|  |  |  |  |
| --- | --- | --- | --- |
|  | |  |  |
| МИНОБРНАУКИ РОССИИ | | | |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования«МИРЭА – Российский технологический университет»РТУ МИРЭА | | | |
| **ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**  **КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1** | | | |
| **по дисциплине** | | | |
| **«Защита информации»** | | | |
|  | | | |
| Выполнил студент группы ИВБО-01-15 | | Шлыков А.В. | |
| Принял | | Воронков С.О. | |
| Работа представлена к защите | «\_\_»\_\_\_\_\_\_\_201\_ г. | | *(подпись студента)* |
|  |  | |  |
| «Допущен к защите» | «\_\_»\_\_\_\_\_\_\_201\_г. | | *(подпись руководителя)* |

Москва 2018

**Задание:**

Разработать программу, декодирующую шифротекст методом частотного анализа.

Программа должна:

- 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. Открываем файл и зашифровываем его с помощью шифра Цезаря со сдвигом 5.
2. Проводим частотный анализ исходного текста и зашифрованного.
3. Сортируем проанализированные таблицы по убыванию частот.
4. Сопоставляем по порядку две таблицы. Например,

|  |  |
| --- | --- |
| А-5 | Г-6 |
| Б-4 | Д-5 |
| В-3 | Е-4 |

И получим таблицу соответствия:

|  |  |
| --- | --- |
| А | Г |
| Б | Д |
| В | Е |

1. Проведём аналогичный частотный анализ для биграмм. И составим аналогичную таблицу соответствия для них.
2. Выберем 5 самых часто встречающихся биграмм и обновим таблицу соответствия, например:

аб-вг

гд-жз

Следовательно, обновим таблицу следующим образом

а-в

б-г

г-ж

д-з

**Вывод:**

Успешность декодирования с использованием частотного анализа составила примерно 22%.

После уточнения биграммами успешность декодидирования составила 49,89 %.