Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра «Информационных систем и технологий»**

**Лабораторная работа №12**

Исследование алгоритмов генерации и верификации электронной цифровой подписи

Выполнил:

Студент 3 курса, 10 группы

Баранчук Владислав

Минск, 2021 г.

1. **Практическая часть**

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

ЭЦП на основе RSA.

В отличие от алгоритма шифрования, отправителем здесь является владелец пары, закрытый/открытый ключ. Процедура формирования электронной подписи под сообщением схожа с шифрованием документа, но в степень закрытого ключа d по вычету n возводится не само сообщение или его части, а дайджест сообщения h.

Сообщение m с подписью ЭЦП будет однозначно аутентифицировано. Авторство сообщения может быть установлено и доказано по паре ключей (d, e) с использованием сертификации. Все необходимые свойства подписи описанным алгоритмом обеспечиваются, что же касается криптостойкости метода ЭЦП, то она определяется криптостойкостью используемого асимметричного криптографического метода и функции однонаправленного шифрования. Необходимо отметить также, что само сообщение m передается в открытом виде. Для того, чтобы обеспечить конфиденциальность передаваемой в нем информации, требуется использование дополнительного шифрования по симметричной или асимметричной схеме (при этом шифрование на ключе d конфиденциальности не обеспечит, поскольку сообщение может быть расшифровано открытым ключом e).

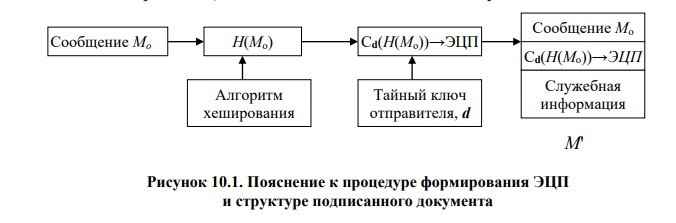


Рис 1.1 – процедура формирования ЭЦП

ЭЦП на основе Эль-Гамаля (ЕGSА).

Идея ЕGSА основана на том, что для обоснования практической невозможности фальсификации цифровой подписи может быть использована более сложная вычислительная задача, чем разложение на множители большого целого числа,- задача дискретного логарифмирования. Кроме того, Эль Гамалю удалось избежать явной слабости алгоритма цифровой подписи RSА, связанной с возможностью подделки цифровой подписи под некоторыми сообщениями без определения секретного ключа.

Рассмотрим подробнее алгоритм цифровой подписи Эль Гамаля. Для того чтобы генерировать пару ключей (открытый ключ - секретный ключ), сначала выбирают некоторое большое простое целое число Р и большое целое число G, причем G < Р. Отправитель и получатель подписанного документа используют при вычислениях одинаковые большие целые числа Р (~10308 или ~21024) и G (~10154 или ~2512), которые не являются секретными.

Отправитель выбирает случайное целое число X, 1 <Х  (Р-1), и вычисляет Y =GX mod Р.

Число Y является открытым ключом, используемым для проверки подписи отправителя. Число Y открыто передается всем потенциальным получателям документов. Число Х является секретным ключом отправителя для подписания документов и должно храниться в секрете.

Для того чтобы подписать сообщение М, сначала отправитель хэширует его с помощью хэш-функции h() в целое число m: m = h(М), 1<m<(Р-1), и генерирует случайное целое число К, 1 < К < (Р -1), такое, что К и (Р-1) являются взаимно простыми. Затем отправитель вычисляет целое число а:

а = GK mod Р и, применяя расширенный алгоритм Евклида, вычисляет с помощью секретного ключа Х целое число b из уравнения m = Х \* а + К \* b (mod (Р-1)).

Пара чисел (а,b) образует цифровую подпись S: S = (а, b), проставляемую под документом М. Тройка чисел (М, а, b) передается получателю, в то время как пара чисел (Х, К) держится в секрете.

После приема подписанного сообщения (М, а, b) получатель должен проверить, соответствует ли подпись S = (а, b) сообщению М. Для этого получатель сначала вычисляет, по принятому сообщению, М число m = h(М),

т.е. хэширует принятое сообщение М.Затем получатель вычисляет значение  
А = Ya ab (mod Р) и признает сообщение М подлинным, если, и только если   
А = Gm (mod Р). Иначе говоря, получатель проверяет справедливость соотношения Ya ab (mod Р) = Gm (mod Р).

Можно строго математически доказать, что последнее равенство будет выполняться тогда, и только тогда, когда подпись S= (а, b) под документом М получена с помощью именно того секретного ключа X, из которого был получен открытый ключ Y. Таким образом, можно надежно удостовериться, что отправителем сообщения М был обладатель именно данного секретного ключа X, не раскрывая при этом сам ключ, и что отправитель подписал именно этот конкретный документ М.

Следует отметить, что выполнение каждой подписи по методу Эль Гамаля требует нового значения К, причем это значение должно выбираться случайным образом. Если нарушитель раскроет когда-либо значение К, повторно используемое отправителем, то он сможет раскрыть секретный ключ Х отправителя.

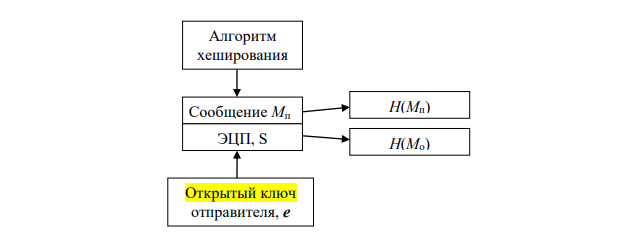


Рис. 2 – Пояснение к алгоритму верификации ЭЦП

Эцп на алгоритме Шнорра.

ЭЦП Шнорра является одной из наиболее эффективных и теоретически обоснованных схем ЭЦП. На ее основе построен стандарт Республики Беларусь СТБ 1176.2-99, южнокорейские стандарты KCDSA и ECKCDSA.

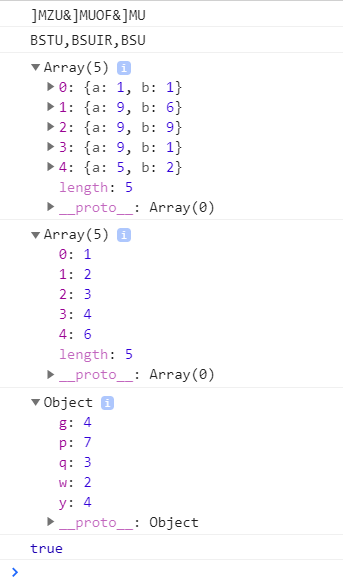


Рис. 1.4 – результат выполнения алгоритмов

**Вывод**

В ходе лабораторной работы были получены знания принципах работы алгоритмов генерации ЭЦП. Изучены алгоритмы RSA, Эль-Гамаля, Шнорра. Так же был реализован программный код, который осуществляет процесс генерации ЭЦП по описанным алгоритмам.