МОСКОВСКИЙ ЭНЕРГЕТИЧЕСКИЙ ИНСТИТУТ (ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)

КАФЕДРА ВЫЧИСЛИТЕЛЬНЫХ МАШИН СИСТЕМ И СЕТЕЙ

Лабораторная работа №1

по курсу «Введение в блокчейн»

Тема: «Цифровая подпись»

Москва 2023

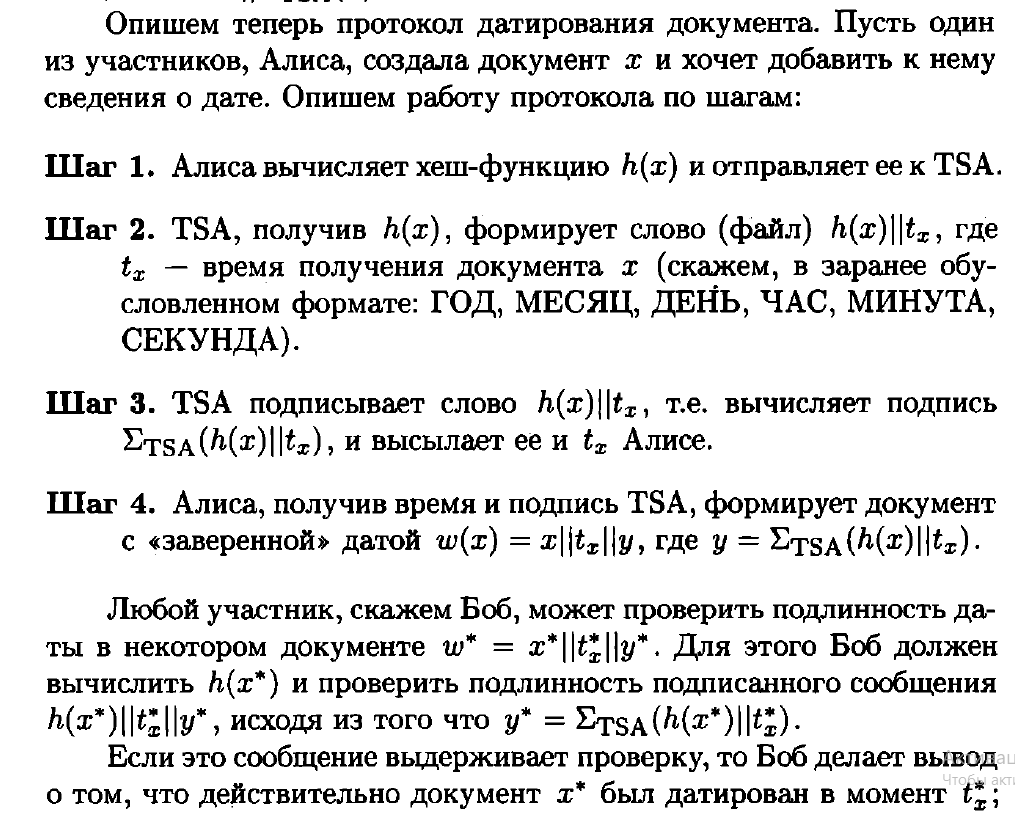
* 1. Теоретическая часть.

NET предоставляет нам следующие хеш-алгоритмы:

* MD5CryptoServiceProvider (Дайджест сообщения 5)
* SHA1CryptoServiceProvider (безопасный алгоритм хеширования с размером ключа 160 бит)
* SHA256Managed (безопасный алгоритм хеширования с размером ключа 256 бит)
* SHA384Managed (безопасный алгоритм хеширования с размером ключа 384 бита)
* SHA512Managed (безопасный алгоритм хеширования с размером ключа 512 бит)
* HMACSHA1 (код аутентификации сообщений на основе хэша с использованием хэш-функции SHA1)
* MACTripleDES (код аутентификации сообщения с использованием TripleDES для входных данных)
* Кроме того, .NET предоставляет нам следующие алгоритмы цифровой подписи:

DSACryptoServiceProvider (Алгоритм цифровой подписи)

RSACryptoServiceProvider (Ривест, Шамир и Адлемен)



Задача №1 (для всех)

Разработать программу (Windows Forms) для создания цифровой подписи и подтверждение подлинности цифровой подписи. Открытые ключи выложить на яндекс диск в виде файлов oKeyFio.pub и в программе загружать открытые ключи из файла. Работу с цифрой подписи оформить в виде отдельного класса или DLL.

Задача №2 (вариант №1)

Подобрать две строки d1 и d2, что у SHA256(d1) и SHA256(d2) совпадают первые 4 байта.

Задача №3 (вариант №2)

Реализовать алгоритм датирования документов TimeStamp протокол. Проверить корректность работы алгоритма

**Электронные ресурсы по теории:**

1. https://www.codeproject.com/Articles/8868/Implementing-Digital-Signing-in-NET