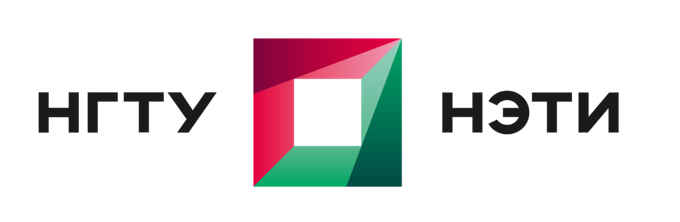
# Министерство науки и Высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное   
учреждение высшего образования

«Новосибирский государственный технический университет»



Кафедра теоретической и прикладной информатики

Лабораторная работа № 7  
по дисциплине «Программные средства защиты информации»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Факультет: | ПМИ |  |  | |
| Группа: | ПМИМ-21 |  |  | |
| Бригада: | 3 | | |  | |
| Студенты: | Бортников. Н, Ефименко А., Кутузова И. | | |  | |
|  |  |  |  | |
| Преподаватель: | Авдеенко Т.В. |  |  | |

Новосибирск

2023

1. **Цель работы**

Изучить различные алгоритмы однонаправленного хэширования данных, основанные на симметричных блочных алгоритмах шифрования.

Ознакомиться со схемами цифровой подписи и получить навыки создания и проверки подлинности электронной цифровой подписи.

1. **Формулировка задания**

I. Реализовать приложение, позволяющее вычислять и проверять ЭЦП, сформированную по алгоритмам RSA и Эль-Гамаля.

II. С помощью реализованного приложения выполнить следующие задания:

1. Протестировать правильность работы разработанного приложения.

2. Для заданных в варианте открытых ключей пользователя проверить подлинность подписанных по алгоритму RSA хэш-значений некоторых сообщений .

3. Абоненты некоторой сети применяют подпись Эль-Гамаля с известными общими параметрами и . Для указанных в варианте секретных параметров абонентов найти открытый ключ и построить подпись для хэш-значения некоторого сообщения . Проверить правильность подписи.

4. Выполнить задание, аналогичное пункту II.2, но для чисел, больших 264

5. Выполнить задание, аналогичное пункту II.3, но для чисел, больших 264

6. Сделать выводы о проделанной работе.

1. **Описание разработанного программного средства**

Решение задачи реализовано в виде программы, написанной на языке C#. Интерфейс, через который осуществляется работа с ней, имеет следующий вид:

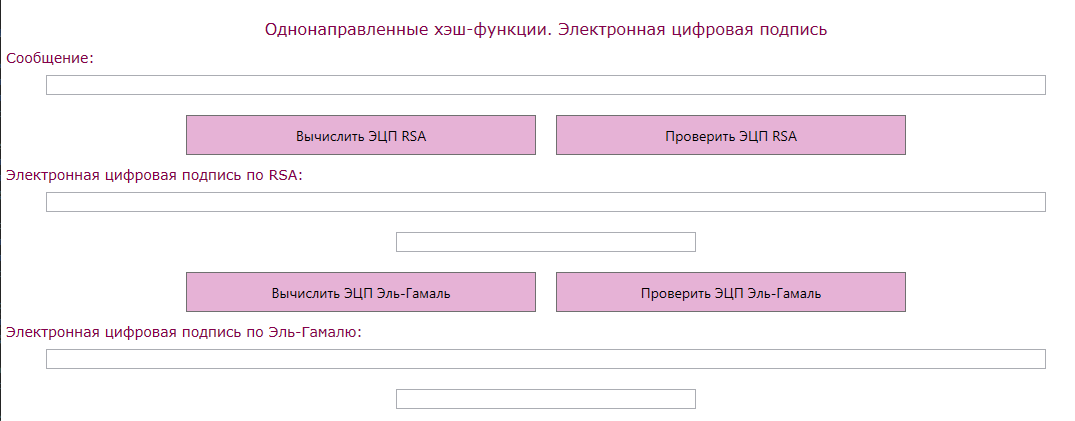
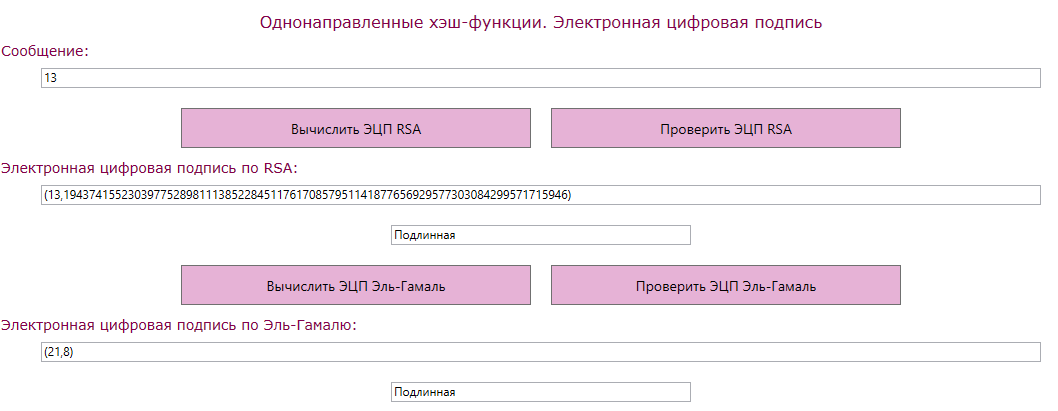


Рис. 1 – Интерфейс реализованного приложения

1. **Тестирование**



1. **Вывод**

При выполнении лабораторной работы были изучены схемы цифровой подписи и получены навыки создания и проверки подлинности электронной цифровой подписи.