Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №6**

Изучение устройства и функциональных особенностей шифровальной машины «Энигма»

Выполнил:

Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

Для выполнения данной лабораторной работы была разработана программа на языке Python. Исходные данные были взяты из лабораторного практикума, из таблиц 4.5 и 4.6.

Для оценки криптостойкости был проведен частотный анализ.

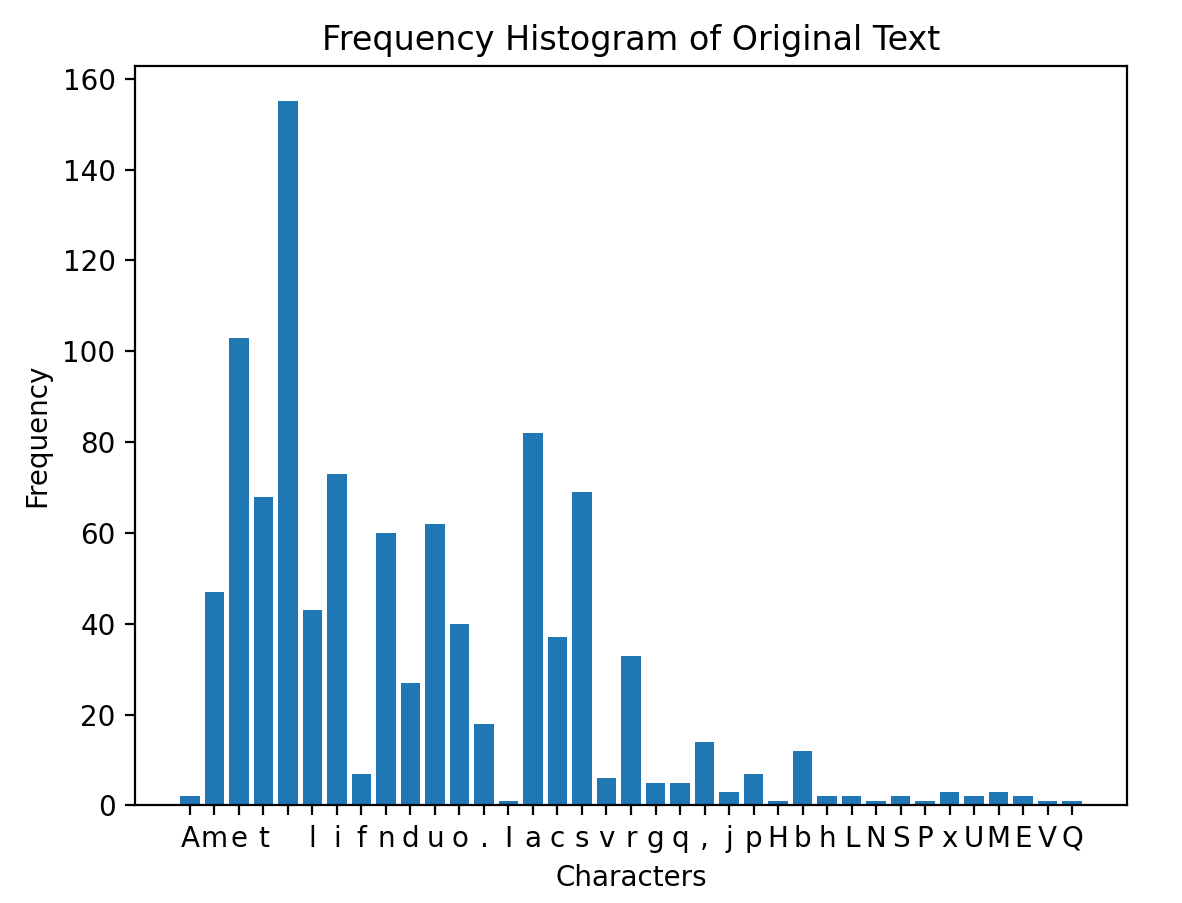


Рисунок 1 — Диаграмма частот входных данных

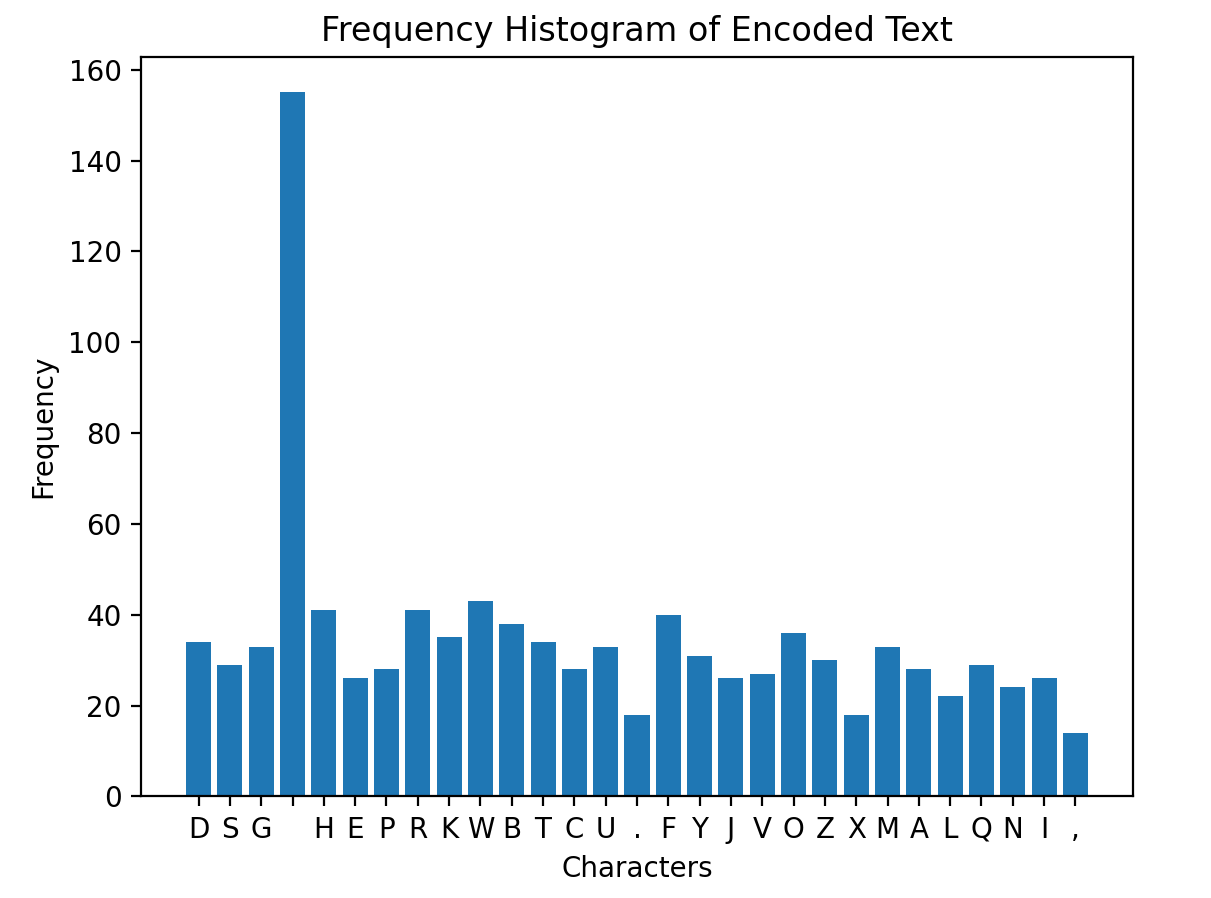


Рисунок 2 — Диаграмма частот зашифрованных данных

Исходя из полученных диаграмм частот можно заметить, что частота появления символов в зашифрованном сообщении примерно одинаковая. При выполнении работы использовалось 3 ротора, которые имеют 17 576 различных положений (26 × 26 × 26). Но на расчет влияют только кольца среднего и правого ротора, таким образом комбинаций колец получается 676 (26 × 26).

**Вывод:** Исходя из полученных диаграмм можно сделать вывод, что частотный анализ не даст практически никаких результатов. Это делает «Энигму» довольно криптостойкой по сравнению с ранее рассматриваемыми шифрами.