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

Подписи, подтверждаемые доверенным лицом

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Лукина Виталия Олеговича

Научный руководитель

к. ф.-м. н., доцент _____ В. Е. Новиков

22.01.2022 г.

Заведующий кафедрой

д. ф.-м. н., доцент _____ М. Б. Абросимов

22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

В современном мире, без использования криптографии, невозможно решить задачи по обеспечению безопасности информации, связанных с целостностью, аутентификацией и невозможностью отказа сторон от авторства.

Подпись от руки тысячелетиями используется для доказательства авторских прав или для выражения согласия с документом. В связи с этим подпись должна удовлетворять следующим требованиям:

1. Подпись должна быть достоверна, она должна убеждает получателя в том, что человек, подписавший документ, сделал это сознательно;

2. Подпись должна быть трудно подделываемой, она должна убеждать получателя в том, что именно подписавший, и никто другой, сознательно подписал документ;

3. Подпись должна быть такой, что её невозможно использовать повторно. Она — часть документа, и мошенник не должен иметь возможность перенести подпись в другой документ;

4. Подписанный документ должен быть неизменяемым;

5. От подписи должно быть невозможно отречься. Подпись и документ материальны. Впоследствии человек, подписавший документ, не сможет утверждать, что документ подписан не им.

В действительности, ни одно из этих требований нельзя назвать бесспорно выполнимым. Подписи подделываются, переводятся с одного листа бумаги на другой, документы изменяются после подписания, однако мы миримся с этими проблемами из-за того, что действия мошенника затруднены и он рискует быть разоблаченным.

В наше время, когда большая часть документооборота, торговых сделок и финансовых переводов происходят в компьютерах или с их помощью. Появление электронной цифровой подписи обусловлено необходимостью заменить привычную подпись от руки в угоду технологическому прогрессу, но при этом сохранив и улучшив ее основные черты.

Электронные цифровые подписи на сегодняшний день широко применяются в разных сферах общественной жизни, например:

1. Банковских платежных системах;
2. Электронная коммерция;
3. Электронный документооборот;
4. Участие в электронных торгах;
5. Подтверждение авторства;
6. Работа с государственными информационными системами;
7. Ключевой компонент сделок, связанных с криптовалютами.

Такое широкое распространение электронных цифровых подписей, обусловлено тем, что алгоритмы электронных цифровых подписей имеют множество модификаций, отвечающих различным требованиям.

Целями данной дипломной работы являются:

1. Изучение математических основ алгоритмов электронной подписи;
2. Изучение теоретических основ электронных подписей;
3. Рассмотрение модификаций электронных подписей;
4. Изучение подписи, подтверждаемой доверенным лицом;

Разработка программного обеспечения для проведения и проверки подписи, подтверждаемой доверенным лицом.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 67 страниц, из них 44 страницы – основное содержание, включая 31 рисунок, список использованных источников из 12 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел содержит необходимые математические основы, на которые опираются протоколы электронных цифровых подписей. В данном разделе приводятся основные определения, теоремы и математические алгоритмы, используемые в дипломной работе.

Второй раздел включает в себя базовые определения, необходимые для понимания принципов работы электронных цифровых подписей, также в данном разделе выделены основные задачи, которые могут быть решены с помощью электронных цифровых подписей, рассмотрены существующие подходы к созданию электронных цифровых подписей и основные модификации подписей.

Ключ электронной подписи (закрытый ключ) — уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Электронная цифровая подпись — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи, принадлежность подписи владельцу сертификата ключа подписи, а в случае успешной проверки подтвердить факт подписания электронного документа.

Наиболее распространенная технология электронной подписи основана на ассиметричном шифровании с открытым ключом и опирается на следующие принципы:

1. Можно сгенерировать пару очень больших чисел (открытый и закрытый ключ) так, чтобы, зная открытый ключ, было невозможно вычислить

закрытый ключ за приемлемое время, и при этом механизм генерации ключей является общеизвестным, и каждому открытому ключу соответствует конкретный закрытый ключ. Если, например, Алиса публикует свой открытый ключ, то можно быть уверенным, что соответствующий закрытый ключ есть только у неё;

2. Существуют оптимальные по сложности и надежности методы шифрования. Они позволяют зашифровать сообщение закрытым ключом так, что расшифровать его можно только парным открытым ключом;

3. Если электронный документ расшифровывается с помощью открытого ключа, то с уверенностью можно сказать, что он был зашифрован с помощью парного закрытого ключа. Если документ расшифрован с помощью открытого ключа Алисы, то это подтверждает её авторство: зашифровать данный документ могла только она, так как она является единственным обладателем закрытого ключа.

В первом подразделе приведены описание и основная идея групповой подписи, протокол реализующий групповую подпись, описана проблема безопасности, заключающаяся в необходимости надежного арбитра.

Во втором подразделе приведены описание и основная идея неоспоримой подписи, описано основное отличие неоспоримой подписи от обычной подписи, которое состоит в том, что подлинность неоспоримой подписи может подтвердить только её автор, что является в некоторых случаях преимуществом, а в некоторых недостатком.

В третьем подразделе приведены описание и основная идея слепой подписи, протокол реализующий слепую подпись, описано главное требование к используемым в протоколе функциям, для корректной работы они должны быть коммутативны.

В четвертом подразделе приведены описание и основная идея доверенной подписи, выделены требования, представляемые безопасной

доверенной подписи, рассмотрена общая схема протокола доверенной подписи.

В третьем разделе представлено теоретическое описание протокола подписи, подтверждаемой доверенным лицом, преимущества, характерные для данного протокола. Также в этом разделе изложен сам протокол подписи, подтверждаемой доверенным лицом и проверена его корректность.

Подпись, подтверждаемая доверенным лицом — это своеобразный компромисс между обычными цифровыми подписями и неоспоримыми подписями. Например, в некоторых случаях Алисе необходимо ограничить круг лиц, имеющих возможность подтверждать подлинность ее подписи. С другой стороны, наличие у Алисы полного контроля подрывает саму возможность использование подписей. Например, Алиса может отказаться сотрудничать как в подтверждении, так и в отрицании подписи, она может заявить об утрате ключей для подтверждения или отрицания, Алисы, в конце концов, просто может не оказаться на месте. Подписи, подтверждаемые доверенным лицом, могут обеспечить Алисе защиту, предоставляемую неоспоримыми подписями, и вместе с тем не позволят ей злоупотреблять этой защитой. Также данный вид подписи может защитить Алису, если она, в самом деле, утратила свой ключ.

Идея данного вида подписи состоит в возможности Алисе подписать сообщение и Бобу проверить её подпись так, чтобы Кэрол (доверенное лицо Алисы) немного позже могла доказать Дэйву (третьему лицу) правильность подписи Алисы.

Следующий протокол реализует подпись, подтверждаемую доверенным лицом:

Генерация общих параметров.

p — больше простое число, g — примитивный корень по модулю p, n — произведение двух различных простых чисел, отличных от p.

Генерация индивидуальных параметров.

x — закрытый ключ Алисы, где $1 < x < n$. $a = g^x \bmod p$ — открытый ключ Алисы. z — закрытый ключ Кэрол, где $1 < z < n$. $h = g^z \bmod p$ — открытый ключ Кэрол.

Генерация подписи.

Алиса отправляет Бобу $\{M, a, b, j\}$, где $a = g^x \bmod p$, $b = h^x \bmod p$, $H(M)$ — хеш-значение от M, $H(a,b)$ — хеш-значение от конкатенации a и b, и $j = \left(H(M) \oplus H(a,b)\right)^3 \bmod n$.

Проверка подписи Бобом.

1. Боб выбирает два случайных числа s и t, таких, что $1 < s, t < p$ и посылает Алисе: $c = g^s h^t \bmod p$;

2. Алиса выбирает случайное значение q, такое, что $1 < q < p$ и посылает Бобу: $d = g^q \bmod p$, $e = (cd)^x \bmod p$;

3. Боб посылает Алисе s и t;

4. Алиса проверяет, что: $g^s h^t = c \bmod p$;

5. Алиса посылает Бобу q;

6. Боб проверяет $d \equiv g^q \bmod p$, $ea^{-q} \equiv a^s b^t \bmod p$, $\left(H(M) \oplus H(a,b)\right)^3 \equiv j \bmod n$.

Если все три тождества выполняются, то Боб считает подпись истинной.

Боб не может использовать запись этого доказательства для убеждения Дэйва в истинности подписи, но Дэйв может выполнить протокол с доверенным лицом Алисы Кэрол, которая уполномочена подтверждать ее подпись. Вот как Кэрол убеждает Дэйва в том, что a и b образуют правильную подпись.

Проверка подписи Дэйвом с помощью Кэрол.

1. Дэйв выбирает случайные u и v, такие, что $1 < u, v < p$ и посылает Кэрол: $k = g^u a^v \bmod p$;

2. Кэрол выбирает случайное значение w, где $1 < w < p$ и посылает Дэйву: $l = g^w \bmod p$, $y = (kl)^z \bmod p$;

3. Дэйв посылает Кэрол u и v;

4. Кэрол проверяет, что: $g^u a^v \equiv k \bmod p$, затем она посылает Дэйву w;

5. Дэйв проверяет, что: $g^w \equiv l \bmod p$, $yh^{-w} \equiv h^u b^v \bmod p$

Если оба тождества верны, то Дэйв считает подпись истинной.

Проверим корректность протокола, для этого рассмотрим сравнение:

$$ea^{-q} \equiv a^s b^t \bmod p$$

Так как $e = (cd)^x \bmod p$, то сравнение можно переписать следующим образом.

$$(cd)^x a^{-q} \equiv a^s b^t \bmod p$$

В новом сравнении $c = g^s h^t \bmod p$ и $d = g^q \bmod p$, отсюда получаем следующее сравнение.

$$(g^s h^t g^q)^x a^{-q} \equiv a^s b^t \bmod p$$

Преобразуем сравнение, для этого поменяем местами показатели степеней, внесем x в скобки, а s, t, q вынесем за скобки.

$$(g^x)^s (h^x)^t (g^x)^q a^{-q} \equiv a^s b^t \bmod p$$

Так как $g^x = a \bmod p$, а $h^x = b \bmod p$, получаем:

$$a^s b^t a^q a^{-q} \equiv a^s b^t \bmod p$$

Так как $a^q a^{-q} \equiv 1 \bmod p$, получаем:

$$a^s b^t \equiv a^s b^t \bmod p$$

Следовательно, рассмотренный протокол подписи, подтверждаемой доверенным лицом корректен.

В четвертом разделе приводится описание реализованной в ходе выполнения дипломной работ программы, написанной на языке

программирования C#, также данный раздел включает в себя скриншот графического интерфейса главного окна программы.

В первом подразделе четвертого раздела продемонстрирована программная реализация генерации общих параметров системы, индивидуальных параметров автора подписи и доверенного лица, а также подпись документа.

Во втором подразделе продемонстрирована программная реализация интерактивного алгоритма проверки подписи автором и пользователем. Представлены скриншоты сгенерированных, в процессе выполнения алгоритма, параметров и результат проверки подписи.

В третьем подразделе продемонстрирована программная реализация интерактивного алгоритма проверки подписи доверенным лицом и пользователем. Представлены скриншоты сгенерированных, в процессе выполнения алгоритма, параметров и результат проверки подписи.

Полный листинг программы приведен в приложении А.

ЗАКЛЮЧЕНИЕ

В данной дипломной работе изложены математические основы алгоритмов электронной подписи.

Изучены теоретические основы электронных подписей и их модификаций, такие как групповая, неоспоримая, слепая, доверенная подпись, а также подпись, подтверждаемая доверенным лицом.

Проверена корректность протокола подписи, подтверждаемой доверенным лицом.

Реализовано программное обеспечение для проведения протоколов подписи и проверки подписи, подтверждаемой доверенным лицом.

Таким образом все поставленные в работе цели полностью выполнены.