|  |  |
| --- | --- |
|  | |
| МИНОБРНАУКИ РОССИИ | |
| Федеральное государственное бюджетное образовательное учреждение  высшего профессионального образования  **" МИРЭА - Российский технологический университет "**  **РТУ МИРЭА** | |
| Факультет информационных технологий (ИТ) |  |
| Кафедра ВТ |  |

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1** | |
| **по дисциплине** | |
| **«Защита информации»** | |
|  | |
| Выполнил студент группы ИВБО-01-15 | *Жукова М. В.* |
| Приняла | *Воронков С.О.* |

|  |  |  |
| --- | --- | --- |
| Лабораторные работы выполнены | «\_\_»\_\_\_\_\_\_\_201\_\_ г. |  |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_201\_\_ г. |  |

Москва

2018

**Задание:** разработать программу, декодирующую зашифрованный текст методом частотного анализа. Программа должна выполнять следующие действия:

* зашифровать исходный текст с использованием шифра Цезаря;
* декодировать полученный текст методом частотного анализа с уточнением биграммам;
* результаты шифрования и декодирования сохранить в отдельные файлы.

**Решение:**

1. Сканируем зашифрованный текст и файл, из которого будут браться частоты естественного языка. Выписываем все найденные символы и биграммы, и подсчитываем их частоту встречания в тескте

2. Сортируем символы по частоте употребления в естественном языке и в зашифрованном файле. Сопоставляем.

3. Два полученных словаря биграмм сортируются по частоте в порядке убывания.

4. Используем 10 наиболее часто встречаемых пар. Биграмм, считываемые из обоих словарей, сопоставляются. Делаем проход по всему зашифрованному тексту, считывая биграммы в виде двух символов, сдвигая на один символ каждый шаг. Если конкатенация этих символов не встречается в десяти часто встречаемых, то записывается первый символ из считанных. В противном случае записывается биграмма из незашифрованного словаря и происходит сдвиг на 2 символа.

**Вывод:** Успешность декодирования с использованием частотного анализа составила ≈ 35%. После уточнения биграммами успешность декодидирования составила ≈60%.