МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ НА ТЕМУ:**

**Исследование криптографических шифров на основе перестановки символов**

Ф.И.О.

Савельев Дмитрий Витальевич

Преподаватель

Берников Владислав Олегович

Минск 2021

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров.

2. Разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования.

3. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

4. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# 1. Теоретические сведения

Сущность перестановочного шифрования состоит в том, что исходный текст (М) и зашифрованный текст (С) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки.

Шифры перестановки относятся к классу симметричных. Элементами текста могут быть отдельные символы (самый распространенный случай), пары, тройки букв и т. д.

Классическими примерами перестановочных шифров являются анаграммы. Анаграмма (от греч. ana – снова и gramma – запись) – литературный прием, состоящий в перестановке букв (или звуков), что в результате дает другое слово или словосочетание, например: проездной – подрезной, листовка – вокалист, апельсин – спаниель.

В классической криптографии шифры перестановки делятся на два подкласса:

• шифры простой, или одинарной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) один раз;

• шифры сложной, или множественной, перестановки – при зашифровании символы открытого текста Мi перемещаются с исходных позиций в новые (в шифртексте Сi) несколько раз.

# 1.1. Шифры одинарной перестановки

# 1.1.1. Шифры простой перестановки

Среди шифров рассматриваемого подкласса иногда выделяют шифры простой перестановки (или перестановки без ключа). Символы открытого текста Мi перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

Пример 1. Простейшим примером является запись открытого текста в обратной последовательности. Так, если Мi = «шифр перестановки», то Сi = «иквонатсереп рфиш». Если переставляются в соответствующем порядке пары букв, то Сi = «киованстрепе фрши». При более длинных сообщениях можно таким же образом перемещать целые слова или блоки слов.

Подобную перестановку можно трактовать как транспозицию. В общем случае для использования шифров одинарной перестановки используется таблица, состоящая из двух строк: в первой строке записываются буквы, во второй – цифры J. Строки состоят из n столбцов. Буквы составляют шифруемое сообщение. Цифры J = j1, j2, …, jn, где j1 – номер позиции в зашифрованном сообщении первого символа открытого текста, j2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т. д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

Если предположить, что некоторое сообщение Мi состоит из букв от m1 до mn, то рассматриваемую таблицу можно представить как показано ниже (табл. 3.1).

Изображение выглядит как стол

Автоматически созданное описание

В первую строку табл. 3.1 могут записываться также числа в порядке возрастания от 1 до n. Понятно, что эти числа соответствуют позициям букв в открытом тексте. Процедура расшифрования также основана на использовании таблиц перестановки. Эти таблицы строятся на основе табл. 3.1.

Для использования на практике рассмотренный метод зашифрования/расшифрования не очень удобен. При больших значениях n приходится работать с таблицами, состоящими из большого числа столбцов. Кроме того, для сообщений разной длины необходимо создавать разные таблицы перестановок.

Следует также отметить сходство рассмотренных алгоритмов зашифрования/расшифрования и алгоритмов перемежения.

# 1.1.2. Шифры простой блочной перестановки

Указанные шифры строятся по тем же правилам, что и шифры простой перестановки. Блок должен состоять из 2 или более символов. Если общее число таких символов в сообщении не кратно длине сообщения, то последний блок можно дополнить произвольными знаками.

# 1.1.3. Шифры маршрутной перестановки

Основой современных шифров рассматриваемого типа является геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слево направо, сверху вниз или каким-либо иным образом) записывается открытый текст. Для получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т. е. по иному маршруту Шифр Скитала (Сцитала). Известно, что в V в. до н. э. в Спарте существовала хорошо отработанная система секретной военной связи. Для этого использовался специальный жезл «скитала» (греч. σκυτάλη) – первое, вероятно, простейшее криптографическое устройство, реализующее метод перестановки (рис. 3.1).



Рисунок 3.1 – Скитала

Для зашифрования и расшифрования необходимо было иметь абсолютно одинаковые жезлы. На такой предмет наматывалась пергаментная лента. Далее на эту ленту построчно наносился текст. Для расшифрования ленту с передаваемым сообщением нужно было намотать так же, как и при нанесении открытого текста.

Следуя вышеприведенным рассуждениям, можно отождествить Скитала с таблицей размерами k×s, где k – количество столбцов, s – количество строк. Поскольку при регулярном обмене данными сообщения часто имеют разную длину, то оба этих параметра за неизменяющийся ключ взять неудобно. Поэтому обычно в качестве известного каждой стороне ключа выбирается один из них (часто это s), а второй вычисляется на основе известного и длины n сообщения Мi:

При этом слагаемое в квадратных скобках должно быть целым числом.

Нетрудно себе представить аналогию между Скитала и таблицей, которая «намотана» на цилиндр. При использовании шифра Скитала для формирования шифртекста сначала выбирается 1-я буква открытого текста, затем (k + 1)-я буква, (2k + 1)-я буква и т. д. для некоторого k, равного числу букв в каждой строке Скиталы. Значение k является постоянной величиной для данной Скиталы.

Организация маршрутной перестановки. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали (рис. 3.2, а), зигзагом (рис. 3.2, б), змейкой (рис. 3.2, в) или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

Изображение выглядит как седзи

Автоматически созданное описание

Рисунок 1.2 – Графическое представление методов маршрутной перестановки: а - по спирали; б - зигзагом; в - змейкой

Маршруты могут быть значительно более изощренными. Например, обход конем шахматной доски таким образом, чтобы в каждой клетке конь побывал один раз. Один из таких маршрутов был найден Л. Эйлером в 1759 г. Для примера на рис. 3.3 показан такой маршрут для обхода таблицы размером 5×4.

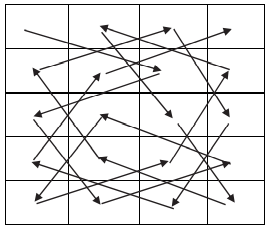


Рисунок 1.3 – Пример маршрута "обход конем"

Не менее занимательным и не менее сложным является организация маршрутов на основе «магических квадратов» – квадратных матриц со вписанными в каждую клетку неповторяющимися последовательными числами от 1, сумма которых по каждому столбцу, каждой строке и каждой диагонали дает одно и то же число.

Создание новых оригинальных маршрутов приветствуется и поощряется при выполнении данной лабораторной работы.

# 1.1.4. Шифр вертикальной перестановки

Данный шифр является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

• количество столбцов в таблице фиксируется и определяется длиной ключа;

• маршрут вписывания: слево направо, сверху вниз;

• шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Ключ может задаваться в виде текста (слова или словосочетания). Лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов.

# 1.2. Шифры множественной перестановки

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

Шифры гаммирования рассматриваются как самостоятельный класс. Такие шифры схожи с перестановочными тем, что в обоих случаях можно использовать табличное представление выполняемых операций на основе ключей. Вместе с тем шифры гаммирования имеют много общего с подстановочными шифрами, поскольку на самом деле при зашифровании происходит подмена одних символов другими.

# 2. Практическое задание

Основное задание

1. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;

• формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;

• оценивать время выполнения операций зашифрования/расшифрования (напоминание: во многих языках программирования есть встроенные методы для замеров времени; при отсутствии такового в используемом языке можно воспользоваться разностью двух дат (например, в миллисекундах: время после выполнения программы – время до начала выполнения преобразования)).

Для работы программы необходим файл с исходным сообщением на английском языке. Программа выполняет шифрование маршрутной перестановкой, а также дешифрование (рис 2.1 и 2.2).

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2.1 – Зашифрованное сообщение методом маршрутной перестановки

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2.2 – Расшифрованное сообщением методом маршрутной перестановки

И, аналогично, с множественной перестановкой.

**Вывод:** Таким образом, я изучил перестановочные методы шифрования, измерил их быстродействие.