стиче знање да Алиса поседује неке тајне информације.

Помоћу низа питања и одговора, уколико је поштован протокол, на крају је Боб убеђен у нешто (са вероватноћом експоненцијално близу 1) само ако је чињеница истинита. Такође, ако је чињеница лажна, вероватноћа је иста да ће Боб открити неку ману у току разговора. У току разговора Боб ће само бити убеђен да је нека чињеница тачна, неће ништа више научити о њој [4].

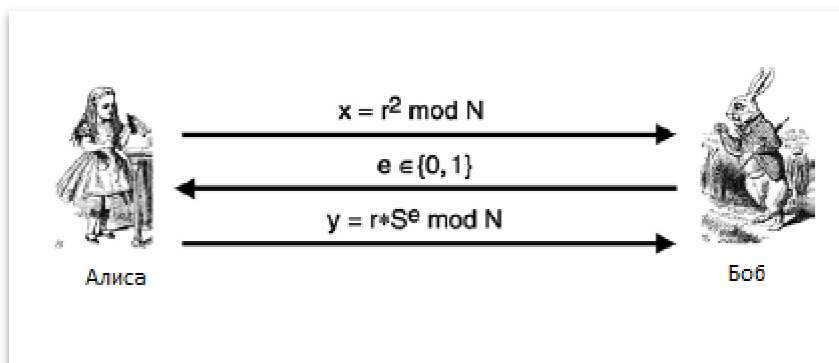
Пример 2: Пећина [1].

Претпоставимо да Алиса зна тајну реч "сезаме отвори се" који отвара пут од R до S . Да ли Алиса може да убеди Боба у то, без одавања информације о томе. Алиса улази у пећину и баца новчић да одлучи на коју ће страну отићи. Боб улази у пећину, и долази до позиције Q , такође баца новчић, претпоставимо да се Алиса налази на позицији P . Боб бира страну којом ће кренути, ако крене страном P затећи ће Алису на правом месту без обзира да ли она зна тајну или не, уколико изабере страну S , Алиса једино може прећи на страну S ако зна тајну реч која отвара врата између R и S . У случају да Алиса не зна тајну реч и жели да превари Боба, шансе су јој $\frac{1}{2}$. Ако се протокол понови n пута, онда је вероватноћа којом ће Алиса преварити Боба бити $(\frac{1}{2})^n$.

Овај пример показује да је доказ нултог знања изводљив у теорији, *Fiat-Shamir*-ов протокол, који је развијен од стране *Fiege, Fiat i Shamir*, омогућава овај протокол употребљив у пракси.

Овај систем се заснива на методу да налажења квадратног корена по модулу n и представља тежак процес факторизације. Претпоставимо да је $n = pg$, где су p и q прости бројеви, Алиса поседује неку тајну S . параметри $v = S^2 \pmod{n}$ су јавни. Алиса мора да убеди Боба да она зна S без откривања било какве информације о S .

Пример 3:



Слика 31. Fiat-Shamir протокол.

Фаза 1: Алиса генерише неку случајну вредност r и прави квадрат r^2 , (која у претходном примеру представља бацање новчића), и шаље $x = r^2 \bmod n$ Бобу.

Фаза 2: Боб генерише случајну вредност $e \in \{0, 1\}$ (која би представљала бацање новчића 0 за једну страну, 1 за другу) и шаље Алиси.

Фаза 3: Алиса одговара са $y = r * S^e \bmod n$, и Боб онда верификује да је:

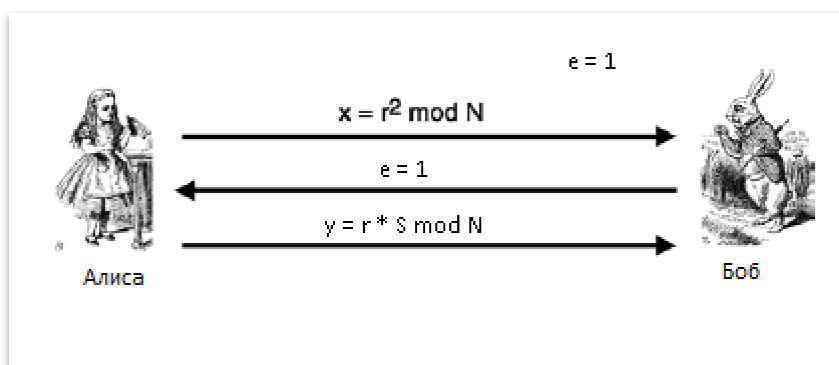
$$y^2 = x * v^e \bmod N$$

и ако је тачна увериће се да Алиса прича истину, што значи да ако се сви држе правила протокола једначина је тачна :

$$y^2 = r^2 * S^{2e} = r^2 (S^2)^e = x * v^e \bmod n$$

приказаћемо случај када постоји могућност да је $e = 1$ и $e = 0$, односно обе стране новчића.

Пример $e = 1$:



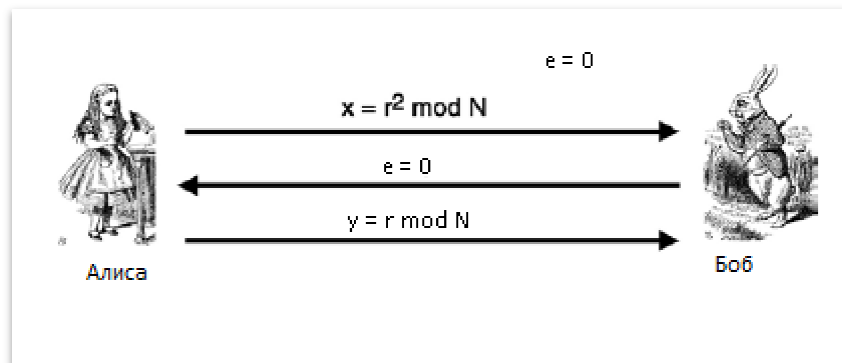
Слика 32. Fiat-Shamir протокол када је $e = 1$.

Ако Боб одговори с вредношћу $e = 1$, Алиса у трећој поруци одговара са $y = r * S \bmod n, (S^e = S^1 = S)$ што значи:

$$y^2 = r^2 * S^2 = x * v \bmod n$$

Када је $e = 1$, Алиса мора да зна тајну S . У примеру са пећином, ако Алиса није на правој страни, она мора да зна тајну како би прешла на другу страну и како би Боб био сигуран да Алиса зна тајну.

Пример $e = 0$:



Слика 33. Fiat-Shamir протокол када је $e = 0$.

Ако је $e = 0$, Алиса одговара са $y = r \bmod N, (S^e = S^0 = 1)$ што представља:

$$y^2 = r^2 = x \bmod N$$

Алиса у овом случају не мора да зна тајну, такође из примера са пећином, јер ако Боб крене њеним путем она неће морати да отвара врата.

Прва фаза у овом Fiat-Shamir протоколу је да Алиса шаље p^2 јер проналажење квадратног корена по модулу је веома тешко [2]. Друга фаза представља изазов, где Боб изазива Алису да му пружи тачан одговор. Трећа фаза се односи на пружање одговора на Бобов изазов, у коме Алиса мора да тачно да одговори, који Боб може да провери користећи једначину:

$$y^2 = r^2 * S^{2e} = r^2 (S^2)^e = x * v^e \bmod N.$$

Математичка основа овог протокола је да Боб може да верификује $y^2 = x * v^e \bmod n$, на основу информације коју је добио, али то не чини протокол безбедним. Да би смо га обезбедили морамо да утврдимо да Труди као нападач може да убеди Боба да зна S и тако га убеди да је она Алиса. Другим речима ако Боб шаље изазове $e = 1$ или $e = 0$, Труди иако не зна тајну, довољно је да следи фазе протокола да би преварила Боба. Из свега овога закључујемо да Боб мора слати $\in \{0,1\}$ на случајан начин, јер тада Труди не може да се држи протокола и може да га превари вероватноћом $\frac{1}{2}$, односно што се више пута понови протокол то су веће шансе да Боб сазна да се ради о превари.

У пракси ако се користе јавни кључеви за аутентификацију Алиса не би знала Бобов јавни кључ и обрнуто. Боб би онда морао Алиси да пошаље свој сертификат како би се аутентификовао пред њом и дао јој свој јавни кључ, што значи да ће и Труди знати да је то Боб, што у овом случају значи да јавни кључеви онемогућавају анонимност у комуникацији.

Fiat-Shamir протокол омогућава да обе стране знају јавне вредности кључева, у којима нема никакве информације о идентитету и размењеним порукама.

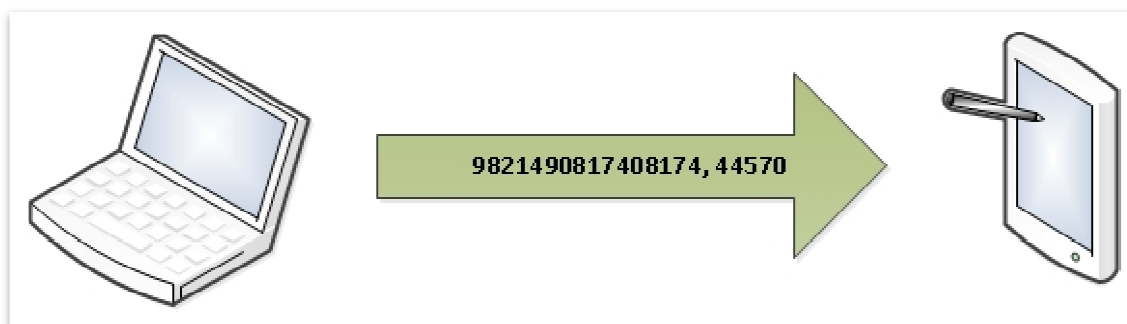
3.10 Верификација гласова

Верификација електронског гласа омогућава гласачу прецизну информацију о свом гласу и безбедности свог рачунара на коме је забележен глас, односно да провери да ли је рачунар заражен одређеним малициозним програмом који може да утиче на исход самог гласачког листића. Идеја је да гласач добије повратну информацију од сервера о забележеном гласу у виду кода, који не открива никакву информацију о изабраном кандидату.



Слика 34. Шифрован глас се шаље изборном серверу, сервер генерише сесијски код “44570” који враћа корисничкој апликацији.

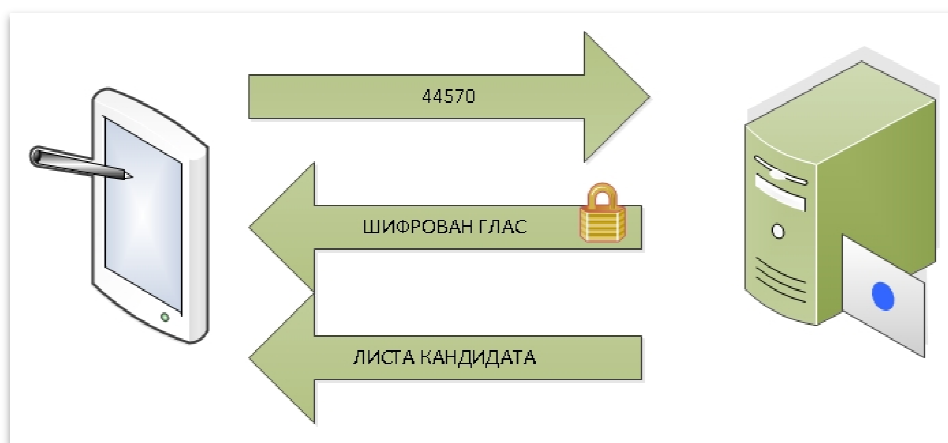
Гласач изабира кандидата и рачунар генерише неки случајан број, ове две информације и глас ће бити шифроване са јавним кључем система и дигитално потписане од стране гласача и послате серверу. Сервер генерише сесијски број који заједно са случајним бројем враћа гласачу као одговор да је успешно обавио гласање. Ове две информације се враћају гласачу помоћу којих он може да провери интегритет свог гласа.



Слика 35. Случајан број “9821490817408174” и сесијски код “44570” су преко изборне апликације приказани у облику QR кода, који се може прочитати помоћу

мобилног уређаја. Идеја овога је да гласач може помоћу кода односно хеш вредности поруке утврди интегритет гласа.

Пример [16] ове све информације ће бити враћене у облику *QR* кода, који ће корисник помоћу свог нпр. Андроид уређаја прочитати ове информације. Апликација ће серверу послати добијен сесијски број и случајан број, сервер ће помоћу дигиталног потписа идентификовати послате вредности, након чега ће сервер послати листу кандидата, апликација ће упоредити шифрате свих кандидата са листе користећи случајан број, и на тај начин ће наћи шифрат који одговара гласу који је послат, и тако проверити интегритет гласа.



Слика 36. Изборна апликација шаље сесијски код “44570” изборном серверу. Сервер идентификује гласача, и враћа дигитално потписан глас и листу гласача на корисников рачунар или мобилни уређај, како би изборна апликација могла да провери интегритет гласа.

3.11 Аутентификација

Процес аутентификације је утврђивање идентитета корисника, односно провера да је неко оно што тврди да јесте. У приватним и јавним рачунарским мрежама, аутентификација се најчешће врши помоћу лозинки, али у неким случајевима је потребан мало јачи степен заштите са пратећим механизмима, ово може да значи коришћење смарт картица, PIN кодова, сертификата итд. Понекад је и потребно да се систем кориснику аутентификује. Аутентификација се дели на 3 основне ставке:

- Оно што знамо.
- Оно што јесмо.
- Оно што имамо.

Оно што знамо може да представља знање одређене шифре или *PIN* кода. Оно што јесмо представљају физичке ствари као што су отисак прста, ирис, потпис, глас итд. Оно што имамо подразумева поседовање нпр. идентификационе картице.

У гласачком систему аутентификација је од изузетног значаја, како би се обезбедио коректан систем гласања и како би се стекло поверење гласача. Очигледна потреба је да се гласач аутентификује систему, али исто толико је важно да се систем аутентификује гласачу како би он био сигуран коме шаље свој глас. Једноставан

пример: Алиса шаље свој глас Бобу, Труди се представи као Боб, прими Алисин глас промени га и промењеног пошаље Бобу.

3.12 Шема дупле коверте

Шема дупле коверте представља шему која штити гласачеву приватност, ова шема се успешно користи у Естонији. Шема дупле коверте (Слика 19) може да се дизајнира користећи асиметрично шифровање и бар два пара кључева. Један пар кључева се користи за шифровање самог гласа (унутрашња коверта), а други пар кључева да заштити гласачев идентитет (спољна коверта). Када гласач обави гласање, глас се шифрује јавним кључем изборног сервера и приватним кључем гласача. За отварање спољне коверте користи се гласачев јавни кључ, и на основу тога знамо од кога је глас стигао.

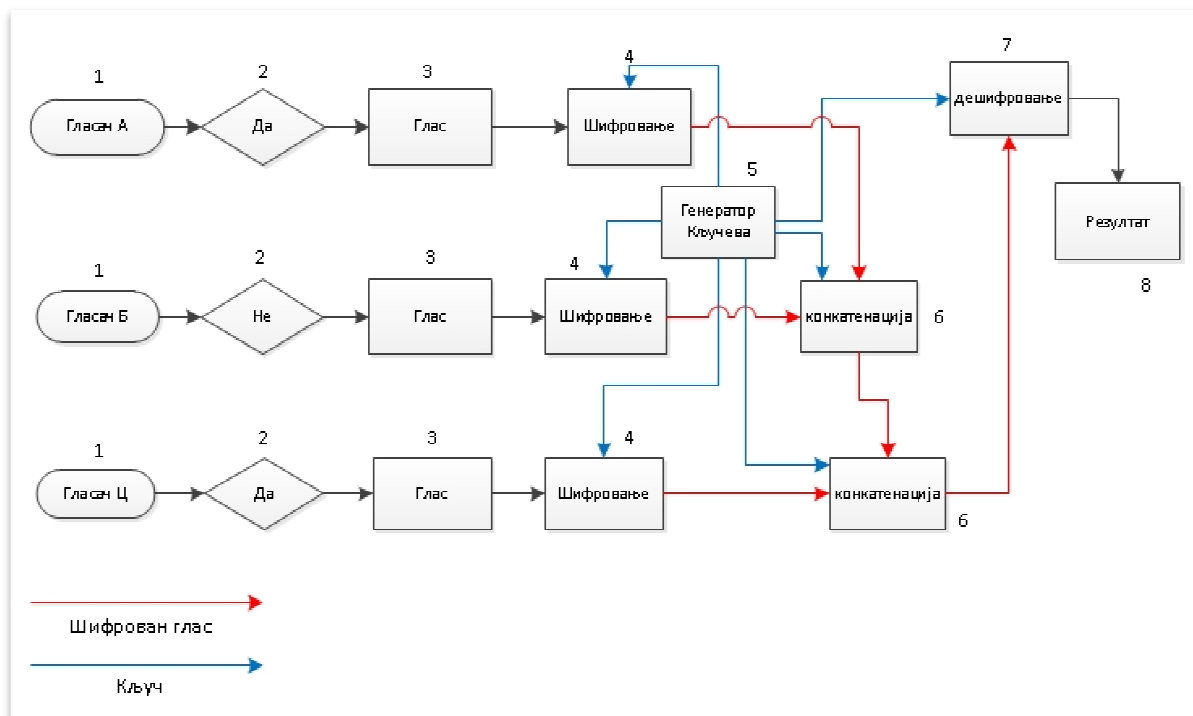
Пар кључева који се користе се генерише по почетку изборног процеса. Кључеви се дистрибуишу до гласача кроз софтвер који се користи за гласање. Приватни кључ за отварање гласачке кутије је доступан само када се изборни процес заврши, и такође захтева да у процедури отварања буду присутни сви званичници из различитих странака, који поседују по део тог кључа (дељење тајни). Спољна коверта представља дигитални потпис гласача. Отварање спољне коверте се врши помоћу гласачевог јавног кључа. Ова шема гласачког система се успешно користи у Естонији.

4 Преглед предложеног решења

У овом поглављу рада предлажемо генеричку шему гласачког система. За потребе експеримента користили смо *Cryptool* развојно окружење.

Cryptool је бесплатан софтвер који има за циљ подизање свести и интересовања у области криптографије. Илустрованим путем омогућава електронско учење и приказивање криптографских концепата, развијен је од стране Немачких компанија и универзитета. Софтвер садржи велики број алата, имплементираних алгоритама за анализу и графичко окружење које омогућава корисницима да се на упознају са тајнама криптографије. *Cryptool* као образовни софтвер добио је неколико међународних признања, као што су: *TeleTrust Special Award 2004*, *EISA 2004*, *IT Security Award NRW 2004*, *Selected Landmark in the Land of Ideas 2008* [19].

4.1 Генеричка шема



Слика 37. Генеричка шема.

На шеми су приказане нумерисане компоненте:

1. Гласач.
2. Избор гласа (за, против).
3. Гласачки листић.
4. Шифровање *Paillier* алгоритмом.
5. Генератор кључева.
6. Конкатенација (додавање гласова).
7. Дешифровање.

8. Приказан резултат.

4.2 Поставка и објашњење експерименталног решења

Представљено решење у *Cryptool*-у садржи 3 гласача који у овом случају имају две изборне опције, „за“ (ДА) и „против“ (НЕ) односно *true* или *false*. У наставку овог подпоглавља детаљно ћемо дискутовати о функционалностима које су представљене у овој шеми која задовољава све особине гласачких система о којима смо писали у деловима рада пре.

Посматраћемо шему кроз фазе:

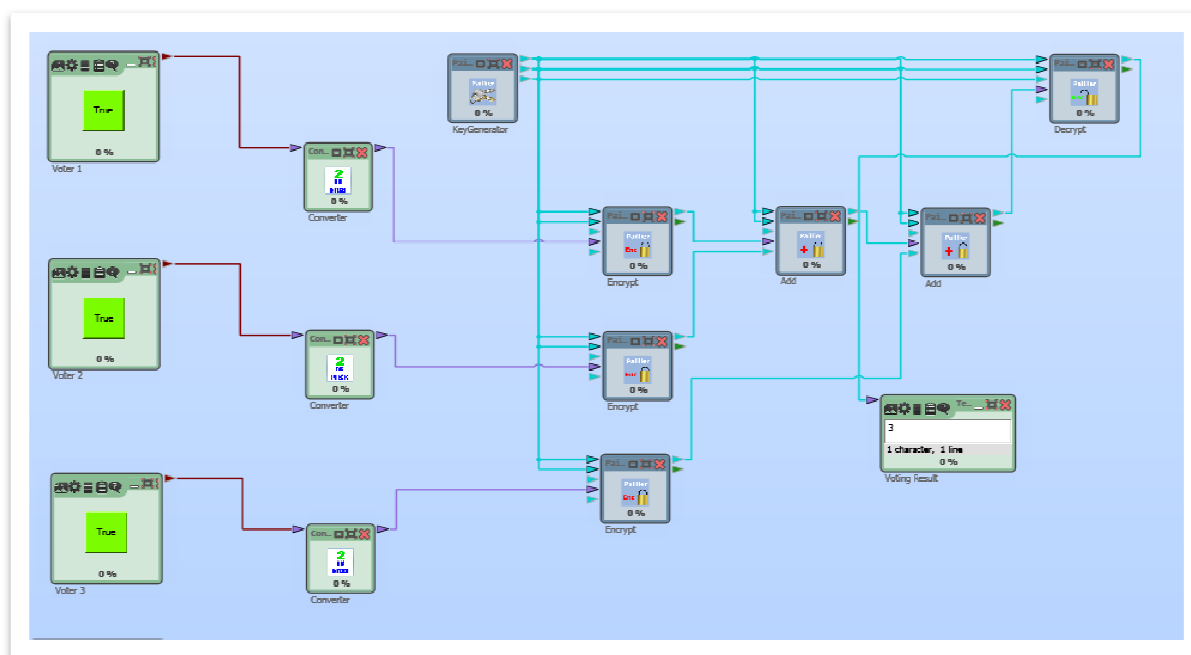
Фаза 1: Гласачу су путем адекватног интерфејса понуђене две изборне опције. Гласач се опредељује само за једну опцију. Тачан интерфејс у овом раду није био предмет истраживања. Овај део рада се односи на саму ергономију софтвера.

Фаза 2: Након успешног избора, глас се шифрује са *Paillier*-овим алгоритмом са кључевима N и G . Кључеви N и G су генерисани преко посебног генератора који је дефинисан од стране *Paillier* алгоритма. Треба запазити у шеми да се сви гласови шифрују са истим кључем независно од броја гласача и гласа.

Фаза 3: Са претпоставком да постоје 3 гласача, како је приказано на шеми, након првог и другог добијеног шифрата (шифрован глас) за гласача 1 и 2, користи се *Paillier*-ова функција додавања (криптографска конкатенација) са кључевима N и G , што резултује са новим податком (који у потпуности енкапсулира гласача 1 и гласача 2) који се на идентичан начин функцијом додавања повезује са шифратом гласача 3 и тако генерише нови енкапсулирани податак. Процес енкапсулације у случају n гласача у потпуности би одговарао особинама бинарног стабла, енкапсулирани податак у овој шеми обезбеђује гласачима потпуну анонимност у одабиру гласа, ова врста анонимности је управо производ хомоморфног својства *Paillier* алгоритма.

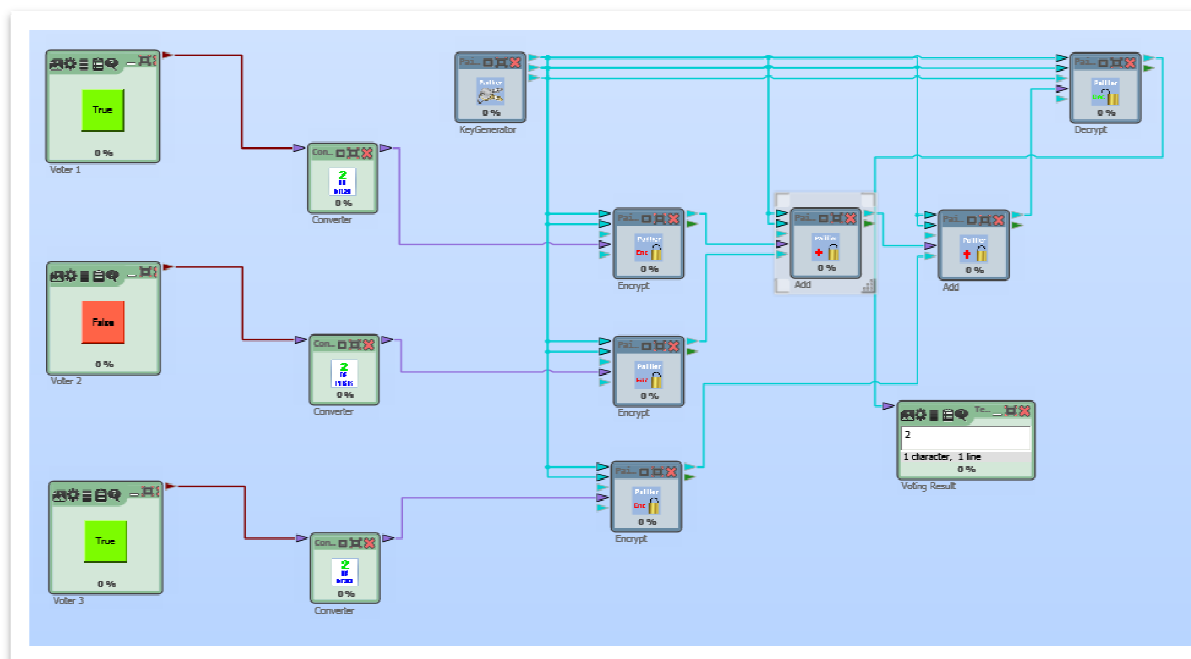
Фаза 4: У последњој фази, на страни субјекта који пребраја гласове, утврђује се број гласова ЗА и ПРОТИВ. До ових информација се долази применом *Paillier*-овог алгоритма у режиму за дешифровање применом одговарајућих кључева. У овој фази је могуће дешифровати све гласове, утврдити изборне опције (пребројати), али није могуће сазнати идентитет гласа или направити тачну везу између гласача и изборне опције на другој страни. Оваква врста анонимности је захтевна код оваквих система, наравно ови системи подразумевају независан систем или подсистем за обављање аутентификације гласача, ради установљења његових гласачких права који су у складу са законом које држава прописује.

У наставку приказана је симулација нашег гласачког система са свим могућим стањима са 3 гласача.



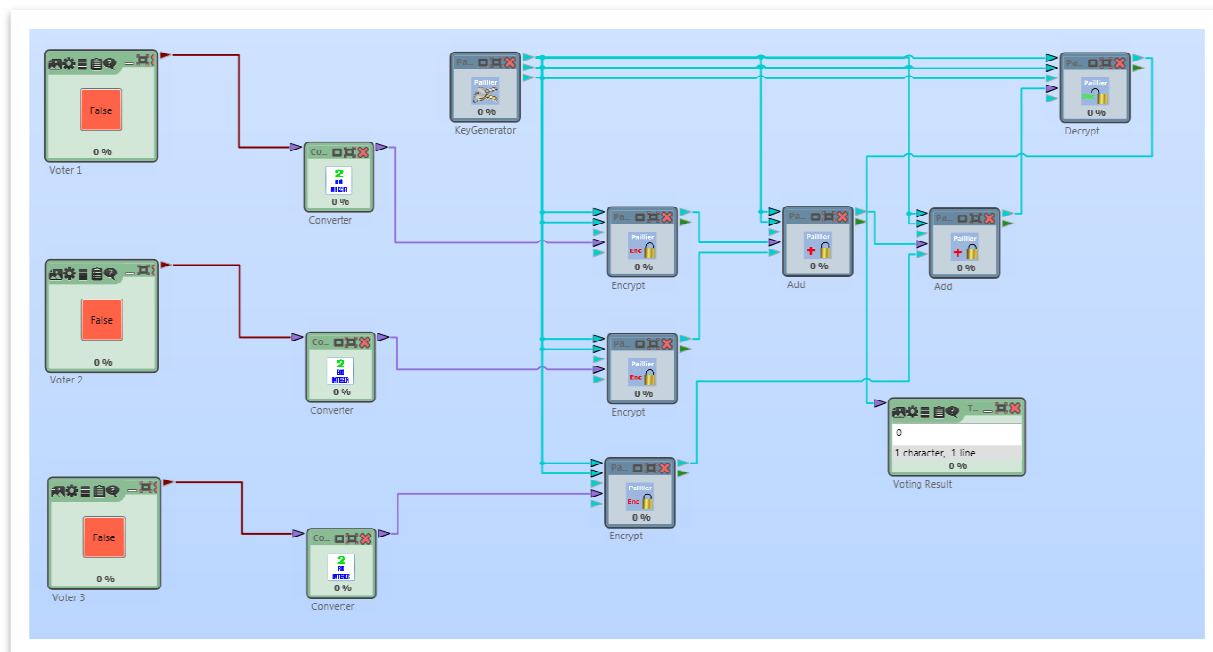
Слика 38. Резултат на предложеној шеми је 3, што значи да су сва три гласача гласала „за”.

На слици 36. Приказан је случај у коме су сва три гласача гласала за исту опцију, што се види на крају шеме, у фази где се гласови дешифрују и пребрајају.



Слика 39. Резултат на предложеној шеми је 2, што значи да су два гласача гласала „за” и један „против”.

На слици 37. Приказан је случај у коме су два гласача гласала за исту опцију, док је трећи гласач изабрао другу опцију, што се види на крају шеме, у фази где се гласови дешифрују и пребрајају.



Слика 40. Резултат на предложеној шеми је 0, што значи да су сва три гласача гласала „против”.

На слици 38. Приказан је случај у коме су три гласача гласала за исту опцију, што се види на крају шеме, у фази где се гласови дешифрирају и пребрајају. У сва три случаја која смо приказали јасно се види да страна која поседује кључеве који су се користили за шифровање није у могућности да сазна било шта друго осим броја гласова.

Због изванредних својстава *Paillier*-овог алгоритма, у наредном подпоглављу због бољег разумевања алгоритма који је уграђен у гласачке системе, објаснићемо дизајн *Paillier*-овог алгоритма.

4.3 Хомоморфност – Паилиеров алгоритам [5]

Хомоморфност је форма енкрипције која омогућава одређене рачунске операције над шифратом, на излазу генерише шифрован резултат, који када се дешифрира одговара резултату операција над оригиналним текстом. Ово је пожељна функција у архитектури модерних комуникационих система. Хомоморфна енкрипција је добра основа за повећање безбедносних мера над непознатим системима и апликацијама које приступају осетљивим информацијама.

За гласачки софтвер постоје два могућа хомоморфна алгоритма са особиним додавања: *Paillier* и *ElGamal*. *Paillier* алгоритам је већ сам по себи добар за случај додавања гласова и много чешће се користи. Оригинална *ElGamal* шема користи особине мултипликације и она се може модификовати да поседује особине хомоморфног додавања, али може доћи до проблема у случају великог броја гласача када ова шема постаје неефикасна, док *Paillier* пружа једноставнију имплементацију и добре перформансе.

Paillier-ов алгоритам је криптолошки систем базиран на систему јавних кључева који је дизајнирао Француски истраживач *Pascal Paillier* 1999. Године [5].

Генерисање кључева:

Генеришу се два проста броја, p и q независно један од другог, где важи:

$$\gcd(pq, (p-1)(q-1)) = 1.$$

Постоји два начина за генерисања g где $g \in \mathbb{Z}_n^*$.

Први начин:

Случајно изабран g из $\mathbb{Z}_n^*$ где важи: $\gcd(g^{\lambda} \bmod n^2 - 1/n, n) = 1$

Где важи да је $\varphi(n) * \varphi(n)$ број валидних генератора, и зато је могућност одабира из

$n\varphi(n)$ од елемената $\mathbb{Z}_n^*$ је релативно велика за n .

Други начин:

Случајно изабрани α и β од елемената $\mathbb{Z}_n^*$ и израчунати $g = (\alpha n + 1)\beta^n \bmod n^2$, у овом случају g увек задовољава услове.

$$\begin{aligned} n &= p * q \\ \lambda &= \text{lcm}(p-1, q-1) \\ \mu &= (L(g^{\lambda} \bmod n^2)) - 1 \bmod n \end{aligned}$$

$$L(u) = u - 1/n$$

Ова инверзна функција постоји ако и само ако је валидни g изабран из претходних случајева.

(n, g) јавни кључеви за шифровање

(λ, μ) приватни кључеви за дешифровање

$\gcd$ – највећи заједнички делилац.

lcm – најмањи заједнички садржалац.

Шифровање:

m - порука

r - случајан број

$r \in \mathbb{Z}_n^*$

$m \in \mathbb{Z}_n$

$E(m)$ - шифрат

$$E(m) = g^m * r^n \bmod n^2$$

Дешифровање:

$$m = L(c^{\lambda} \bmod n^2) * \mu \bmod n$$

Значајне особине *Paillier* алгоритма су његове хомоморфне особине. Како су функције шифровања додатно хомоморфне, оне се могу описати као:

Хомоморфно додавање текста:

Резултат два шифрата ће се дешифровати и одговарати суми два отворена текста.

$$D(E(m1, r1) * E(m2, r2) \bmod n^2) = m1 + m2 \bmod n$$

Резултат шифрата и отвореног текста са растућим g ће одговарати дешифрованој вредности одговарајућег текста.

$$D(E(m1, r1) * g^{m2} \bmod n^2) = m1 + m2 \bmod n$$

Где за важи: да свако $m1, m2$ припада скупу Z_n .

Ове хомоморфне особине могу бити коришћене од стране сигурних електронских система. Претпоставимо једноставан изборни систем где гласач бира “за” или “против” у свом гласу. Неки број гласача m бира свој глас (1 или 0). Сваки гласач шифрује свој избор пре одабира гласа. Изборни званичници узимају резултат шифрованих гласова које дешифрују, резултат који садржи вредност n који представља збир свих гласова. Тако званичници знају је n број гласова гласало “за” а $m-n$ гласало “против”. Улога случајног броја r осигурава да ће два еквивалентна гласа бити шифрована у идентичан шифрат, је са занемарљивом вероватноћом, како би осигурали гласачеву, у овом случају анонимност.

Пример:

Претпоставимо да имамо N_v – број гласача и N_c – број изборних кандидата. Сваки глас морамо да представимо у нумеричкој форми и шифрујемо Paillier-ом. Свако шифровање захтева случајан број, тако да сваки глас буде различито шифрован. Серверска база b мора бити већа од броја гласача. На крају изборног процеса изборни званичници ће имати бар број N_v од шифрованих гласова. И онда могу да израчунају шифрован резултат који је резултат свих шифрованих гласова на $\bmod n^2$.

Резултат је представљен формулом: $T = \prod_{i=1}^{N_v} C_i \bmod n^2$

Пример из [5]:

Претпоставимо да имамо 9 гласача и 5 кандидата, где је база $b = 10$, ($b > N_v$). У овом примеру се бира 2 кандидата, постоји могућност за изабир једног кандидата или празан листић.

	Кандидат 1	Кандидат 2	Кандидат 3	Кандидат 4	Кандидат 5	Гласови који се шифрују
Алиса		•				$m = 10^1 = 10$
Боб			•		•	$m = 10^2 + 10^4 = 10100$
Карол						$m = 0$
Дејв				•		$m = 10^3 = 1000$
Ева	•			•		$m = 10^0 + 10^3 = 1001$
Фред		•		•		$m = 10^1 + 10^3 = 1010$
Жил			•	•		$m = 10^2 + 10^3 = 1100$
Хелен		•		•		$m = 10^1 + 10^3 = 1010$
Исак	•					$m = 10^0 = 1$
Укупно	2	3	2	5	1	

Слика 41. Листа кандидата, гласача и забележених гласова.

Као што видимо са слике највећи могући шифрован глас износи:

$$m_{\max} = 10^4 + 10^3 = 11000$$

Док максималан резултат износи:

$$T_{\max} = Nv * m_{\max} = 9 * 11000 = 99000$$

Генерисање кључа:

Бирамо просте бројеве на случајан начин $p=293$, $q=433$.

$$\gcd(pq, (p-1)(q-1)) = 1$$

$$n = pq = 125869$$

$$n^2 = 16095743161$$

$$\lambda = \frac{(p-1)(q-1)}{(p-1)(q-1)} = 31536$$

Након тога користимо Paillier-ов генератор кључева где $g \in \mathbb{Z}_n$.

$$\gcd\left(\frac{g^\lambda \bmod n^2 - 1}{n}, n\right) = 1 \quad g = 6497955158$$

$$\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n =$$

$$= \left(\frac{6497955158^{31536} \bmod 16095743161 - 1}{126869}\right)^{-1} \bmod 126869 = 53022$$

Гласови који се шифрују	Случајан број r	Шифрован глас
$m = 10^1 = 10$	35145	1303928735
$m = 10^2 + 10^4 = 10100$	74384	848742150
$m = 0$	96584	7185465039
$m = 10^3 = 1000$	10966	80933260
$m = 10^0 + 10^3 = 1001$	17953	722036441
$m = 10^1 + 10^3 = 1010$	7292*	350667930*
$m = 10^2 + 10^3 = 1100$	24819	4980449314
$m = 10^1 + 10^3 = 1010$	4955*	7412822644*
$m = 10^0 = 1$	118037	3033281324
23251		

Слика 42. Представљене вредности шифрованих гласова.

Бројање гласова:

$$\begin{aligned}
 T &= \prod N v c \bmod n^2 \\
 &= (1303928735 * 848742150 * 7185465039 * 80933260 \\
 &\quad * 722036441 * 350667930 * 4980449314 * 7412822644 \\
 &\quad * 3033281324) \bmod 16095743161 = 2747997353
 \end{aligned}$$

Дешифровање:

$$\begin{aligned}
 m &= L(c^\lambda \bmod n^2) * \mu \bmod n \\
 &= \left(\frac{(2747997353^{31536} \bmod 126095743161) - 1}{126869} \right) \\
 &\quad * 53022 \bmod 126869 = 15232
 \end{aligned}$$

5 Закључак

У овом делу рада представимо таксативно сумиране резултате и коначни закључак на основу спроведеног истраживања ове области. Такође, биће представљене идеје за будући развој апликације и безбедносних протокола, који имају за циљ да створе безбедне техничке услове за гласање преко Интернета.

5.1 Сумирани циљеви рада и остварени доприноси

На основу истраживања ове теме и постојећих система који се већ неколико година успешно користе у страним земљама, сматрамо да систем има добар основ за имплементацију и реализацију у Србији. Безбедносни протоколи који представљају основу овог система, данас се широко користе у нашој земљи у различитим гранама економије и трговине и другим Интернет сервисима. Поред свих захтеваних безбедносних мера и даље је највећи проблем поверење. Овај тип гласања биће стална тема критике као модеран систем који би био главна мета напада и због тог разлога је тешко добити наклоност и поверење друштва.

Увођење овог система благовремено би утицало на повећање излазности, претежно млађе генерације. Такође, старијим особама нашег друштва и особама са посебним потребама створиле би се могућности за излазак на гласање. Имплементацијом и коришћењем овог система у наредним годинама буџет који се формира за сваке изборе, знатно би био мањи уколико би дошло до шире употребе оваквих система. Основни мотив овог рада је био да се дизајнира апстрактна верзија система за гласање који ће помоћу имплементације различитих криптолошких протокола у каснијим верзијама онемогућити све типове компромитације и могуће манипулације над системом.

Након истраживања различитих протокола за бројање и шифровање гласова као што су *Mixnets*, *El-Gamal* и *Paillier* дошли смо до закључка да хомоморфне особине сабирања и *Paillier*-ов алгоритам представљају добар основ за постизање анонимности и бројање гласова. Добар систем дефинитивно постоји, на једноставан начин смо демонстрирали модел који представља основу и почетак неког много већег система. О значају ове теме и потребе да се технолошки унапреди, завршићемо са цитатом: “Они који гласају не одлучују ништа, они који броје гласове одлучују све” - *Joseph Stalin*.

5.2 Предлог за будући рад

Примарни циљ будућег рада ће бити истраживање и имплементација протокола и подпротокола који нису поменути у овом раду. Генерисање кључева и електронских система за идентификацију, потребних за систем гласања преко Интернета. Такође, будући циљ је и развој прве верзије апликације за гласање.

Један од будућих пројеката је упоређивање захтева који су потребни да би се дизајнирао и имплементирао успешан систем за гласање, тако да испуњава захтеве као што су: сигурност, анонимност, тајност, легалне и техничке полисе изборног процеса.

Литература

- [1] Mark Stamp, *Information Security*, San Jose University, New Jersey, 2006.
- [2] Милан Милосављевић, Саша Адамовић, *Криптологија 2* [књига], Универзитет Сингидунум, Београд, 2014. -1 : Т.1 : стр. 239. -978-86-7912-537-8.
- [3] Ben Adida, "Advances in Cryptographic Voting Systems", Department of Electrical Engineering and Computer Science, <http://electionmathematics.org/em-voting-systems/rivest-student-adida-phd.pdf>, MIT 2006.
- [4] Warren D. Smith, "Cryptography meets voting", http://www.hit.bme.hu/~buttyan/courses/BMEVIHI5316/Smith.Crypto_meets_voting.pdf, 2005.
- [5] Sansar Choinyambuu, "Homomorphic Tallying with Paillier Cryptosystem", E-Voting seminar, 2009.
- [6] Kristian Gjøsteen, "Analysis of an internet voting protocol", <https://eprint.iacr.org/2010/380.pdf>, 2010.
- [7] "Uncovering the veil on Geneva's internet voting solution", Geneva State Chancellery, Geneva Information Tehnology Centre.
- [8] Vabariigi Valimiskomisjon, "Internet Voting in Estonia", <http://vvk.ee/voting-methods-in-estonia/engindex/> Tallinn, Estonia.
- [9] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow "Elliptic Curve Cryptography in Practice" University of Michigan, University of Pennsylvania.
- [10] Ulrica Löfstedt, "E-Government services in local governments – a study of development in Swedish municipalities", Mid Sweden University, 2007.
- [11] Marine Stenbro, "A Survey of Modern Electronic Voting Technologies", Norwegian University of Science and Technology, Trondheim, Norway 2010.
- [12] Branden Williams, "Will End to End Encryption Save Us All", Јануар 2010.
- [13] http://popis2011.stat.rs/?page_id=1221, Републички завод за статистику, резултати пописа 2011.
- [14] Електронска управа (e-government), http://www.link-elearning.com/dlmaterijali/materijali/DLIIT2/sadrzajNJpdf/IIT2_27.pdf .
- [15] Douglas W. Jones "A Brief History of Voting", The University of Iowa Department of Computer Science, 2001.

[16] “What is Verification of I-votes”, http://www.vvk.ee/public/Verification_of_I-Votes.pdf .

[17] др Владимир Божовић, “Неš функције”, Природно-математички факултет, Подгорица.

[18] др Зоран Бањац, Немања Мачек, Иван Дабић, “НЕŠ FUNKCIJE; LOZINKE; OPHCRACK”, ВШЕР, Београд 2009.

[19] Cryptool, <http://en.wikipedia.org/wiki/CrypTool>.

[20] E-voting, <http://aceproject.org/ace-en/focus/e-voting/countries>

[21] Саша Аџић, “Електронско гласање“, Подгорица 2011.

[22] Link group, “Elektronska uprava (e-Government)”.