БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №10**

**«Исследование алгоритмов генерации и**

**верификации электронной цифровой подписи**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2022

**Цель:** изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии.

**Ход работы**

**Задание.** Разработать приложение, которое реализует генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра.

В роли сообщения будет выступать строка со значением ФИО.

**RSA**

Зашифрованный хеш сообщения представлен на рисунке 1.

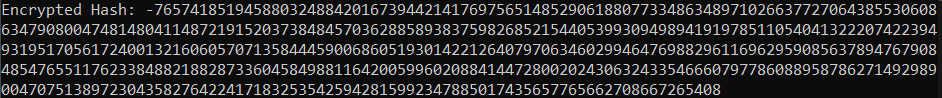


Рисунок 1 – Зашифрованный хеш сообщения

Расшифрованный хеш сообщения представлен на рисунке 2.

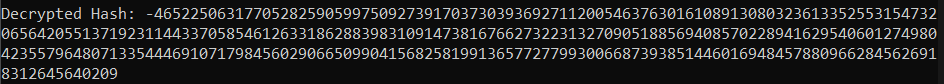


Рисунок 2 – Расшифрованный хеш сообщения

Вывод о том, верифицирована ли цифровая подпись представлен на рисунке 3.



Рисунок 3 – Подпись верифицирована

**Эль-Гамаль**

Результат работы алгоритма верификации ЭЦП на основе алгоритма Эль-Гамаля представлен на рисунке 4.

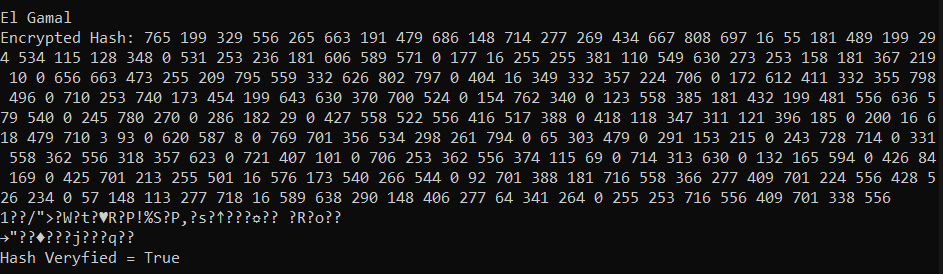


Рисунок 4 – Результат работы шифра Эль-Гамаля

**Шнорр**

Результат работы алгоритма верификации ЭЦП на основе алгоритма Шнорра представлен на рисунке 5.

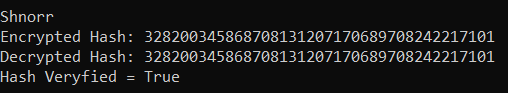


Рисунок 5 – Результат работы шифра Шнорра

**Вывод:** в ходе лабораторной работы были закреплены теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации ЭЦП, получены навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамаля и Шнорра, а также DSA, разработано приложение для реализации алгоритмов генерации и верификации ЭЦП.