|  |
| --- |
| Описание: https://lh6.googleusercontent.com/QcftzNtI05T0Y6fjdSh1Rr2rt8oqZ1IvnLvbn1jLJ7CCyteVir3k-xBLv4SL1wAgWJsRhmmJSR0UW-RP63_GQenE4vVWv05BRoZTsmIcBccVTnfxwmsnNMvjg599x9SqZd8E3dkd |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования"МИРЭА - Российский технологический университет"РТУ МИРЭА |

Институт информационных технологий

Кафедра вычислительной техники

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

**по дисциплине**

**«Защита информации»**

Студент группы ИВБО-07-15 Попов Н.С.

Принял Воронков С. О.

Москва 2018

Постановка задачи:

Разработать программу, реализующую шифр Цезаря. Программа должна зашифровывать и расшифровывать текст при помощи ключа, так же производить дешифровку посредством частотного анализа и биграмм.

Ход выполнения работы:

1. В программу загружается большой текст и одна случайно выбранная из него глава.
2. С помощью метода, реализующего шифрование посредством шифра Цезаря, шифруется глава.
3. Полученный текст дешифруется методом, реализующим дешифрование посредством шифра Цезаря и методом, реализующим дешифрование посредством частотного анализа. Причем второй метод сначала сопоставляет наиболее часто встречающиеся биграммы главы с наиболее часто встречающимися биграммами большого текста, а после сопоставляет по одной оставшиеся буквы.

Вывод:

Дешифрация посредством частотного анализа, в отличии от шифра Цезаря, не восстанавливает исходный текст на 100%.