МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №10 НА ТЕМУ:**

**Исследование алгоритмов генерации и верификации электронной цифровой подписи**

Выполнил студент 3 курса 1 группы

Кашперко Василиса Сергеева

2023 г.

**Цель:** изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

**Теоретические сведения**

Математические основы асимметричных шифров

Электронная цифровая подпись (ЭЦП) – важный элемент современных информационных систем, использующих методы и технологии криптографического преобразования информации.

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

• аутентифицирование лица, подписавшего сообщение;

• контроль целостности подписанного сообщения;

• защита сообщения от подделок;

• доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшие отличительные особенности ЭЦП:

• ЭЦП представляет собой бинарную последовательность

(в отличие от графического образа, каковым является подпись от руки);

• указанная бинарная последовательность зависит от содержания подписываемого сообщения.

Основным компонентом в технологии ЭЦП является ключ.

В соответствии с этим обстоятельством перечисленные выше функции ЭЦП могут быть реализованы на основе классических методов зашифрования/расшифрования:

• на основе симметричных систем (с тайным ключом);

• на основе симметричных систем и посредника;

• на основе асимметричных систем (с открытым ключом).

Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа.

ЭЦП на основе хешей подписываемых сообщений

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь ), а его хеша, H(), что позволяет:

– сокращает время генерации/верификации подписи;

– снизить вероятность ошибок в итоговом документе.

Общая структура подписанного документа – – представляет конкатенацию этого документа и ЭЦП *S*. И еще может конкатенироваться служебная информация (дата, время отправки, информация об отправителе).

Важное свойство цифровой подписи: её может проверить каждый, кто имеет доступ к *открытому ключу* её автора.

Если – подпись подлинная и документ целостный, что значит, что где – полученный документ, – исходный документ.

При генерации ЭЦП (по классической схеме) для сообщения *М* отправитель последовательно выполняет следующие действия:

– вычисляет хеш (хеш-образ) сообщения *М*: *Н*(*М*);

– вычисляет содержание ЭЦП (собственно ЭЦП *S*) по хешу *Н(М)* с использованием своего закрытого ключа *d*: *S* = (*Н*(*М*));

– присоединяет (конкатенирует) ЭЦП к сообщению М и некоторой служебной информации, создавая таким образом итоговое сообщение *М'*;

–  посылает сообщение *М'* получателю;

Получив сообщение *М'*, другая сторона последовательно выполняет следующие действия:

– отделяет цифровую подпись *S* от сообщения *М* (для общего случая применим одинаковые символьные обозначения);

– применяет к сообщению М операцию хеширования, используя ту же функцию, что и отправитель, и получает хеш-образ полученного сообщения;

– используя открытый ключ отправителя, расшифровывает S, т. е. извлекает из ЭЦП хеш-образ отправленного сообщения;

– проверяет соответствие (равенство) обоих хеш-образов, и если они совпадают, то отправитель действительно является тем, за кого себя выдает, а сообщение при передаче не подверглось искажению.

Необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом.

**Практическая часть**

В ходе лабораторной работы было разработано авторское оконное приложение в соответствии с целью лабораторной работы. При этом были использованы результаты выполнения предыдущих лабораторных работ, а также доступные библиотеками и программные коды.

Приложение реализует следующие операции:

• генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра;

• оценку времени выполнения указанных процедур при заданных ключевых параметрах.

*ЭЦП на основе RSA*

Может рассматриваться 2 ситуации:

1) сообщение подписывается и передается в открытом (незашифрованном) виде;

2) сообщение подписывается и передается в зашифрованном виде.

Первый случай соответствует схеме и операциям рис. 1 и рис. 2, а подпись *S* вычисляется на основе соотношения, представленного ниже



и – элементы тайного ключа отправителя. Передаваемое сообщение *М'* = ||*S*.

Получатель анализирует сообщение ||*S*. Расшифровывает по формуле, приведенной ниже



Далее вычисляется *Н* (). Если *H* () = *H* (), подпись верифицирована. На рисунке 5 приведен пример, когда полученный документ не претерпел никаких изменений и его хеш совпал с хешем, полученным из ЭЦП.

Если подписываемое сообщение *М*(*М'*) также должно передаваться в зашифрованном виде, то обычно *М'* шифруется на стороне отправителя стандартным образом: с помощью открытого ключа получателя ( и ), который перед основным процессом верификации подписи расшифровывает послание своим тайным ключом: и . Далее осуществляются вычисления и анализ, как и в первом случае.

Если делать анализ времени зашифрования и расшифрования, то можно отметить, что время зашифрования меньше, чем время расшифрования, что удовлетворяет условию: «вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом». Время расшифрования варьирует ±1 мс.

*ЭЦП на основе Эль-Гамаля*

1) Алгоритм начинается с того, что мы создаем ключевую информацию.

*p* – простое число;

*g* – случайное число (*g, x* < *p*);

*x –* случайное число (*g, x* < *p*);

вычисляем => ***p, y, g* – открытый ключ**, ***x* – закрытый ключ**

2) **A** шифрует документ ***M*** своим закрытым ключом:

*k –* случайное число, взаимнопростое с (*p* - 1).

Генерируем подпись, состоящую из двух чисел: *а* и *b*, являющиеся цифровой подписью *S =* {*a, b*}*:*

3) **A** отправляет **B** подписанное сообщение: *M*, *a*, *b.*

4) **B** получает *M*, *a*, *b* (сообщение *М'* = ||*S*)и сверяет подпись (рис. 9): подпись принадлежит **A**, если

где – хеш полученного сообщения

*ЭЦП на основе Шнорра*

Является основой ЭЦП Беларуси. Является вариантом алгоритма ЭЦП Эль-Гамаля.

*Особенность*: число *p* должно быть очень большим, чтобы сделать действительно трудную проблему дискретного логарифма (Рекомендуемая длина *p* должна составлять по крайней мере 1024 бита).

Ключевая информация:

*p* – простое число в диапазоне от 512 до 1024 битов;

*q –* 160-битное простое число, делитель (*p* - 1)

*g* – любое число (*g* != 1), такое что

***p, g, q* – открытый ключ** (могут применяться группой пользователей)

*x –* случайное число (*x* < *q*): ***x –* тайный ключ** (секретный ключ имеет длину не менее 160 символов)

Для *подписи сообщения*  выбираем случайное число *k* (1 < *k* *< q*) и вычисляем параметр *a* (Рис.13):

Далее вычисляется хеш от конкатенации сообщения и числа *a: h = H(*||*a).*

*! Хеш-функция непосредственно не применяется к сообщению.*

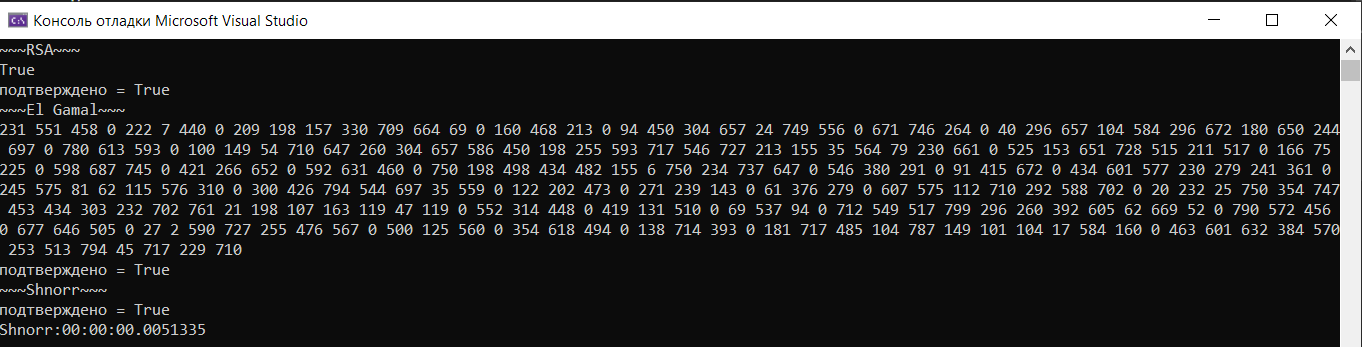
Создается хеш-образ подписываемого сообщения, спереди присоединенного к числу *a.*

Далее вычисляется значение *b:*

Получателю отправляются: *М'* = ||*S; S =* {*h, b*}

Для проверки подписи получатель вычисляет

Затем он проверяет выполнение равенства: *h* = *H(*||*X).* Подпись достоверна, если равенство выполняется.



Выше приведен результат работы программы.

**Вывод:** мы провели лабораторную работу, в ходе которой исследовали методы создания и проверки электронной цифровой подписи (ЭЦП). Кроме того, мы разработали приложение, которое наглядно демонстрирует процесс вычисления ЭЦП и проверки целостности данных.

**Контрольные вопросы**

*1. Дать определение ЭЦП.*

**Электронная цифровая подпись** – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа.

*2. Охарактеризовать основные функции ЭЦП.*

• аутентифицирование лица, подписавшего сообщение;

• контроль целостности подписанного сообщения;

• защита сообщения от подделок;

• доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

*3. В чем заключаются сходства и различия между собственноручной и электронной подписью?*

ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

• аутентифицирование лица, подписавшего сообщение;

• контроль целостности подписанного сообщения;

• защита сообщения от подделок;

• доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшие отличительные особенности ЭЦП:

• ЭЦП представляет собой бинарную последовательность

(в отличие от графического образа, каковым является подпись от руки);

• указанная бинарная последовательность зависит от содержания подписываемого сообщения.

*4. Охарактеризовать основные способы реализации ЭЦП.*

В соответствии с этим обстоятельством перечисленные выше функции ЭЦП могут быть реализованы на основе классических методов зашифрования/расшифрования:

• на основе симметричных систем (с тайным ключом);

• на основе симметричных систем и посредника;

• на основе асимметричных систем (с открытым ключом).

*5. Имеется ли различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных (ЭЦП) сообщений?*

Да, имеется.При передаче зашифрованных сообщений используется ключ для зашифрования сообщения таким образом, чтобы его могли расшифровать только те, у кого есть ключ для расшифровки. Ключ для шифрования и ключ для расшифровки могут быть различными. Это означает, что отправитель использует ключ для шифрования сообщения перед его отправкой, а получатель использует свой ключ для расшифровки сообщения при его получении.

При передаче подписанных сообщений используется ключ для создания цифровой подписи сообщения, которая может быть проверена на подлинность и целостность сообщения. При создании цифровой подписи используется частный ключ отправителя, который должен быть известен только ему, а при проверке подписи используется открытый ключ отправителя, который может быть известен всем. Если цифровая подпись верифицируется, то можно считать, что сообщение не было изменено и его отправитель подлинный.

*6. Охарактеризовать криптостойкость ЭЦП на основе RSA, схемы Эль-Гамаля, схемы Шнорра, а также на основе DSA.*

Криптостойкость ЭЦП основанной на алгоритме RSA, схеме Эль-Гамаля, схеме Шнорра и DSA, зависит от длины ключа и качества генерации случайных чисел.

RSA: RSA является одним из самых широко используемых алгоритмов ЭЦП. Криптостойкость ЭЦП на основе RSA зависит от сложности факторизации больших чисел на простые множители. Для достижения достаточной криптостойкости, длина ключа RSA должна быть не менее 2048 бит. Однако, с учетом быстрого развития вычислительной техники, в будущем рекомендуется использовать более длинные ключи RSA.

Схема Эль-Гамаля: Схема Эль-Гамаля основана на сложности дискретного логарифмирования. Криптостойкость ЭЦП на основе этой схемы также зависит от длины ключа. Рекомендуется использовать ключи длиной не менее 2048 бит.

Схема Шнорра: Схема Шнорра также основана на сложности дискретного логарифмирования. Она обладает преимуществами перед RSA и схемой Эль-Гамаля в том, что она имеет более короткие ключи при той же криптостойкости. Однако, криптостойкость ЭЦП на основе схемы Шнорра также зависит от длины ключа. Рекомендуется использовать ключи длиной не менее 256 бит.

DSA: DSA основана на сложности дискретного логарифмирования в конечных полях. Криптостойкость ЭЦП на основе DSA также зависит от длины ключа. Рекомендуется использовать ключи длиной не менее 2048 бит.

*7. Какие элементы составляют ключевую информацию алгоритмов реализации ЭЦП, перечисленных в вопросе 6?*

Ключевая информация включает в себя параметры, используемые для генерации открытого и секретного ключей, а также сами открытый и секретный ключи. Открытый ключ является публичной информацией и может быть распространен широко. Секретный ключ, с другой стороны, должен храниться в безопасном месте и использоваться только владельцем ключа для подписи сообщений.

Важно отметить, что безопасность ЭЦП напрямую зависит от безопасности ключей. Поэтому генерация ключей должна быть проведена с учетом рекомендаций по безопасности и должна выполняться с помощью криптографически надежных методов. Кроме того, секретные ключи должны быть защищены от несанкционированного доступа, например, с помощью шифрования или использования физических устройств, таких как смарт-карты или USB-ключи.

*8. Дать сравнительные характеристики схемам ЭЦП, перечисленным в вопросе 6.*

**RSA:**

* Прост в реализации и широко используется;
* Быстрый алгоритм шифрования и расшифрования;
* Длина ключа может быть очень большой, что обеспечивает высокий уровень безопасности;
* Использование RSA для ЭЦП требует большой вычислительной мощности.

**Схема Эль-Гамаля:**

* Меньше вычислительной сложности, чем RSA;
* Имеет более высокую стойкость к атакам на основе квантовых вычислений, чем RSA;
* Длина ключа должна быть больше, чем в RSA, для обеспечения такого же уровня безопасности.

**Схема Шнорра:**

* Характеризуется высокой эффективностью и высоким уровнем безопасности;
* Обладает сравнительно небольшой длиной подписи и ключа, что делает его полезным для систем с ограниченными ресурсами.

**DSA:**

* Быстрый алгоритм подписи и проверки подписи;
* Меньшая длина ключа, чем RSA и Эль-Гамаля, при сохранении высокого уровня безопасности;
* Не поддерживает шифрование, только подпись.
* Выбор конкретной схемы ЭЦП зависит от требований к безопасности и эффективности, а также от особенностей конкретного применения.

*9. Охарактеризовать особенности государственного стандарта ЭЦП в Республике Беларусь.*

Государственный стандарт РБ определяет понятие ЭЦП в следующем виде:

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.