Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Система для электронного голосования

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Курылева Дмитрия Петровича

Научный руководитель

доцент, к.ф.-м.н. _____ А. В. Жаркова

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В. Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

Голосование, безусловно, является неотъемлемым атрибутом нашей жизни. С выборами мы встречаемся постоянно, начиная от голосования за любимую песню на концерте и заканчивая таким серьёзным делом, как выборы президента страны. В связи с бурным развитием сетевых технологий стало возможным задуматься о реализации выборов в глобальной сети. Но голосовать через Интернет за любимую песню и за президента – это две огромные разницы, поэтому стоит понимать, что требования к безопасности и защите информации во втором случае значительно больше, чем в первом. Таким образом, реализация подобного проекта является делом чрезвычайно сложным, как в физическом плане, так и с точки зрения защиты информации.

Целью настоящей работы является разработка и реализация комплекса программ, имитирующих безопасные выборы посредством передачи данных через сеть.

Для достижения поставленной цели требуется решить следующие задачи:

1) изучить различные протоколы тайного голосования;

2) рассмотреть алгоритмы и протоколы, необходимые для реализации системы на базе выбранного протокола голосования.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 4 приложений. Общий объем работы – 101 страница, из них 51 страница – основное содержание, включая 26 рисунков и 1 таблицу, список использованных источников из 26 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 дипломной работы «Необходимые понятия» приводятся необходимые определения из области криптографии (шифр, шифрование, расшифрование, криптограмма и так далее) и универсальной алгебры (группа, кольцо, поле и так далее) [1-5].

Во 2 разделе работы «Шифрование» приводится согласно [6-13] обзор алгоритмов шифрования, симметричных и асимметричных. В симметричных алгоритмах шифрования, для того чтобы зашифровать сообщение и для его последующей расшифровки, используется один и тот же ключ, а при асимметричном шифровании процедуры шифрования и расшифрования осуществляются на разных ключах.

К симметричным алгоритмам шифрования относятся стандарты ГОСТ 28147-89 [6], AES [7], DES [8], ГОСТ 34.12-2015 [9]. К асимметричным алгоритмам шифрования относятся стандарт DSA [11], алгоритм Эль-Гамаля [12], шифрсистема RSA [13]. В данном разделе приводится обзор симметричных блочных шифров DES и «Кузнечик», а также асимметричных криптосистем Эль-Гамаля и RSA.

Для реализации в практической части дипломной работы были выбраны:

– симметричный блочный шифр «Кузнечик», входящий в национальный стандарт шифрования Российской Федерации ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»;

– асимметричная шифрсистема RSA, являющаяся наиболее распространенной системой с открытым ключом.

В 3 разделе работы «Безопасные выборы» приводится обзор протоколов голосования таких, как традиционное «бумажное» голосование, два упрощенных протокола голосования и протокол голосования с двумя избирательными комиссиями [14-19].

Компьютерное голосование никогда не будет использовано для обычных выборов, пока не появится протокол, который одновременно предохраняет от мошенничества и защищает тайну личности. Согласно [15] идеальный протокол должен обладать по меньшей мере следующими шестью свойствами:

1) голосовать могут только те, кто имеет на это право;
2) каждый может голосовать не более одного раза;
3) никто не может узнать, за кого проголосовал конкретный избиратель;
4) никто не может проголосовать вместо другого;
5) никто не может тайно изменить чей-то голос;
6) каждый голосующий может проверить, что его голос учитывался при подведении итогов голосования.

Кроме того, для некоторых схем голосования может понадобиться следующее требование:

7) каждый знает, кто голосовал, а кто нет.

В 3 разделе работы приведено соответствие рассмотренных протоколов данным свойствам идеального протокола голосования, также приведен сравнительный анализ рассмотренных протоколов голосования, на основании которого был выбран для дальнейшей реализации протокол голосования с двумя избирательными комиссиями. Данный протокол был предложен Ханну Нурми (Hannu Nurmi), Арто Саломаа (Arto Salomaa) и Лилой Сантин (Lila Santean). Функции центральной избирательной комиссии (ЦИК), согласно протоколу, распределены между двумя комиссиями: центральным управлением регистрации (ЦУР), выполняющим регистрацию пользователей, и отдельной ЦИК для приема и подсчета бюллетеней.

В 4 разделе работы «Программная реализация» описывается программный продукт, разработанный и реализованный в результате проделанной работы, состоящий из трёх программ:

– программа, предназначенная для избирателей – Клиент для голосования;

– программа, отвечающая за управление регистрацией – ЦУР;

– программа, отвечающая за прием голосов и подсчет результатов – ЦИК.

Программы написаны на языке C# в среде программирования Visual Studio 2017. Также для работы программ была реализована отдельная библиотека классов, которая содержит классы для работы с шифрованием и обменом данных между программами.

Реализованный комплекс программ позволяет проводить безопасные выборы с двумя избирательными комиссиями в соответствии с выбранным протоколом голосования. В данном разделе дипломной работы рассматривается полный процесс проведения выборов. Приведен порядок действий всех участников выборов, а также рисунки, демонстрирующие окна программ во время проведения выборов.

В приложениях 1-4 к дипломной работе представлены листинги написанных программ и библиотеки классов. Для написания программ использовались источники [20-26].

ЗАКЛЮЧЕНИЕ

Несомненно, криптографические протоколы могут быть использованы при построении систем, посредством которых люди выражают свое мнение. При этом при проектировании таких систем голосования безопасность и соображения секретности, конечно, должны быть приняты во внимание.

В данной дипломной работе рассмотрены некоторые протоколы голосования, при этом большая часть работы посвящена протоколу голосования с двумя избирательными комиссиями. Данный протокол не идеален, однако стоит понимать, что и схема используемого традиционного «бумажного» голосования имеет как свои достоинства, так и недостатки. Уязвимым местом рассмотренного протокола является тот факт, что избирателям все-таки приходится надеяться на честность ЦУР и ЦИК, так как в сговоре комиссии могут узнать, за кого проголосовал конкретный избиратель.

В ходе дипломной работы был разработан и реализован на языке программирования C# программный комплекс, имитирующий безопасные выборы посредством голосования с двумя избирательными комиссиями с использованием самостоятельно реализованных блочного шифра «Кузнечик», входящего в национальный стандарт РФ ГОСТ Р 34.12-2015, и асимметричной системы шифрования RSA.

При правильной организации разработанную систему для электронного голосования можно использовать для проведения безопасных локальных выборов.

Таким образом, все поставленные задачи полностью выполнены, цель работы можно считать достигнутой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : учеб. пособие / В. Н. Салий // Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского [Электронный ресурс]. Саратов, 2017. 43 с. : ил., табл. URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2017/10/18/saliy_v.n._kriptograficheskie_metody_i_sredstva_zashchity_informacii.pdf (дата обращения: 09.01.2018). Загл. с экрана. Яз. рус.

2 Амелин, Р. В. Информационная безопасность [Электронный ресурс] : учеб. пособие / Р. В. Амелин // УЦ «Новые технологии в образовании» [Электронный ресурс] : [сайт]. URL: http://nto.immpu.sgu.ru/sites/default/files/3/__77037.pdf (дата обращения: 16.11.2017). Загл. с экрана. Яз. рус.

3 Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» // КонсультантПлюс [Электронный ресурс] : надежная правовая поддержка. URL: https://www.consultant.ru/document/cons_doc_LAW_112701 (дата обращения: 26.12.2017). Загл. с экрана. Яз. рус.

4 Основы криптографии : учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. 2-е изд., испр. и доп. М. : Гелиос АРВ, 2002. 480 с.

5 Жданов О. Криптографические методы защиты информации [Электронный ресурс] / О. Жданов, Ю. Ушаков // НОУ ИНТУИТ [Электронный ресурс] : [сайт]. URL: https://www.intuit.ru/studies/courses/13837/1234/info (дата обращения: 20.09.2017). Загл с экрана. Яз. рус.

6 ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

[Электронный ресурс] // Государственный стандарт Союза ССР [Электронный ресурс]. URL: http://gostshifr.url.ph/gost_28147_89.pdf (дата обращения: 12.12.2017). Загл. с экрана. Яз. рус.

7 Announcing the Advanced Encryption Standard (AES) [Электронный ресурс] // NIST [Электронный ресурс] : National Institute of Standards and Technology. 2001. 51 p. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (дата обращения: 12.12.2017). Загл. с экрана. Яз. рус.

8 Data Encryption Standard (DES) [Электронный ресурс] // NIST [Электронный ресурс] : National Institute of Standards and Technology. 1999. 27 p. URL: https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf (дата обращения: 12.12.2017). Загл. с экрана. Яз. англ.

9 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс]. URL: http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 12.12.2017). Загл. с экрана. Яз. рус.

10 ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс]. URL: https://www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf (дата обращения: 12.10.2017). Загл. с экрана. Яз. рус.

11 Digital Signature Standard [Электронный ресурс] // NIST [Электронный ресурс] : National Institute of Standards and Technology. 2009. 131 p. URL: https://csrc.nist.gov/csrc/media/publications/fips/186/3/archive/2009-06-25/documents/fips_186-3.pdf (дата обращения: 12.12.2017). Загл. с экрана. Яз. англ.

12 Молдовян, Н. А. Введение в криптосистемы с открытым ключом [Электронный ресурс] : учебное пособие / Н. А. Молдовян, А. А. Молдовян. СПб. : БХВ-Петербург, 2005. 288 с. Загл. с экрана. Яз. рус.

13 Коутинхо, С. Введение в теорию чисел. Алгоритм RSA [Электронный ресурс] / С. Коутинхо; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. М. : Постмаркет, 2001. 328 с. Загл. с экрана. Яз. рус.

14 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. М. : Триумф, 2003. 806 с.

15 Ященко, В. В. Введение в криптографию [Электронный ресурс] / В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко, Г. А. Кабатянский, П. Н. Девянин, В. Г. Проскурин, А. В. Черемушкин, П. А. Гырдымов, А. Ю. Зубов, А. В. Зязин, В. Н. Овчинников, М. И. Анохин. М. : МЦНМО, 2012. 348 с. Загл. с экрана. Яз. рус.

16 Анисимов, В. В. Протоколы голосования [Электронный ресурс] / В. В. Анисимов // Учебная и научная деятельность Анисимова Владимира Викторовича [Электронный ресурс] : [сайт]. URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema15 (дата обращения: 12.10.2017). Загл. с экрана. Яз. рус.

17 Nurmi, H. Secret ballot elections in computer networks [Электронный ресурс] / H. Nurmi, A. Salomaa, L. Santean // Computers and Security, 36 (10). 1991. P. 553–560. Загл. с экрана. Яз. англ.

18 Salomaa, A. Verifying and recasting secret ballots in computer networks. [Электронный ресурс] / A. Salomaa // New Results and New Trends in Computer Science. Berlin : Springer-Verlag, 1991. P. 283–289. Загл. с экрана. Яз. англ.

19 Саломаа, А. Криптография с открытым ключом. [Электронный ресурс] / А. Саломаа; пер. с англ. И. А. Вихлянцев, А. А. Болотов. М. : Мир, 1995. 318 с. Загл. с экрана. Яз. рус.

20 Троелсен, Э. Язык программирования C# и платформа .NET 4.6 [Электронный ресурс] / Э. Троелсен, Ф. Джепикс. М. : Издательский дом «Вильямс», 2016. 1440 с. Загл. с экрана. Яз. рус.

21 Рихтер, Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C# [Электронный ресурс] / Дж. Рихтер. СПб. : Питер, 2013. 896 с. Загл. с экрана. Яз. рус.

22 Сетевое программирование в .NET Framework [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ruru/library/4as0wz7t(v=vs.110).aspx (дата обращения: 10.10.2017). Загл. с экрана. Яз. рус.

23 Пошаговые руководства по Windows Forms [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/zftbwa2b(v=vs.110).aspx (дата обращения: 14.10.2017). Загл. с экрана. Яз. рус.

24 Модель криптографии .NET Framework [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/0ss79b2x(v=vs.100).aspx (дата обращения: 16.10.2017). Загл. с экрана. Яз. рус.

25 Коллекции (C# и Visual Basic) [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/ybcx56wz(v=vs.120).aspx (дата обращения: 15.11.2017). Загл. с экрана. Яз. рус.

26 Коллекции (C# и Visual Basic) [Электронный ресурс] // Microsoft Developer Network [Электронный ресурс] : [сайт]. URL: https://msdn.microsoft.com/ru-ru/library/7y3x785f(v=vs.110).aspx (дата обращения: 20.11.2017). Загл. с экрана. Яз. рус.