**МИНОБРНАУКИ РОССИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «ВГУ»)**

Факультет прикладной математики, информатики и механики

Кафедра ERP-систем и бизнес-процессов

ОТЧЕТ

о преддипломной практике

магистра 11 группы 2 курса

факультета прикладной математики, информатики и механики

Место прохождения практики: кафедра ERP-систем и бизнес-процессов

Сроки прохождения практики: 04.05-31.05

Тема практики: Криптоанализ в обучающей программе El-Gamal\_Tutor

Выполнил \_\_\_\_\_\_\_\_\_\_\_\_ В. А. Ковун

Магистр 2 курса *(подпись)*

Руководитель от кафедры \_\_\_\_\_\_\_\_\_\_\_\_ Б. Н. Воронков

к.т.н., доцент  *(подпись)*

Воронеж – 2018

Содержание

[Постановка задачи 3](#_Toc515569669)

[Ход работы 3](#_Toc515569670)

[Вывод 6](#_Toc515569672)

# Постановка задачи

Реализовать функционал дискретного логарифмирования для электронной обучающей программы El-Gamal\_Tutor.

# Ход работы

El-Gamal\_Tutor – обучающая программа, созданная для использования в лабораторных работах по дисциплинам, связанным с изучением методов и средств защиты информации.

Для добавления в программу были выбраны три экспоненциальных алгоритма дискретного логарифмирования: ро-метод Полларда, алгоритм Гельфонда-Шенкса и алгоритм Сильвера-Полига-Хеллмана. Каждый алгоритм реализован в соответствующем классе.

Класс PollardsRho содержит функции вычисления дискретного логарифма ро-методом Полларда.

Класс BabyStepGiantStep содержит функции вычисления дискретного логарифма с помощью алгоритма Гельфонда-Шенкса, также известного как алгоритм больших и малых шагов.

Класс SilverPohligHellman содержит функции вычисления дискретного логарифма с помощью алгоритма Сильвера-Полига-Хеллмана.

Класс BigIntegerSqrt содержит метод расширения класса BigInteger для извлечения квадратного корня из больших чисел методом Ньютона. Этот метод требуется в алгоритме Сильвера-Полига-Хеллмана.

Графический интерфейс пользователя реализован посредством нескольких форм, часть из которых относится к обучающей части приложения, а другая часть – к дополнительной. Описание всех алгоритмов добавлено в обучающую часть программы, сами алгоритмы можно использовать в дополнительной части программы.

# 

Рис. 1. Форма дискретного логарифмирования

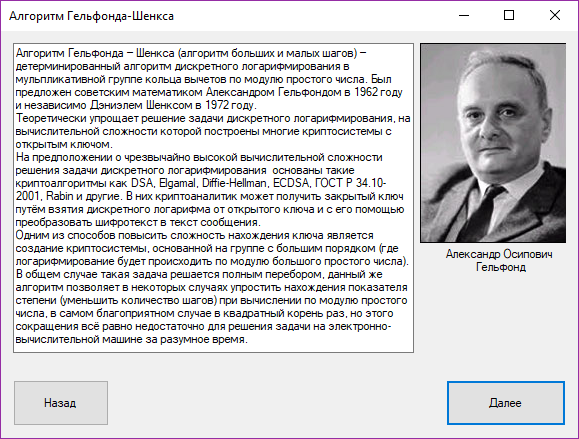


Рис. 2. Информация об алгоритме Гельфонда-Шенкса в обучающей

части программы.

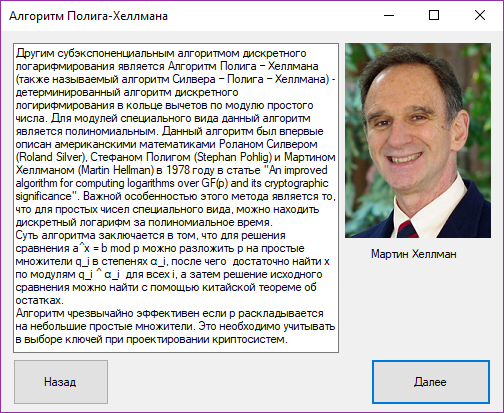
****

Рис. 3. Информация об алгоритме Полига-Хеллмана в

обучающей части программы.

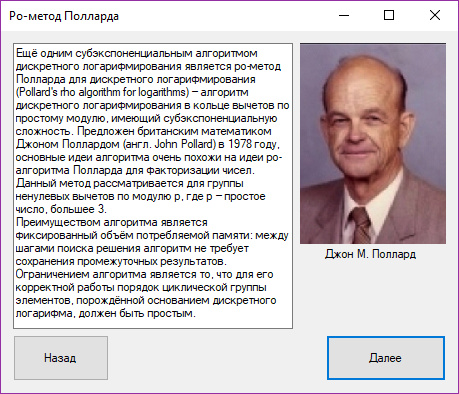
****

Рис. 4. Информация о ро-методе Полларда

в обучающей части программы.

# Вывод

В ходе работы для программы El-Gamal\_Tutor были реализованы три различных алгоритма дискретного логарифмирования. Описания алгоритмов добавлены в обучающую часть программы для обучения студентов основам криптоанализа системы Эль-Гамаля.