МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Протокол аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Шашкова Ильи Владимировича

Научный руководитель
к. ф.-м. н., доцент _____ В. Е. Новиков
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

Аутентификация как процесс существует с начала появления информационных систем. Для подтверждения своей личности всегда используется специально организованная секретная информация. Например, в древней Греции для этих целей использовались устные пароли. С развитием технологий развивались и методы, которыми пользовались при подтверждении своей личности. Постепенно в решение этой задачи все больше и больше начали включаться приборы, которые производили действия без участия человека.

Появление первых ЭВМ позволило перенести передачу информации в виртуальную среду. С началом этого процесса задача аутентификация стала наиболее острой проблемой. Так как теперь убедиться, в том, что остальные участники сети именно те, за кого себя выдают было гораздо сложнее. Начали создаваться первые протоколы аутентификации в информационных сетях. Дополнительным толчком в развитии протоколов аутентификации являлось возможность использования вычислительных возможностей ЭВМ. Причем эта возможность давала преимущество, как обычным пользователям, так и злоумышленникам. Протоколы становились все сложнее, а злоумышленники, пытающиеся их обмануть, все изобретательнее.

Схемы аутентификации с момента своего появления существенно изменились. На данный момент самыми распространенными схемами аутентификации являются парольные системы и схемы аутентификации вида «запрос-ответ». Общим свойством данных типов аутентификации является передача по открытой сети информации о секрете. Это позволяет перехватывать информацию злоумышленнику и, иногда, по перехваченной таким образом информации, злоумышленник может восстановить секрет.

В противовес данным системам выступают протоколы аутентификации на основе доказательств с нулевым разглашением. Такие протоколы аутентификации обладают тем свойством, что ни один участник протокола не узнает больше информации о секрете, чем знал до начала работы

протокола. Однако данные протоколы не получили широкого распространения, так как обладают существенным недостатком, а именно: интерактивность и трудоемкость операций, что влияет на скорость работы данных протоколов.

Задачи дипломной работы:

1) Рассмотреть протокол аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма.

2) Описать проблемы, связанные с прикладным использованием данного протокола.

3) Разработать программный комплекс, позволяющий провести процесс аутентификации на основе описанного протокола.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 4 приложений. Общий объем работы – 83 страницы, из них 55 страница – основное содержание, включая 51 рисунок, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В 1-ом разделе приведены теоритические сведения, используемые при решении основной задачи работы. А именно приведены необходимые сведения из теории групп, из теории чисел, из теории эллиптических кривых, групп точек эллиптической кривой и теоритические сведения, связанные с задачей дискретного логарифмирования.

Во 2-ом разделе представлены основные криптографические протоколы, необходимые для решения основной задачи работы. К ним относятся: протоколы доказательства с нулевым разглашением и протокол подбрасывания монеты. Кроме того, здесь же представлено описание криптосистемы RSA, которая используется в протоколе подбрасывания монеты.

Раздел 3 является основным разделом работы. В нем приведены описания протокола аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма и особенности его использования. Также здесь представлены проблемы, связанные с использованием указанного протокола на практике и приведены сведения об областях его применения.

Многораундовый протокол аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма в группе вычетов по простому модулю. Пегги хочет доказать Виктору, что она знает x, являющийся решением уравнения $a^x \equiv b \pmod p$, p – большое простое число, a – первообразный корень по модулю p, x – произвольное натуральное, взаимно простое с $p-1$. Числа a, b, p объявляются открытым идентификатором Пегги и являются общедоступными, а x хранится в секрете у Пегги. Очевидно, что числа a, x, b, p должны быть сгенерированы до начала прохождения аутентификации.

1) Пегги генерирует показатель y, где $1 < y \leq p-2$ и вычисляет образ $h \equiv a^y \pmod p$. Затем Пегги посылает h Виктору.

2) Виктор и Пегги, используя протокол подбрасывания монеты на основе криптосистемы с открытым ключом, совместно генерируют бит q.

3) Исходя из значения q, полученного на предыдущем шаге, Пегги посылает Виктору или $z = y$, если $q = 0$, или $z = yx^{-1}$, если $q = 1$.

4) Виктор проверяет что для q, полученного на шаге 2, истинно сравнение: $a^z \equiv h (\mathrm{mod}\ p)$ для $q = 0$ или $b^z \equiv h (\mathrm{mod}\ p)$ для $q = 1$.

5) Если равенство, составленное Виктором на шаге 4, ложно, то выносится вердикт, что Пегги не знает секретный показатель x. Если же равенство верно, то Виктор может по своему желанию попросить Пегги повторить этапы протокола еще раз, или принять решение о том, что Пегги знает секретный показатель x. ■

В разделе 4 приведен пример работы программного комплекса, с помощью которого можно провести описанный выше протокол.

Программный комплекс разработан на языке C# и включает в себя три составляющих компонента, а именно: реализация основного функционала криптосистемы RSA, реализация вспомогательных функция для проведения протокола подбрасывания монеты на основе криптосистемы с открытым ключом и основные этапы многораундового протокола аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма в группе вычетов по простому модулю.

Все программы работают с файлами и для их использования необходимо наличия протокола для обмена файлами.

К реализованному функционалу криптосистемы RSA относится генерация модуля, генерация ключей по заданному модулю и шифрование\дешифрование файлов.

Для проведения протокола подбрасывания монеты создан программный модуль, позволяющий создавать стороны монеты в виде двух файлов, один для «решки», второй для «орла». В этом же модуле

предусмотрена вспомогательная функция генерации случайного бита, на основе которого пользователь сделает свой случайный выбор.

В программном обеспечении протокола аутентификации реализованы следующие шаги:

1) Шаг 1. Генерация случайного показателя y на основе известных открытых параметров логарифма, которые подаются на вход в виде файла. На основе полученного y программа вычисляет h. Оба полученных значения сохраняются в соответствующие файлы.

2) Шаг 3. Вычисление z на основе полученного ранее случайного бита q и вычисленного на 1-ом шаге y. z также сохраняется в файл.

3) Шаг 4. Проверка знания дискретного логарифма на основе вычисленного ранее бита q и представленных в виде файлов h, z, открытых параметрах логарифма.

Три описанных выше модуля приведены в соответствующих подразделах 4.1 «Программное обеспечение криптосистемы RSA», 4.2 «Программное обеспечение протокола подбрасывания монеты на основе криптосистемы с открытым ключом» и 4.3 «Программное обеспечение протокола аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма».

В подразделе 4.4 приведен пример проведения аутентификации с помощью разработанного программного комплекса.

Для реализации шага 2 протокола аутентификации, в котором вычисляется случайный бит, используется протокол подбрасывания монеты на основе криптосистемы с открытым ключом, в качестве которой была выбрана система RSA.

На рисунке 26 приведен интерфейс программы, отвечающий за реализацию 1-го шага протокола аутентификации.

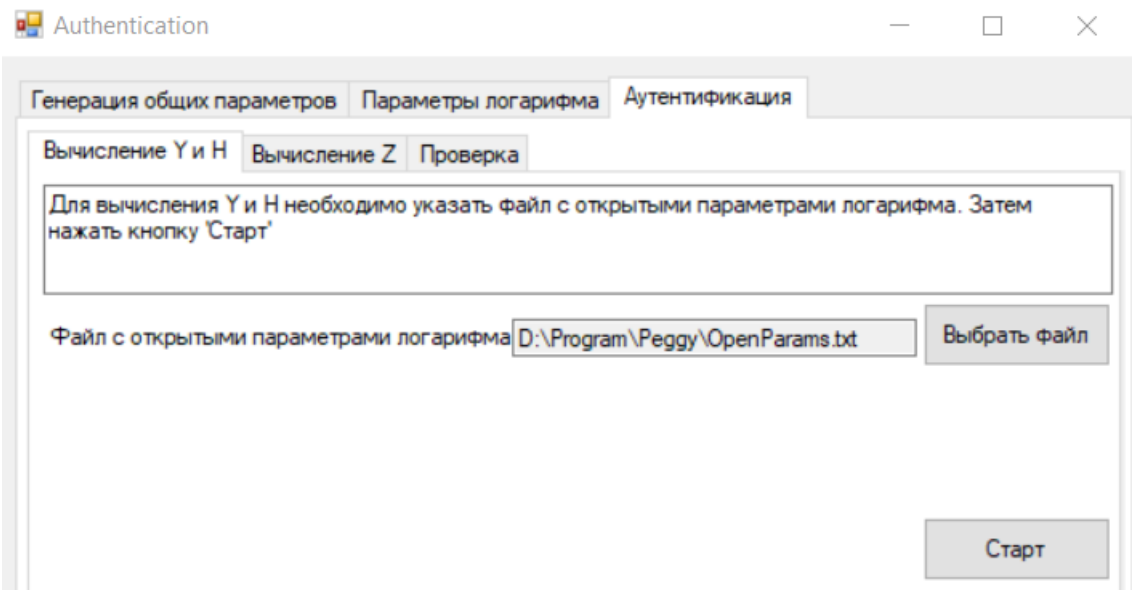

Рисунок 26 – Создание Y и вычисление H

На рисунке 36 приведен процесс создания файлов-сторон монеты.

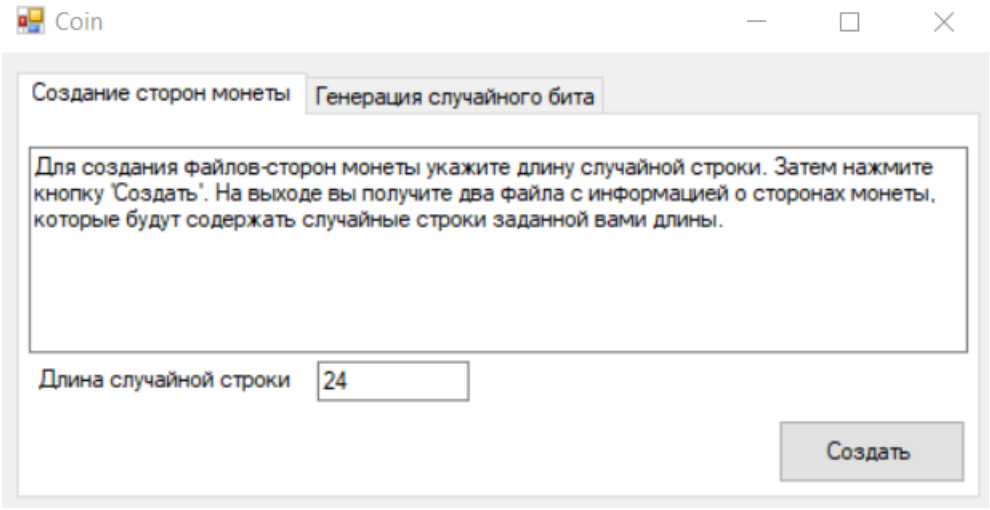

Рисунок 36 – Создание файлов-сторон монеты

На рисунке 37 результат создания файлов-сторон монет.

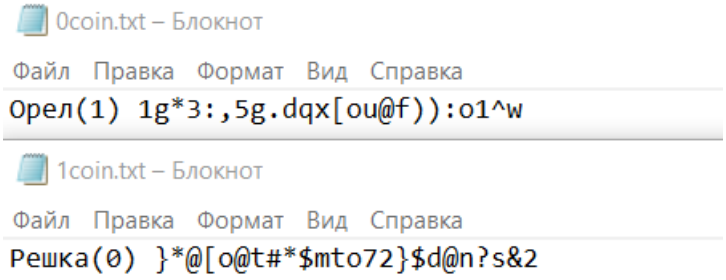

Рисунок 37 – Файлы-стороны монеты

На рисунке 41 показан процесс шифрования файла-стороны монеты на открытом ключе претендента на третьем шаге протокола подбрасывания монеты.

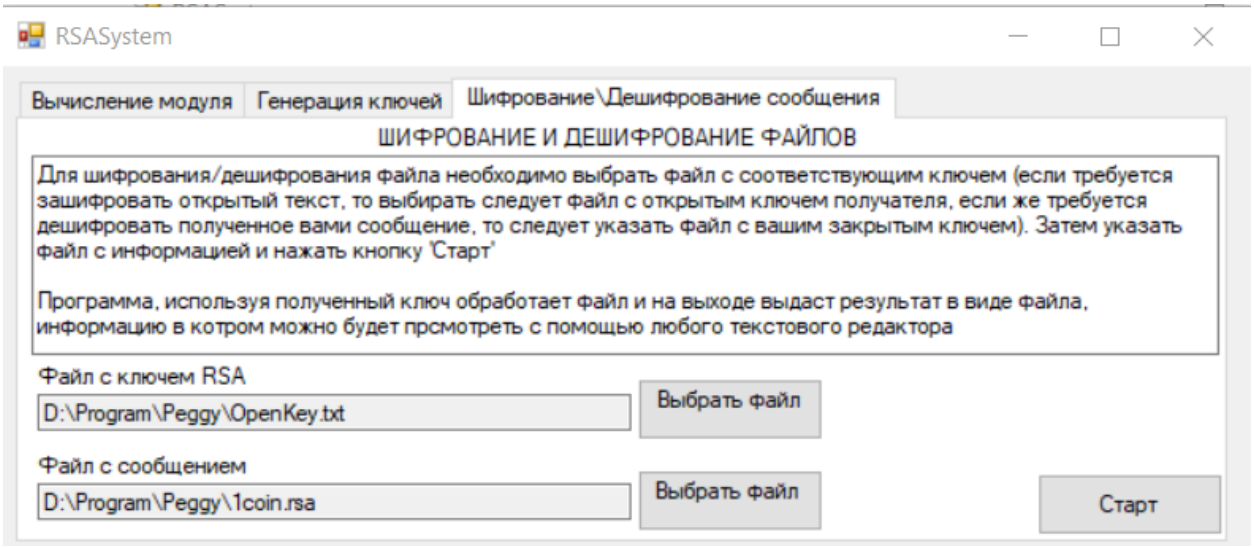

Рисунок 41 – Выбор файла и его шифрование претендентом на третьем шаге протокола подбрасывания монеты

На рисунке 46 приведен результат броска монеты.

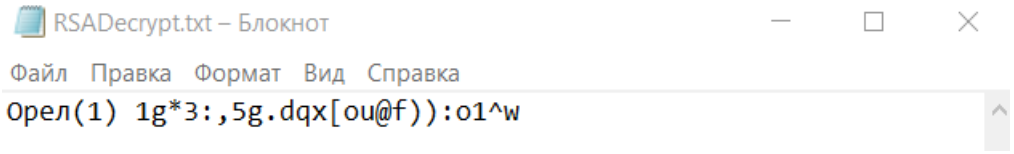

Рисунок 46 – Итоговое значение броска монеты, полученное на пятом шаге

На рисунке 47 приведен процесс вычисления ответа верификатору.

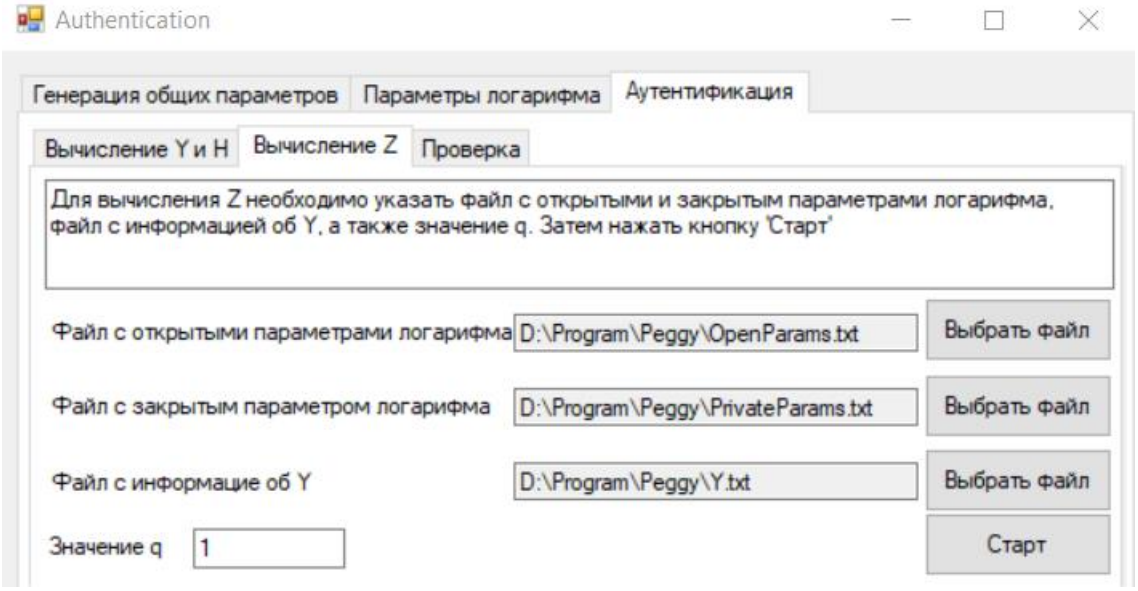

Рисунок 47 – Процесс вычисления *Z*

На рисунке 49 приведен процесс проверки верификатором файлов, полученных от претендента.

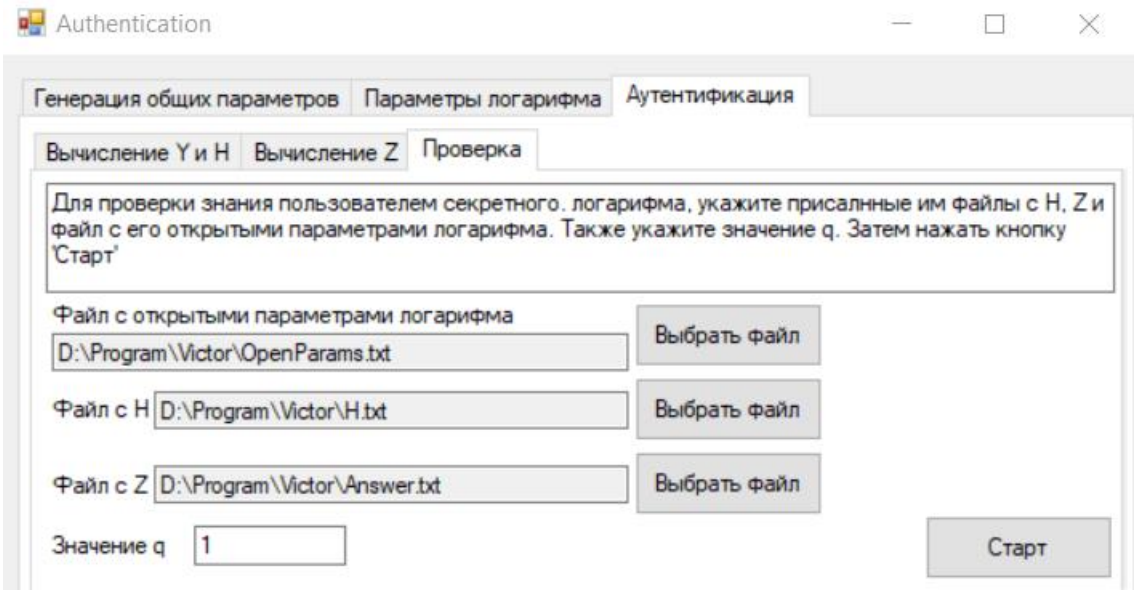

Рисунок 49 – Процесс проверки данных претендента

Если все файлы указаны верно и в них содержится корректная и правильная информация, то программа сообщит об успешном прохождении аккредитации аутентификации, рисунок 50.

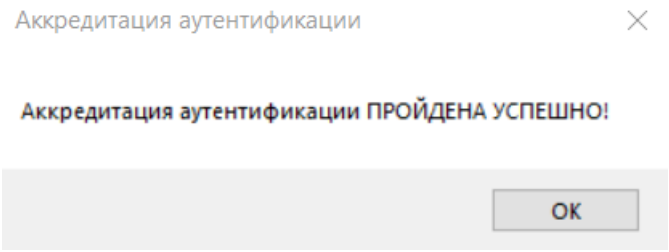

Рисунок 50 – Результат работы программы, если информация, полученная от претендента верная

Если указаны неверные файлы или информация в них некорректная, то аккредитацию протокола не будет пройдена, о чем программа сообщит, рисунок 51.

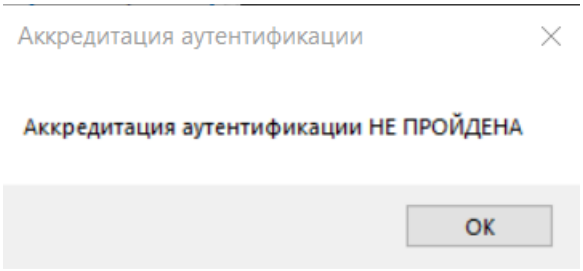

Рисунок 51 – Результат работы программы, если претендент не знает секретный логарифм

Если в процессе работы возникнет ошибка, к примеру, на вход подан файл с некорректной информацией, то программа сообщит об этом с описанием ошибки, рисунок 52.

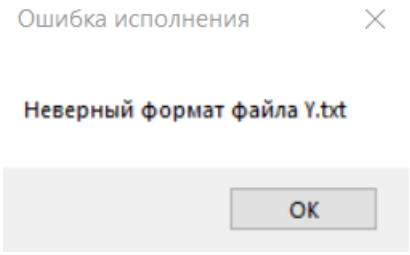

Рисунок 52 – Информационное окно об ошибке

ЗАКЛЮЧЕНИЕ

В данной работе была рассмотрена возможности применения доказательства с нулевым разглашением знания дискретного логарифма в качестве протокола аутентификации. Разработано программное обеспечение на языке C#, реализующее основные этапы протокола аутентификации на основе доказательства с нулевым разглашением знания дискретного логарифма. Таким образом, все поставленные задачи выполнены.

Рассмотренный в данной работе протокол аутентификации может использоваться во многих задачах, существенно не уступая другим схемам аутентификации. Это обусловлено тем, что при аутентификации с помощью доказательства с нулевым разглашением отсутствие раскрытия какой-либо информации о секрете достигается путем увеличения интерактивности протокола. С другой стороны информация о секрете сама по себе не является громоздкой, что дает существенное преимущество в использовании данного протокола в системах, где есть ограничение на количество хранимой информации, необходимой для аутентификации.

Плюсами данного протокола является существенный уровень защиты претендента при аутентификации и создании ключей.

К минусам данного протокола можно отнести большее время работы протокола по сравнению с другими, более распространенными, схемами аутентификации.