МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра комп'ютерної алгебри та дискретної математики

(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

на здобуття освітньо-кваліфікаційного рівня «магістр»

(освітньо-кваліфікаційний рівень)

на тему Криптографічні методи розв'язування проблем електронного голосування

Providing secret electronic voting with cryptographic means

Виконала: студентка денної форми навчання
спеціальності 123 – Комп'ютерна інженерія

(шифр і назва напряму підготовки, спеціальності)

Біла Юлія Василівна

(прізвище, ім'я, по-батькові)

Керівник доц. Варбанець С. П.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент доц. Федоровський С.В.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:

Протокол засідання кафедри

№___ від «___»_____ 2020 р.

Завідувач кафедри

_____ Варбанець П. Д.

(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___

протокол № __ від «___» ____ 2020 р.

Оцінка _____/_____/_____

(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

_____ Казакова Н.Ф.

(підпис) (прізвище, ініціали)

Одеса – 2020

АННОТАЦІЯ

Темою даної дипломної роботи є побудова математичної моделі шифрування для захисту секретної технології електронного голосування від втручання активного хакера.

Мета даної роботи полягає у підвищенні процесу забезпеченості захисту технології таємного електронного голосування. Ця мета досягається шляхом розробки практичних алгоритмів перетворення інформації з властивістю неоднозначності для відновлення повідомлення з перетвореного тексту.

З більшості методів електронного голосування були обрані три «основних», які і стали предметом порівняння. Це ідея електронного бюлетеня Бісмарка, сістема Бена Адіда та система електронного голосування Scantegrity.

За основу взято протокол заперечуваного шифрування, так як основним критерієм високої якості є досить висока стійкість до силової атаки зловмисника. Алгоритм шифрування заснований на деяких рівняннях, які мають кілька різних рішень в наборі можливих рішень.

АННОТАЦИЯ

Темой данной дипломной работы является построение математической модели шифрования для защиты секретной технологии электронного голосования от вмешательства активного хакера.

Цель данной работы заключается в повышении процесса обеспеченности защиты технологии тайного электронного голосования. Эта цель достигается путем разработки практических алгоритмов преобразования информации со свойством неоднозначности для восстановления сообщения с преобразованного текста.

Из большинства методов электронного голосования были выбраны три «основных», которые и стали предметом сравнения. Это идея электронного бюллетеня Бисмарка, Система Бена Адида и система электронного голосования Scantegrity.

За основу взят протокол отрицательного шифрования, так как основным критерием высокого качества является достаточно высокая устойчивость к силовой атаки злоумышленника. Алгоритм шифрования основан на некоторых уравнениях, которые имеют несколько различных решений в наборе возможных решений.

ANNOTATION

The main topic of diploma project is the producing of a mathematical encryption model to protect the secret technology of electronic voting from the intervention of an active hacker.

The goal of this work is to enhance the process of ensuring the protection of secret electronic voting technology. This goal is achieved by developing practical algorithms for transforming information with the ambiguity property for recovering a message from the transformed text.

Of the majority of electronic voting methods, three “basic” ones were chosen, which became the subject of comparison. This is the idea behind Bismarck's e-newsletter, Ben Adid's System and Scantegrity's e-voting system.

The deniable encryption protocol is taken as a basis, since the main criterion for high quality is a sufficiently high resistance to a force attack by an intruder. The encryption algorithm is based on some equations that have several different solutions in the set of possible solutions.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Скорочення

mod – конгруенція по модулю

ЕЦП – електронний цифровий підпис

ВК – відкритий ключ

СК – секретний ключ

ВШ – відкрите шифрування

ЗШ – заперечуване шифрування

НСД – несанкціонований доступ

BCP – планування безперервності бізнесу

XOR – виключна диз'юнкція

БД – база даних

Терміни

QR-код – матричний (двовимірний код)

PIN-код – аналог паролю, але цей код складається лише с цифр

SIM-картка – ідентифікаційний модуль абонента у виде смарт-карти, що застосовується у мобільному зв'язку

ID-картка – самодостатній документ, який посвідчує особу та підтверджує громадянство України, не потребує зчитування даних з чипу, подання додаткових довідок чи сертифікатів

RSA – криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел

AES – симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт)

DES – це симетричний алгоритм шифрування певних даних, стандарт шифрування прийнятий урядом США з 1976 до кінця 1990-х

ГОСТ 28147-89 – радянський і російський стандарт симетричного шифрування, введений в 1990 році

ВСТУП

В даний час інформаційні технології широко використовуються в найважливіших сферах діяльності сучасного суспільства, таких як управлінська, фінансова та економічна сфери. Особливе місце в управлінській діяльності займають технології державного управління, в сукупності представляють собою так званий «Електронний уряд». Такі технології стрімко розвиваються і впроваджуються в провідних країнах світу, в тому числі і в Україні. Метою Електронного уряду є підвищення ефективності державного управління за допомогою впровадження інформаційних технологій. Одним з актуальних питань, пов'язаних з розвитком Електронного уряду, є розробка і впровадження технології таємного електронного голосування через Інтернет.

В електронному голосуванні, як і в традиційному, для голосуючого необхідно забезпечити його анонімність, а також захистити від покупки голосів недобросовісними політиками. У зв'язку з використанням інформаційних технологій в процесі електронного голосування може бути організована автоматизована атака зловмисника на одержувача чи відправника. Запобігання даної ситуації є важливою і вельми актуальним завданням при розробці відповідної технології таємного електронного голосування.

Окреслені завдання забезпечення анонімності та запобігання атак зловмисника можуть бути вирішені за допомогою криптографічних методів захисту інформації і, зокрема, з використанням псевдовірогідного захисного перетворення інформації (заперечуваного шифрування).

Даний тип перетворення інформації дозволяє отримати одну і ту ж криптограму з двох різних повідомлень, одне з яких є істинним і не підлягає розсекречення, а друге, що є помилковим, може бути пред'явлено зловмисникові в разі примушуючої атаки.

Існують теоретичні рішення задачі захисту через Інтернет з використанням псевдовірогідного захисного перетворення, проте їх практичне

впровадження ускладнюється необхідністю виконання багатокрокових інтерактивних процедур, які задають досить високі вимоги до обчислювальних ресурсів і роблять систему електронного голосування досить дорогою. Розробка протоколів заперечуваного шифрування з більш високою продуктивністю в порівнянні з відомими і, які не вимагають виконання багатокрокових інтерактивних процедур голосування полегшує завдання впровадження систем електронного голосування і являє собою значний інтерес для практики інформаційної безпеки, що визначає актуальність теми дослідження.

Мета даної роботи полягає у підвищенні процесу забезпеченості захисту технології таємного електронного голосування. Дана мета досягається шляхом розробки практичних алгоритмів та протоколів перетворення інформації, що володіють властивістю неоднозначності відновлення повідомлення з перетвореного тексту.

Для вирішення поставленої мети були сформульовані та вирішені наступні задачі:

– аналіз та вивчення предметної області;

– дослідження технології таємного електронного голосування, виявлення її переваг та недоліків, проблем та існуючих рішень;

– огляд існуючих методів таємного електронного голосування та виявлення їх недоліків;

– розробка системи електронного голосування з використанням генераторів інверсних конгруентних псевдовипадкових чисел для генерації кільцевого підпису та перетворення секретного повідомлення криптограми, яке містить істинний голос виборця;

– розробка протоколу псевдоімовірнісного захисного перетворення на основі конгруенцій більш високого порядку по модулю, що є добутком двох простих чисел для генерації кільцевого підпису та перетворення секретного повідомлення криптограми, яке містить істинний голос виборця;

– тестування розробленої системи.

Об'єктом дослідження є процес забезпечення інформаційної безпеки.

Предметом – методи, алгоритми та протоколи асиметричних псевдовірогідних захисних перетворень.

ВИСНОВОК

У роботі було проведено аналіз предметної області, досліджено ризики дистанційного електронного голосування, існуючі методи електронного голосування, які є ідеї та системи. Були виявлені переваги та недоліки того чи іншого методу електронного голосування.

Розглянуті моделі порушника інформаційної безпеки, а також захисні перетворення інформації, їх класифікація. Розглянуто модель примушуючої атаки, класифікація примушуючої атаки в залежності від сторони, яка атакується та часу скоєння атаки.

Розглянуто класифікацію та властивості протоколів таємного електронного голосування через Інтернет. Наведено огляд існуючих рішень в даній області.

Наведено огляд існуючих протоколів відкритого шифрування (ВШ), їх переваги та недоліки, можливість застосування на практиці. Також була розглянута модель протоколів відкритого шифрування, яка буде використовуватися у дипломній роботі.

Розроблено алгоритм, його головні результати та покроковий план реалізації алгоритму.

У результаті роботи було створено інтернет систему електронного голосування. У подальших планах – розширити функціонал програми, додати авторизацію та автентифікацію користувачів, додати адмінську частину з більш захищеним доступом. Тоді розроблена система може використовуватись не тільки для особистих потреб, а й для виборів у компанії з великою кількістю співробітників, які знаходяться у різних містах. Також дана система може використовуватися для голосування на рівні країни, для проведення референдумів або виборів у президенти чи парламент, як і наведено в якості прикладу у даній роботі.

Також було прийнято участь у IX Міжнародній науково-практичній конференції, текст публікації представлений у додатку А.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Молдавян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – Санкт-Петербург, Лань, 2001. – С.61, С.146.
2. Бюллетень Бисмарка как метод электронных выборов [Електронний ресурс] – Режим доступу: http://e-gov.by/themes/egov- obzor/byulleten-bismarka-kak-metod-elektronnyx- vyborov.
3. Ben Adida Advances in Cryptographic Voting Systems [Електронний ресурс] – Режим доступу: groups.csail.mit.edu/cis/theses/adida-phd.pdf.
4. Diffie W., Hellman M.E. New Directions in Cryptography// IEEE Transactions on Information Theory, 1996 V. IT-22 C.644-654.
5. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – Москва, Постмаркет, 2001 – С.323
6. Rabin M. O. Digitalized signatures and public-key functions as intractable as factorization // MIT. — 1979.
7. Мао В. Уязвимая среда (модель угрозы Долева — Яо) // Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768с
8. J. Y. Halpern and R. Pucella. A Logic for Reasoning about Evidence, Volume 26, Pp. 1-34.
9. Ran Canetti, Cynthia Dwork, Moni Naor, Rafail Ostrovsky. Deniable encryption. // Crypto, Santa Barbara, California, August 1997. – Pp. 90-104.
10. Z. Rja¡¦skov´a. ―Electronic Voting Schemes,‖ Master thesis. Department of Computer Science Faculty of Mathematics, Physics and Informatics Comenius University, Bratislava, April 2002.
11. Klonowski M., Kubiak P., Kutyłowsk M. Practical Deniable Encryption. // SOFSEM 2008: Theory and Practice of Computer Science,34th Conference on Current Trends in Theory and Practice of Computer Science, Nový Smokovec, Slovakia, January 19-25, 2008. – Pp.599-609.

12. ElGamal Taher. A public key cryptosystem and a signature scheme based on discrete logarithms // Advances in cryptology / Springer. — 1985. — Pp. 10–18.
13. M.H.Ibrahim. A Method for Obtaining Deniable Public-Key Encryption, International Journal of Network Security, Vol.8, No.1, PP.1–9, Jan. 2009.
14. M.H.Ibrahim. Receiver-deniable Public-Key Encryption, International Journal of Network Security, Vol.8, No.2, PP.159-165, Mar. 2009.
15. Adam O'Neill, Chris Peikert, Brent Waters. Bi-deniable public key encryption. // CRYPTO, Santa Barbara, California, August 2011.- Pp. 525-542.
16. Ivan Damgard, Jesper Buus Nielsen. Improved non-committing encryption schemes based on a general complexity assumption. In CRYPTO, pages 432-450, Santa Barbara, California, August 2000.
17. Craig Gentry, Chris Peikert, Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In STOC, pages 197-206, Victoria, British Columbia, Canada, May 2008.
18. Rikke Bendlin, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Claudio Orlandi. Lower and upper bounds for deniable public-key encryption. ASIACRYPT, pages 125-142, Seoul, Korea, December 2011.
19. Marcel Sebek, Fully Bideniable Public-Key Encryption, October 23, 2013.
20. Bo Meng, JiangQing Wang. An Efficient Receiver Deniable Encryption Scheme and Its Applications.// Journal of networks, vol. 5, no. 6, june 2010.
21. Bresson E., Catalano D., Pointcheval D. A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications. // Laih CS, ed.Aciacrypt 2003, Berlin: Springer. - 2003. 37-54.
22. Молдовян Н.А., Щербаков А.В. Протокол бесключевого отрицаемого шифрования – Вопросы защиты информации 2016 No2. – с.9-14.
23. N. Moldovyan, A. Moldovyan - Practical Method for Bi-Deniable Public-Key Encryption, 18th Conference Open Innovations Association and Seminar on

Information Security and Protection of Information Technology (FRUCT-ISPIT), 2016.

24. J. Benaloh, D. Tuinstra. Receipt-free secret-ballot elections. – Proceeding of the Twenty-Sixth Annual ACM Symposium on theory of Computing, Montreal, Quebec, Canada. May, 1994. ACM New York, NY, USA.
25. Benaloh J.C.: Verifiable secret-ballot elections. PhD Thesis, Yale University, Department of Computer Science, Number 561. 1987.
26. Hirt M., Sako K.: Efficient receipt-free voting based on homomorphic encryption. In Pro- ceeding of EUROCRYPT ’00, LNCS 1807. pp. 539-556. 2000.
27. H. Zhong, L. Huang, Y. Luo. A Multi-Candidate Electronic Voting Scheme Based on Secure Sum Protocol // Journal of Computer Research and Development, 43 (8), 2006 – Pp. 1405-1410.
28. A. Juels, M. Jakobsson. Coercion-resistant electronic elections, 2002. http://www.voteauction.net/VOTEAUCTION/165.pdf.
29. A. Acquisti. Reciept-Free Homomorphic Elections and Write-in Voter Verified Ballots. – Technical Report 2004/105, International Association for Cryptologic Research, May, 2, 2004.
30. B. Lee, K. Kim. Receipt-free electronic voting protocol through collaboration of voter and honest verifier // http://citeseer.nj.nec.com/lee00receiptfree.html, 2000.
31. T.M. Barakat. A New Sender-Side Public-Key Deniable Encryption Scheme with Fast Decryption. KSII Transactions on Internet and Information Systems vol.8 No 9. Sep. 2014, Pp. 3231-3249.
32. Howlader, J., Basu, S. Sender-Side Public Key Deniable Encryption Scheme. Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference, Pp. 9-13.
33. Vaitkevicius M.:Method sand protocols of pseudo probabilistic defensive transform of information for technologies of secret electronic vote. PhD Thesis. p. 110 (in Russian).

34. VarbanetsP., VarbanetsS.: Inversive generator of the second order with a variable shift for the sequence of PRN's. Annales Univ. Sci. Budapest., Sect. Comp. 46. pp. 255–273. 2017.
35. Мао В. Современная криптография. Теория и практика. – М.: Вильямс, 2005. – 763 с.
36. HTML [Електронний ресурс] – Режим доступу: https://developer.mozilla.org/ru/docs/Web/HTML.
37. CSS [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/CSS.
38. JavaScript [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/nix/blog/257617/.
39. Node.js [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Node.js
40. Біла Ю.В., Криптографічні методи вирішення проблем електронного голосування, Матеріали 9-ої міжнародної науково-практичної конференції (ІУСТ-2020), С. 208