Учреждение образования

«Белорусский государственный технологический университет»

**Основы информационной безопасности**

**Лабораторная работа №7**

**«Электронно-цифровая подпись»**

Выполнил:

Студент 2 курса 2 группы ФИТ

Мойсеёнок Денис

Преподаватель:

Ржеутская Надежда Викентьевна

Минск 2025

**Цель**: изучить и закрепить умение реализации электронно-цифровой подписи на примере RSA.

**Вопросы:**

1. Дайте определение понятию «электронная цифровая подпись».

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

2. Объясните порядок использования ключей (открытый, закрытый) при отправке и проверке ЭЦП.

В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи - открытый ключ отправителя. Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания.

3. Перечислите специальные схемы ЭЦП.

Наиболее известные схемы создания электронной цифровой подписи:

– Диффи – Хеллмана;

− DSA;

− RSA;

− Эль-Гамаля (ElGamal);

− Рабина;

− Шнорра;

− Диффи – Лампорта.

4. Назовите недостатки алгоритма цифровой подписи RSA

Недостатки алгоритма цифровой подписи RSA:

* При вычислении ключей для системы цифровой подписи RSA необходимо проверять ряд дополнительных условий. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение.
* Для обеспечения криптостойкости цифровой подписи RSA по отношению к попыткам фальсификации, например, на уровне алгоритма шифрования DES, необходимо использовать при вычислениях ключей очень большие целые числа, что требует значительных вычислительных затрат, превышающих на 20–30% вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости.
* Цифровая подпись RSА уязвима к так называемой мультипликативной атаке. Иначе говоря, алгоритм цифровой подписи RSA позволяет злоумышленнику без знания секретного ключа сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов.

**Задания:**

1. Объясните последовательность выполнения процедур генерации и проверки ЭЦП.

* Сначала пользователь А вычисляет числа по формуле, т. е. шифрует сообщение своим закрытым ключом:

В результате этих действий пользователь А подписывает сообщение.

* Затем пользователь А вычисляет числа по формуле, т. е. шифрует то, что получилось на шаге 1, открытым ключом пользователя Б:

На этом этапе сообщение шифруется, чтобы никто посторонний не мог его прочитать.

* Последовательность чисел передается пользователю Б.
* Пользователь Б получает и вначале вычисляет последовательность числа по формуле, используя свой закрытый ключ

При этом сообщение расшифровывается.

* Затем пользователь Б определяет числа по формуле, используя открытый ключ пользователя A:

За счет выполнения этого этапа проводится проверка подписи пользователя A.

2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.

* Сначала пользователь А вычисляет числа по формуле, т. е. шифрует сообщение своим закрытым ключом:
* Затем пользователь А вычисляет числа по формуле, т. е. шифрует то, что получилось на шаге 1, открытым ключом пользователя Б:
* Последовательность чисел передается пользователю Б.
* Пользователь Б получает и вначале вычисляет последовательность числа по формуле, используя свой закрытый ключ
* Затем пользователь Б определяет числа по формуле, используя открытый ключ пользователя A:

3. Опишите схему протокола ЭЦП на основе алгоритма RSA.

− отправитель знает содержание сообщения, которое он подписывает;

− получатель, зная открытый ключ проверки подписи, может проверить правильность подписи полученного сообщения в любое время без какого-либо разрешения и участия отправителя;

− безопасность схемы подписи гарантируется.

При создании цифровой подписи по классической схеме отправитель:

− применяет к исходному сообщению T хеш-функцию h(T) и получает хеш-образ r сообщения;

− вычисляет цифровую подпись s по хеш-образу r с использованием своего закрытого ключа;

− посылает сообщение T вместе с цифровой подписью s получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

− применяет к полученному сообщению T хеш-функцию h(T) и получает хеш-образ h сообщения;

− расшифровывает хеш-образ h′ из цифровой подписи s с использованием открытого ключа отправителя;

− проверяет соответствие хеш-образов h и h′, и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.