Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет

информатики и радиоэлектроники»

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ

Кафедра интеллектуальных информационных технологий

Лабораторная работа № 2

“Вариант 3”

Отчет

Выполнил:

студент гр. 221703

Веркович Е.В.

Проверил: Крищенович В.А.

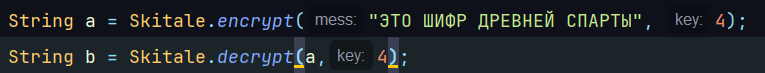
Минск 2024

**Задание 1:**

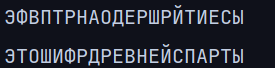
**1) Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом. Язык исходного текста русский или английский по выбору исполнителя.**

**Демонстрация работы программы:**

Применяем функцию шифрования и дешифрования с ключом 4

****

Выводим результат на экран



**2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод илиисходный текст для автоматического сравнения результата дешифрования.**



**3) Оценить криптографическую стойкость реализованного шифра.**

Оценка криптографической стойкости шифра скитала

Шифр скитала является одним из древнейших методов шифрования. Его стойкость основывается на перестановке символов исходного сообщения, что делает его уязвимым к различным видам атак. Основные аспекты оценки стойкости:

1. Тип атаки: Шифры перестановки (в том числе шифр скитала) подвержены атакам с использованием методов анализа частотных характеристик и анализа перестановки символов, поскольку шифр не изменяет частотное распределение символов.

2. Ключ шифра: В данном случае ключом является количество строк, на которые разбивается сообщение. Это значение легко подобрать перебором, поскольку в реальной ситуации оно часто ограничено малыми числами.

3. Обратимость шифра: Поскольку шифр только переставляет символы, без усложнения замены, он легко обратим при наличии знаний о размере ключа (количестве строк).

Таким образом, стойкость данного шифра крайне низкая для современных криптографических целей. Его можно взломать даже с помощью анализа шифротекста вручную или при помощи простого перебора ключа.

**4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.**

Варианты усложнения шифра

Для повышения стойкости можно предложить следующие усложнения:

**1. Использование случайного заполнителя:**

- Вместо заполнения блоков пробелами можно использовать случайные символы для увеличения сложности анализа шифротекста.

**2. Добавление слоя шифра замены:**

- После перестановки символов, можно добавить элемент замены символов (например, шифр Цезаря или более сложный алгоритм замены), чтобы изменить частотные характеристики сообщения.

**3. Использование динамического ключа:**

- Вместо фиксированного ключа можно использовать динамический ключ, который изменяется на основе характеристик сообщения или других параметров, например длины сообщения.

Алгоритм усложненного шифра

Алгоритм шифрования:

**1. Очистить исходное сообщение от лишних символов.**

**2. Разбить сообщение на блоки по количеству строк, заданному ключом.**

**3. Для каждого блока:**

- Если длина блока меньше необходимого размера, дополнить его случайными символами.

- Переставить символы по схеме скиталы.

**4. После перестановки применить шифр замены к каждому символу блока (например, Цезарь с динамическим смещением, зависящим от позиции символа).**

**5. Объединить обработанные блоки в единое зашифрованное сообщение.**

Алгоритм дешифрования:

**1. Разбить зашифрованное сообщение на блоки по тому же количеству строк, которое использовалось для шифрования.**

**2. Для каждого блока:**

**- Применить обратный шифр замены.**

**- Выполнить обратную перестановку символов по схеме скиталы.**

**3. Убрать случайные символы заполнения (при наличии).**

**4. Объединить обработанные блоки в исходное сообщение.**

Это добавит шифру дополнительную сложность и повысит стойкость против атак на основе анализа перестановок и частотного анализа.