Ковкель Никита, ФИТ 3-4

Информационная безопасность

Отчет по лабораторной работе № 6.

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров

**Практическая часть**

Для проверки правильности работы приложения-симулятора при различных первоначальных настройках роторов первым было введено сообщение, состоящее из одной буквы “A” со сдвигом 0-0-0.

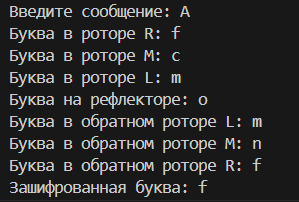


Рисунок 1.1 – Результат первой проверки зашифровки сообщения

На рисунке 1.1 представлены все этапы шифрования буквы “A” со сдвигом 0-0-0. На первом этапе переходим на Gamma rotor (правый) и получаем букву “F”:





Далее на втором этапе переходим на Beta rotor(средний) и получаем букву “C”:





Далее на третьем этапе переходим на I rotor (левый) и получаем букву “M”:





Потом идём на рефлектор, и меняем букву “М” на “О”:



Далее идём на I rotor (левый) и получаем букву “M”:





Далее переходим на Beta rotor(средний) и получаем букву “N”:





Далее переходим на Beta rotor(средний) и получаем букву “F”:





Результат шифрования: буква “A” со сдвигом 0-0-0 шифруется как “F”.

В данной версии Энигмы, все роторы и рефлекторы имеют фиксированные перестановки букв, которые не меняются в процессе шифрования. Это делает шифр уязвимым к атакам, основанным на известных шаблонах языка и статистическом анализе текста. В оригинальной машине Энигма, перестановки роторов менялись после каждого нажатия клавиши, что существенно усложняло криптоанализ. Кроме того, данная версия машины Энигма не включает механизмы, такие как панель переключателей и особые настройки роторов, которые добавляли дополнительный уровень сложности и безопасности в оригинальную машину Энигма. В целом, эта версия машины Энигма является простой имитацией и не обеспечивает достаточный уровень криптостойкости

**Вывод:** на данной лабораторной работе мы изучили и приобрели практические навыки разработки и использования приложений для реализации перестановочных шифров.