­МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования «Оренбургский государственный университет»

**РЕКЛАМНО-ТЕХНИЧЕСКОЕ ОПИСАНИЕ**

Прикладная программа

«Программная реализация алгоритма шифрования RSA»

Авторы

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.А. Щудро

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А. Петросян

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Лысенко

«28» февраля 2024 г.

Оренбург

2024

**1 Функциональное назначение программы, область ее применения и ограничения**

Прикладная программа «Программная реализация алгоритма шифрования RSA» является программным средством, способным генерировать открытые и приватные ключи для различных пользователей, шифровать введенное сообщение и расшифровывать зашифрованное сообщение.

**2 Используемые технические средства**

Для работы программы требуется персональный компьютер, удовлетворяющий следующим системным требованиям:

Минимальная конфигурация:

* процессор с частотой не менее 233 МГц;
* свободное место на жестком диске не менее 100 Мб;
* объем оперативной памяти 64 МБ.

Требования к информационной и программной совместимости:

* язык программирования – C++;
* Операционная система – Windows;
* объем памяти под программу не менее 2 Мб.

**3 Количественные характеристики электронного ресурса**

Таблица 1 – Количественные характеристики электронного ресурса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название | Наличие | Количество | | Примечание |
| 1 | 2 | 3 | | 4 |
| Количество основных окон прикладной программы |  | 1 | окна |  |
| Вспомогательные материалы:  руководство пользователю  тестовый пример |  | 1 | руководство |  |
| 1 | пример |
| Список рекомендуемых источников:  печатные источники  аннотированные интернет-источники | | 2 | источник |  |
| нет | ресурс |
|  | | | | |

**4 Специальные условия применения и требования организационного, технического и технологического характера**

**4.1 Руководство программиста**

Программа разработана по технологии ООП.

Для установки программы необходимо распаковать архив, содержащий программу, в удобное место.

На вход поступает имя объекта.

Затем (при существующем в списке программы имени объекта) поступает сообщение для кодирования и декодирования.

При кодировании символы сообщения по одному преобразуются сначала в свою числовую форму, а затем кодируются при помощи открытого ключа ранее введённого объекта.

При декодировании алгоритм преобразует закодированные символы сообщения при помощи закрытого (секретного) ключа ранее введённого объекта.

На рисунке 1 приведена схема алгоритма работы программы.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Автоматически созданное описание

Рисунок 1 – Блок схемы алгоритмов работы функций encryption, decryption, nod, mutuallySimply

Изображение выглядит как диаграмма, текст, зарисовка, Технический чертеж

Автоматически созданное описание

Рисунок 2 – Блок схема алгоритма работы функции Key\_generation

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 3 – Блок схема алгоритма работы функции Word\_encryption

Изображение выглядит как диаграмма, текст, План, Технический чертеж

Автоматически созданное описание

Рисунок 4 – Блок схема алгоритма работы функции Find\_user

Изображение выглядит как текст, диаграмма, зарисовка

Автоматически созданное описание

Рисунок 5 – Блок схема алгоритма работы основной части программы

**4.2 Руководство пользователя**

Для начала работы с программным средством необходимо иметь операционную систему Windows.

Программа представляет собой консольное приложение, при открытии которого открывается окно, приведенное на рисунке 2.

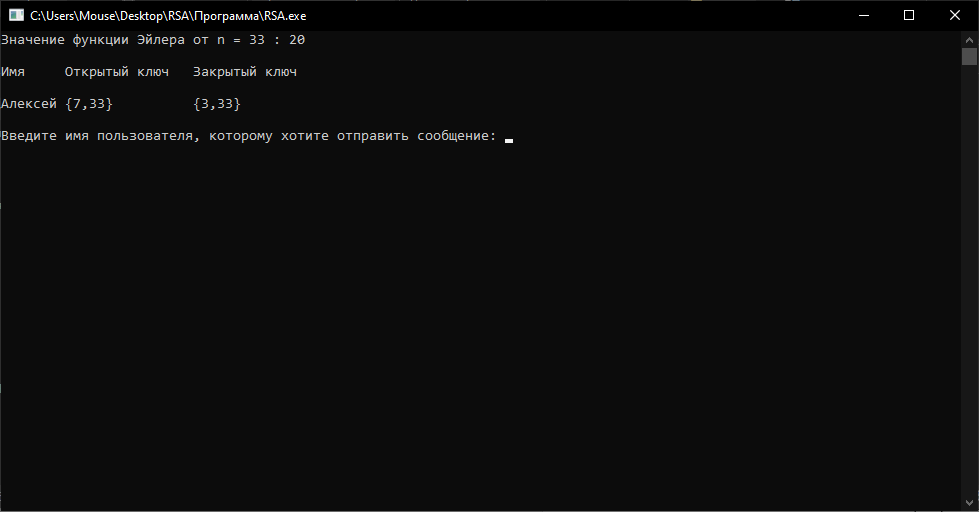


Рисунок 2 – Окно программы

Пользователю необходимо ввести имя объекта, которому он хочет отправить сообщение (на данный момент объект всего один – Алексей). При поступлении несуществующего в списке программы имени объекта, будет выведено сообщение, что данный пользователь не найден, и программы прекратит свою работу.

Если было введено имя существующего в списке программы объекты, то пользователю будет предложено ввести сообщение для отправки и дальнейшего кодирования и декодирования. На данный момент программа может работать только с сообщениями, состоящими из символов русского алфавита нижнего регистра и пробелов (при введении иных символов, они будут закодированы, а затем декодированы неверно).

При полностью корректном введении данных программа выведен подробный процесс кодирования и декодирования сообщения, а также сообщение, получившееся после этих 2 процессов.

1. **Список использованной литературы**

1 Бернет С., Пэйн С.: Криптография. Официальное руководство RSA Security. - 2-е издание. Пер. с англ. М.: Бином, 2009, 384 c.

2 Р.А. Хади, А.В. Аграновский: Практическая криптография. СОЛОН-Пресс, 2009, 257 с.

**6 Условия передачи программной документации или ее продажи**

Передача электронного ресурса и прилагаемой к нему сопроводительной документации осуществляется в соответствии с лицензионным договором о передаче неисключительных прав на использование произведения.