Математические основы защиты информации и информационной безопасности.

Лабораторная работа №1.

Подмогильный Иван Александрович.

Содержание

# 1 Цель работы

Освоить на практике шифрование шифров Цезаря и Атбаша.

# 2 Задание

1. Реализовать шифр Цезаря
2. Реализовать шифр Атбаш

# 3 Выполнение лабораторной работы

Написал код для зашивровки кодов шифром Цезаря

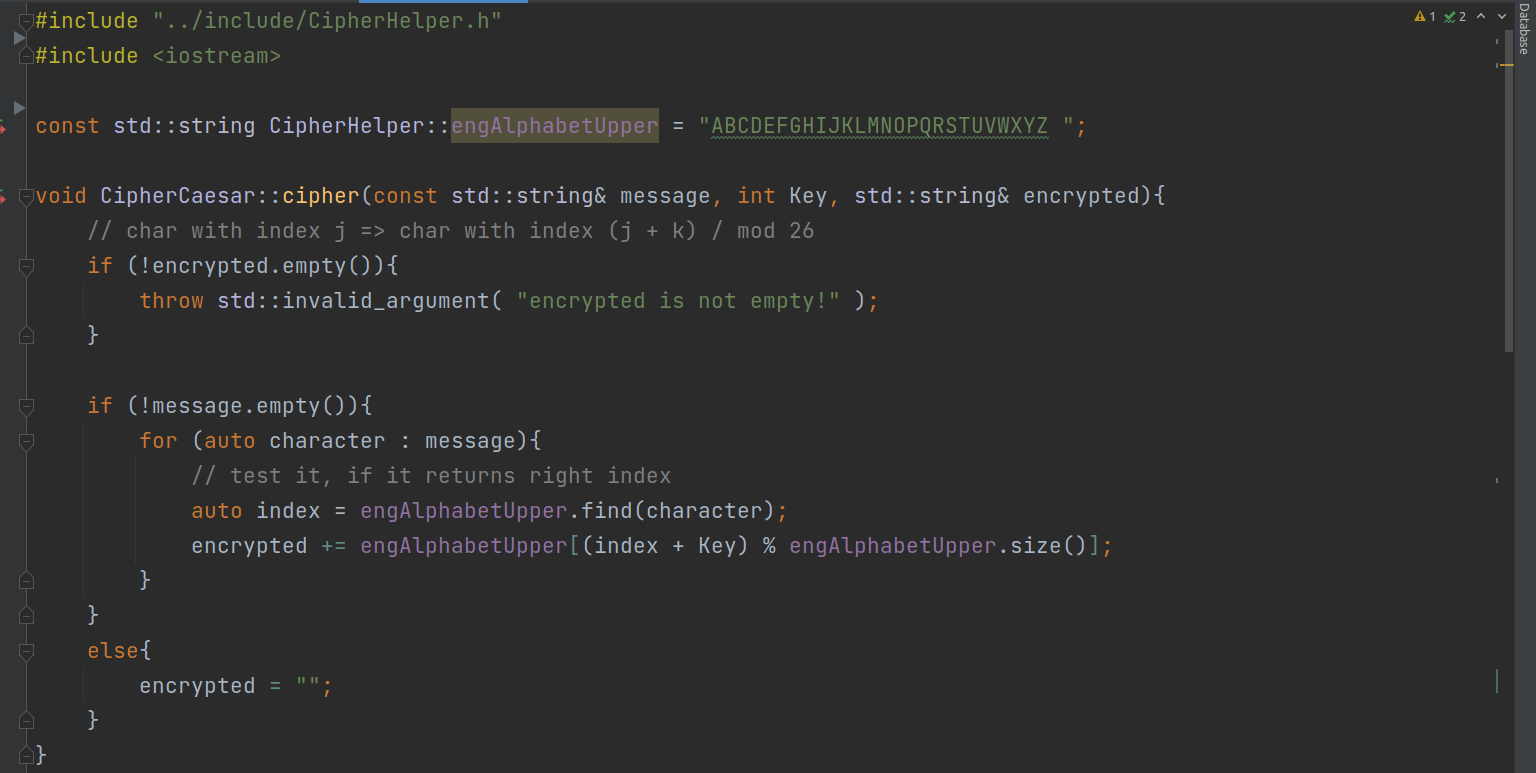


Figure 1: Caesar cipher

Написал код для дешивровки кодов шифром Цезаря

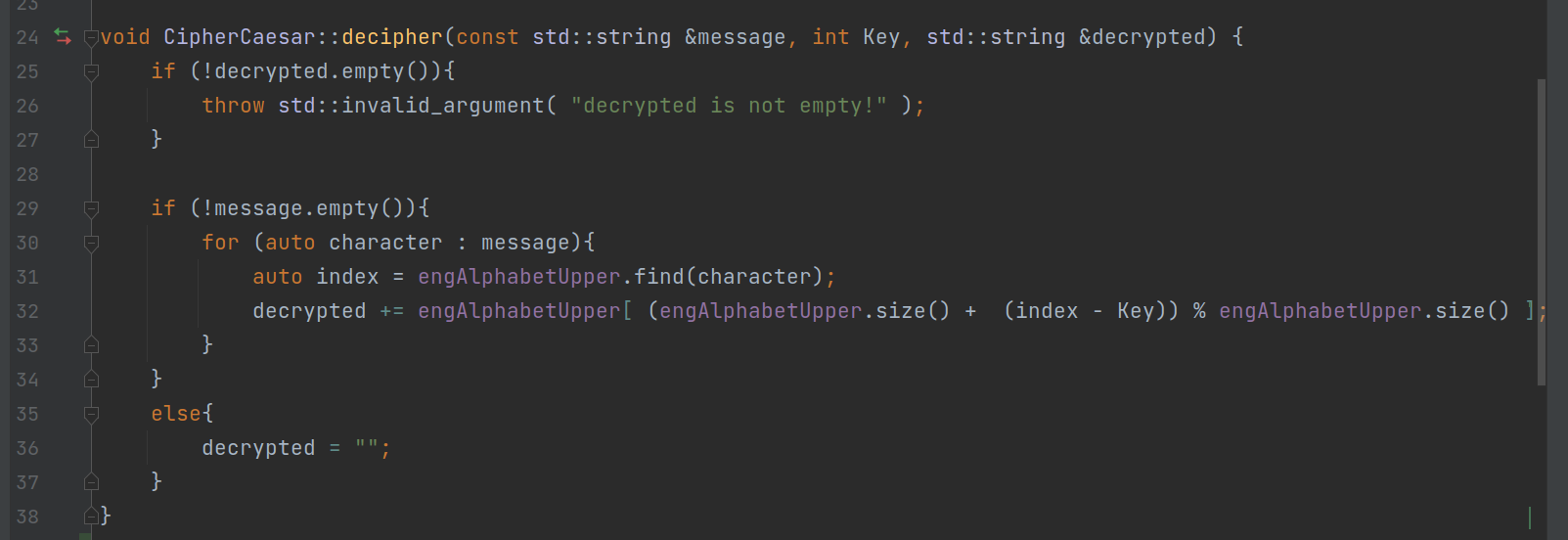


Figure 2: Caesar decipher

Написал код для зашивровки кодов шифром Атбаша

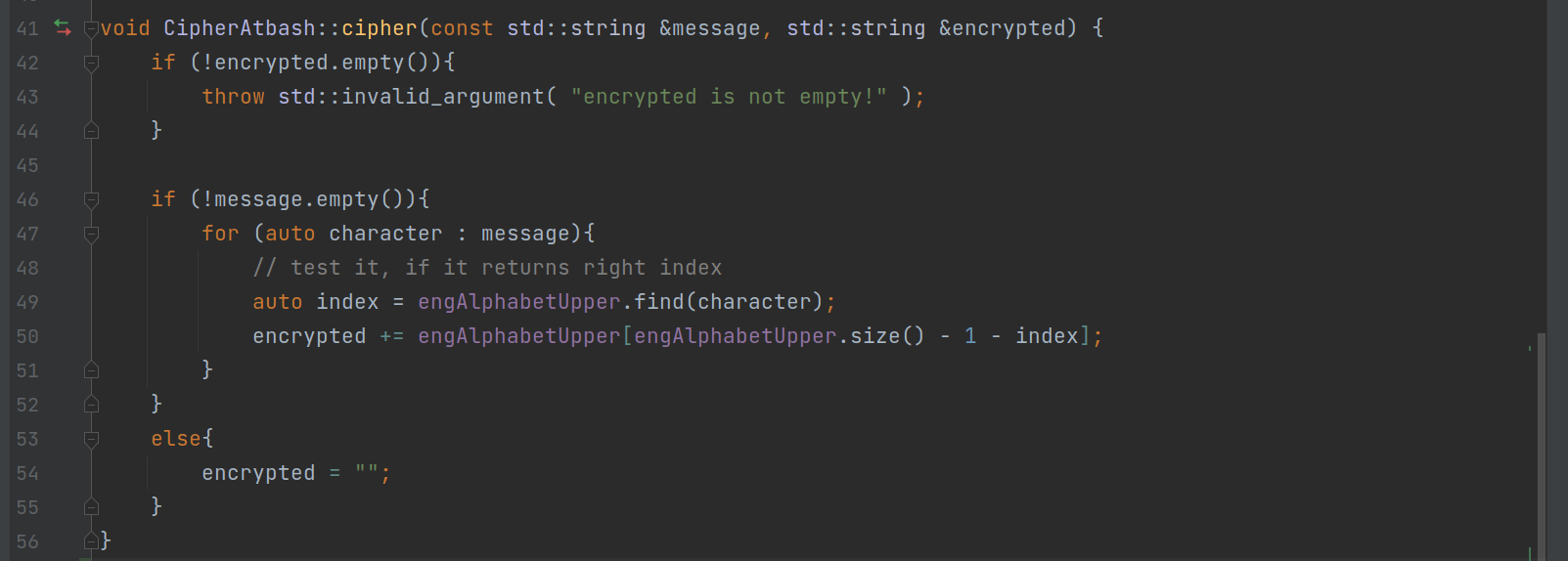


Figure 3: Atbash cipher

Написал код для дешивровки кодов шифром Атбаша

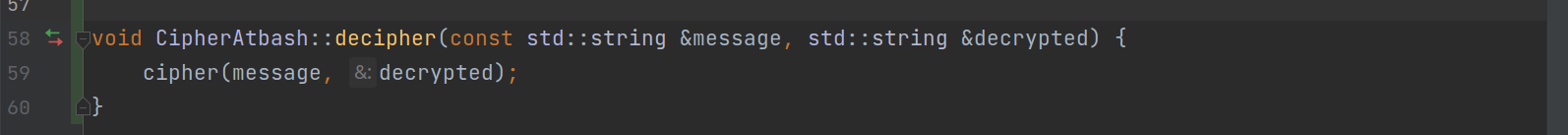


Figure 4: Atbash decipher

Написал заголовочный файл для класса реализации CipherHelper

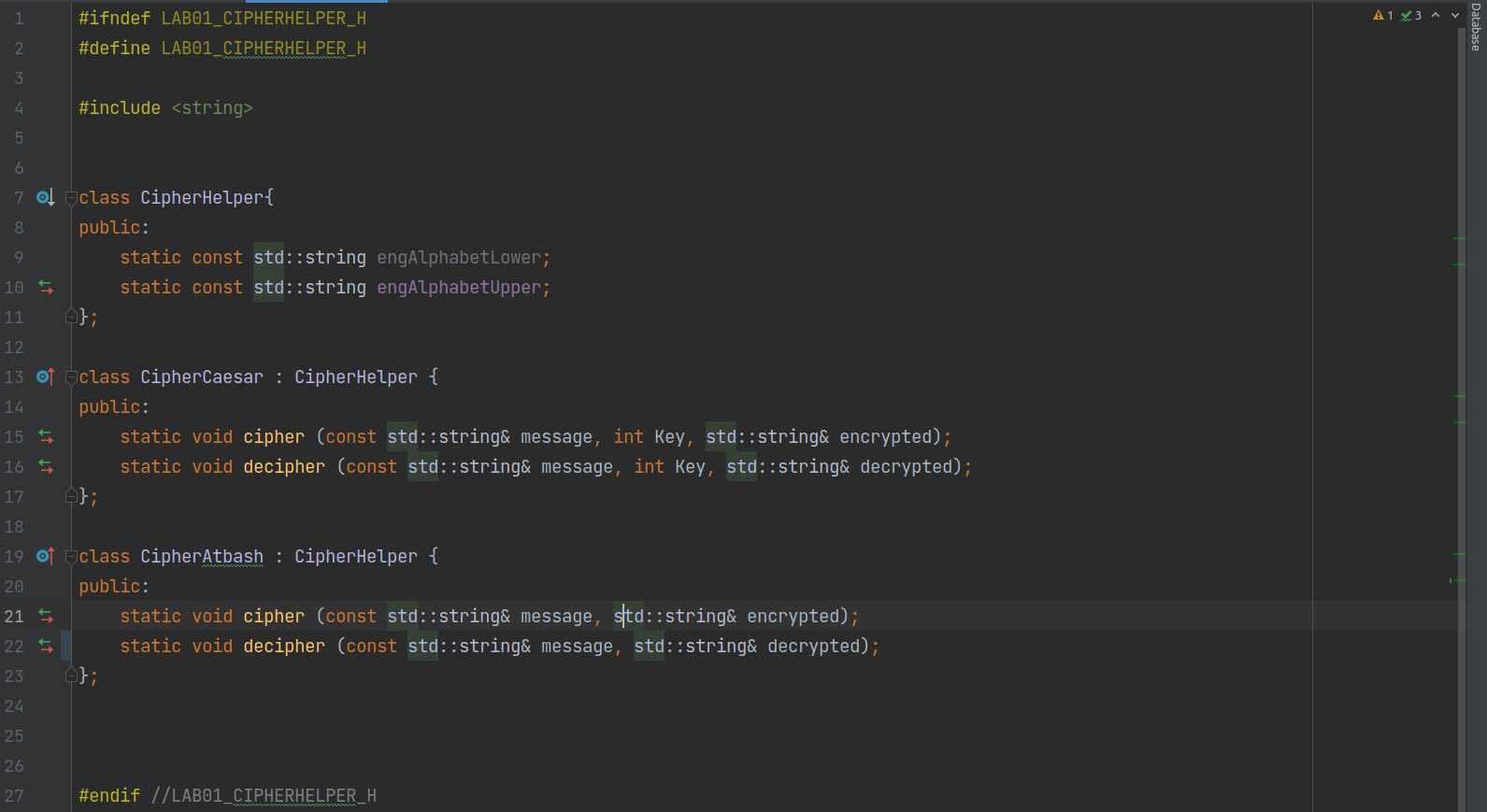


Figure 5: Header file

Написал CMakeLists.txt файл, который создаёт библиотеку из класса CipherHelper и бинарник main

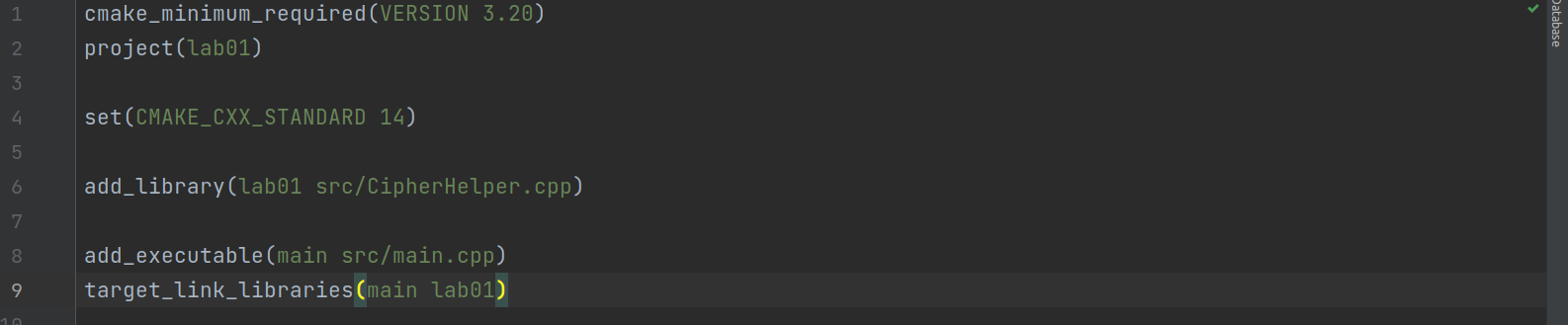


Figure 6: CmakeLists.txt file

Написал main.cpp файл, в котором есть тесты реализованных функций. Часть шифра Цезаря:

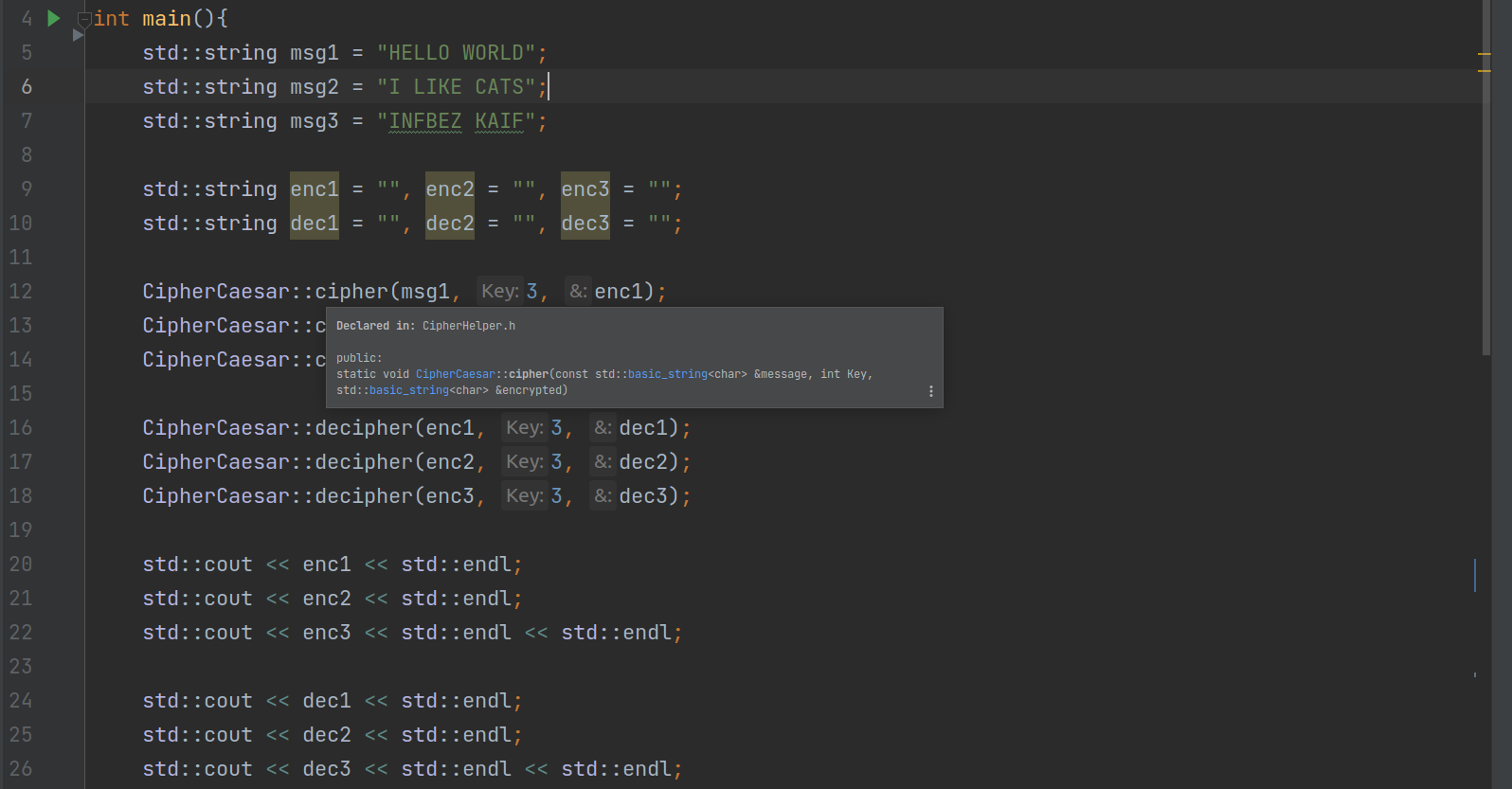


Figure 7: main.cpp

Часть шифра Атбаша:

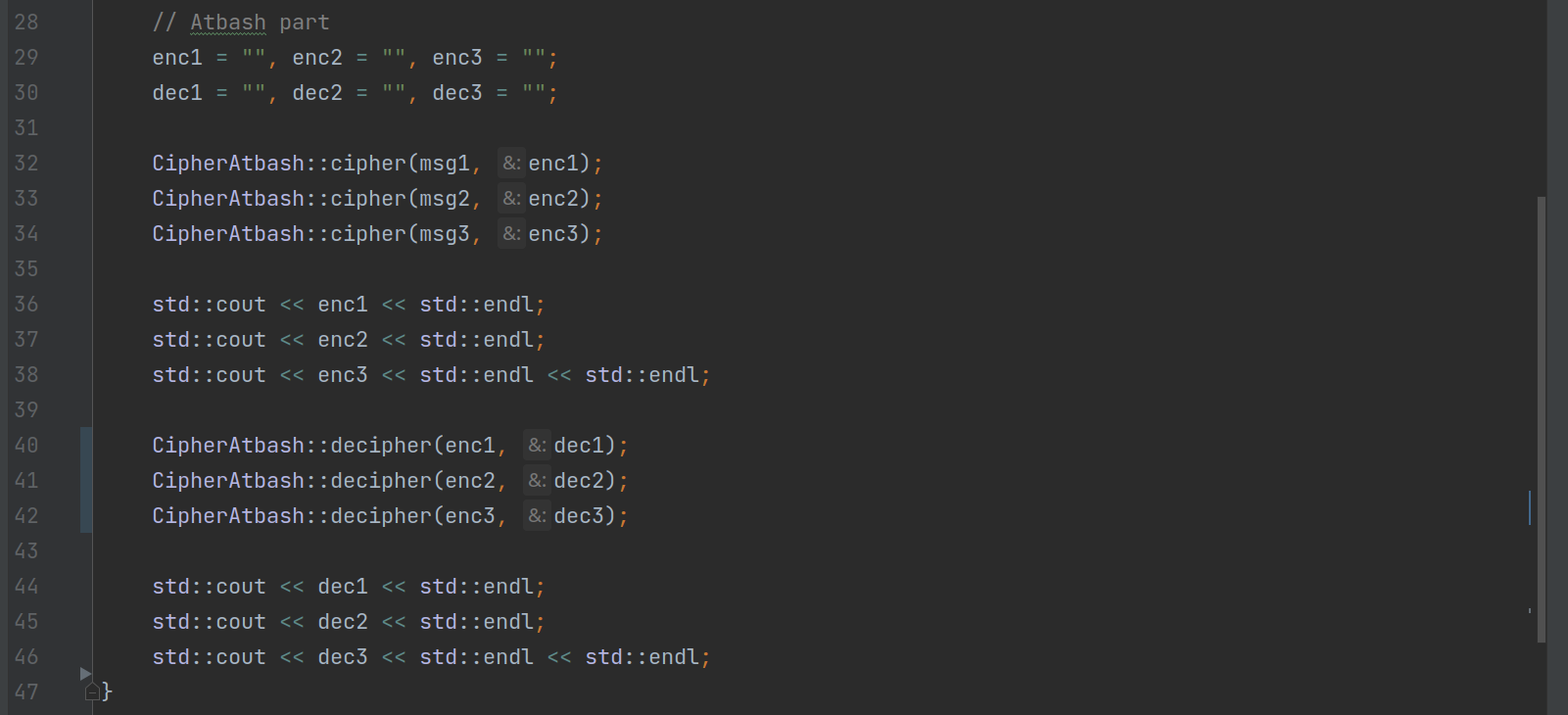


Figure 8: main.cpp

Результаты тестов. Первые три строчки это зашифрованные сообщения шифром Цезаря. Следующие три строчки, это расшифрованные сообщения. Следующие три строчки, это те же сообщения, но зашифрованные шифром Атбаш. И последние три строчки - расшифрованные сообщения.

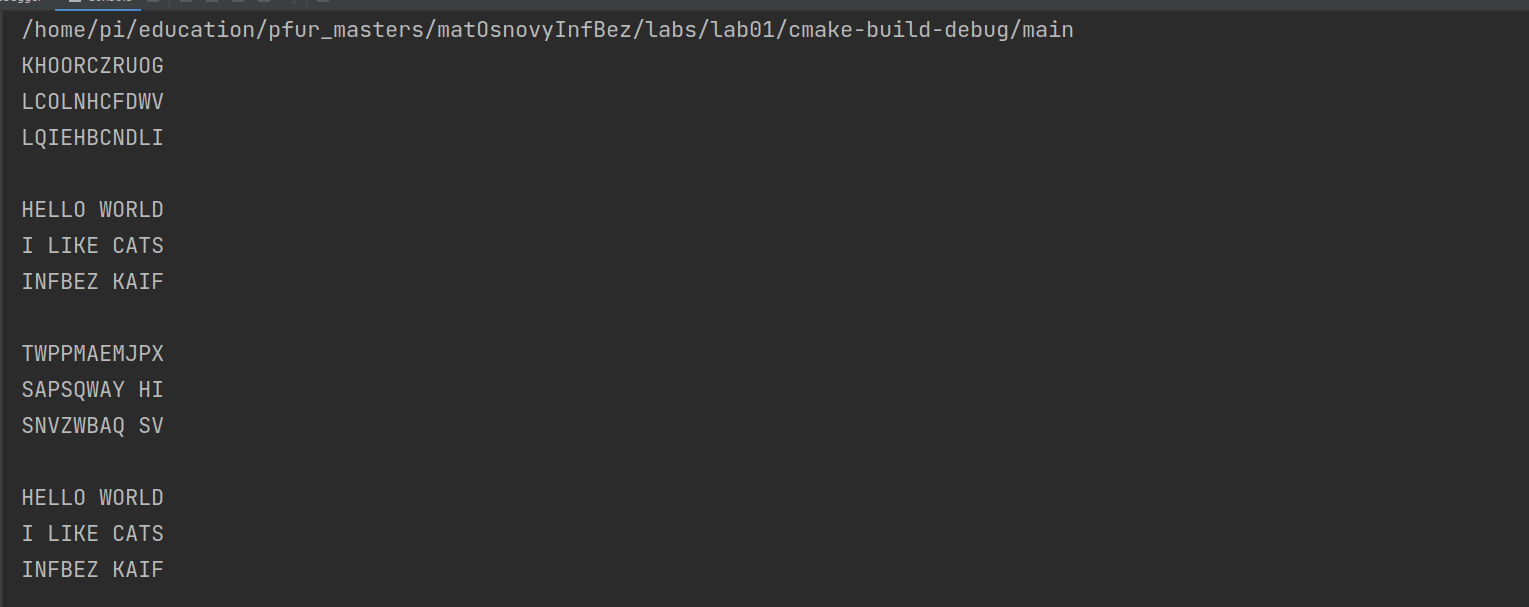


Figure 9: tests

# 4 Выводы

Освоил на практике применение методов шифрования Цезаря и Атбаша.