Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ

по дисциплине «Информационная безопасность и защита информации»
Симметричные шифры
Вариант 6

Преподаватель _____ А. А. Сиарас
подпись, дата инициалы, фамилия

Студент КИ19-07Б, 031941597 _____ А. А. Горбацевич
номер группы, зачётной книжки подпись, дата инициалы, фамилия

Красноярск 2021

Содержание

1 Цель работы

Освоить принципы работы симметричных методов шифрования.

2 Задание

Разработать алгоритм шифрования Плейфера; реализовать программу использующую данный шифр для шифрования/расшифрования данных; протестировать алгоритм.

3 Выполнение работы

3.1 Описание метода шифрования

Для шифрования текста берётся ключевое слово, из него удаляются повторы букв, затем оно записывается в матрицу 5 на 5. Если длины слова не хватает для заполнения матрицы, она дополняется отсутствующими буквами из алфавита. Для шифрования исходного текста, нужно разбить его на пары символов, причём если в паре стоят одинаковые буквы или остался всего один символ, то после первого символа добавляется «X», затем на матрице выбирается прямоугольник, углы которого соответствуют символам пары, далее происходит шифрование по следующим правилам:

1. Если символы пары из исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
2. Если символы пары из исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
3. Если символы пары из исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «X», если они не несут смысла в исходном сообщении.

3.2 Реализация метода шифрования на ЯП

Для реализации шифра был выбран C# на платформе .NET 5, с использованием UI-тулкита AvaloniaUI.

Исходный код проекта выложен в репозиторий на GitHub: https://github.com/NuarkNoir/UPC/tree/master/4sem/isaip/01/PlayfairCypher.

3.3 Тестирование

Для тестирования был выбран стандартный фреймвворк тестирования .NET приложений NUnit.

Исходный код тестов находится в поддиректории PlayfairTests проекта на GitHub https://github.com/NuarkNoir/UPC/tree/master/4sem/isaip/01/PlayfairCypher/PlayfairTests.