Лабораторная работа № 3

Исследование криптографических шифров на основе перестановки символов

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. Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программного средства (L_LUX).
3. Разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования.
4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.
5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.
6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

3.1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Сущность перестановочного шифрования состоит в том, что, исходный текст (M) и зашифрованный текст (C) 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 распространённый случай), пары, тройки букв и так далее.

Классическими примерами перестановочных шифров являются *анаграммы*. Анаграмма (от греч. ανα – «снова» и γράμμα – «запись») – литературный приём, 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 M_i перемещаются с исходных позиций в новые (в шифртексте C_i) один раз,
- шифры *сложной* или *множественной перестановки* – при зашифровании символы открытого текста M_i перемещаются с исходных позиций в новые (в шифртексте C_i) несколько раз.

3.1.1. Шифры одинарной перестановки

3.1.1.1. Шифры простой перестановки

Среди шифров рассматриваемого подкласса иногда выделяют *шифры простой перестановки* (или *перестановки без ключа*). Символы открытого текста M_i 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 M_i = «шифр перестановки», то C_i = «иквонатсереп рфиш». Если переставляются в соответствующем порядке пары букв, то C_i = «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 $J = j_1, j_2, \ldots, j_n$, где j_1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где j_2 – 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 M_i состоит из букв от m_1 до m_n, то рассматриваемую таблицу можно представить как показано ниже (таблица 3.1).

Таблица 3.1. Общий вид таблицы для шифра одинарной перестановки

m_1	m_2	…	m_n
j_1	j_2	…	j_n

В первую строку таблицы 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 таблиц вида 3.1.

Пример 2. Пусть M_i = «кибервойны», здесь $n = 10$. Далее принимаем правило (ключ) перестановки: $j_1=5$, $j_2=3$, $j_3=1$, $j_4=6$, $j_5=4$, $j_6=2$, $j_7=10$, $j_8=7$, $j_9=8$, $j_{10}=9$.

Составим таблицу для зашифрования сообщения в форме табл. 3.1.

Таблица 3.2

к	и	б	е	р	в	о	й	н	ы
5	3	1	6	4	2	10	7	8	9

Представим эту таблицу только числами.

Таблица 3.3.

1	2	3	4	5	6	7	8	9	10
5	3	1	6	4	2	10	7	8	9

В соответствии с принятым ключом зашифрованное сообщение будет иметь вид: C_i = «бвиркейныо».

Легко подсчитать, что при отсутствии повторяющихся букв в шифруемом сообщении длиной *n* символов всего существует *n*! Неповторяющихся ключей.

Для расшифрования сообщения, следуя логике рассмотренных процедур зашифрования, нам нужно также составить таблицу, первой строкой которой будет зашифрованный текст (таблица 3.4.). Здесь применяется примерно такой же подход, как и в шифрах подстановки.

Таблица 3.4.

б	в	и	р	к	е	й	н	ы	о
1	2	3	4	5	6	7	8	9	10

Таблицу 3.4 дополним 3-ей строкой, числа в столбцах которой соответствуют первой строке таблицы 3.3, одновременно составляя неизменную пару: 1 соответствует 3, 2 – 6 и т.д. (см. табл. 3.5).

Таблица 3.5

б	в	и	р	к	е	й	н	ы	о
1	2	3	4	5	6	7	8	9	10
3	6	2	5	1	4	8	9	10	9

Теперь расшифрованному сообщению «бвиркейныо» будет соответствовать обратная перестановка: символы первой строки таблицы 3.5 нужно расположить в порядке в соответствии с 3-й строкой: 1 – «к», 2 – «и» и т. д.

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, которые изучались и анализировались в лабораторной работе №7 из [1].

3.1.1.2. Шифры простой блочной перестановки

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

Пример 3. Пусть M_i = «кибервойны», примем длину блока, равную 2.

Для зашифрования построим таблицу (табл. 3.6).

Таблица 3.6

ки	бе	рв	ой	ны
5	1	4	2	3

В соответствии с табл. 3.6 получим C_i = «беойнырвки». Расшифрование производится по правилам, схожим с правилами для шифров простой перестановки.

3.1.1.3. Шифры маршрутной перестановки

Основой современных шифров рассматриваемого типа является геометрическая фигура. Обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слева-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 (см. аналогию с методами перемежения/деперемежения данных в лабораторной работе №7 [1]).

Шифр Скитала (Сцитала). Известно, что в V веке 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 [15]

Для зашифрования и расшифрования необходимо было иметь абсолютно одинаковые жезлы. На такой предмет наматывалась пергаментная лента. Далее на эту ленто построчно наносился текст. Для расшифрования ленту с передаваемым сообщением нужно было намотать так же, как и при нанесении открытого текста. Подобным образом работает шифр, который иллюстрирует пример на рисунке 3.5 в [2].

Следуя вышеприведенным рассуждениям, может отождествить скитала с таблицей размерами: 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 M_i:

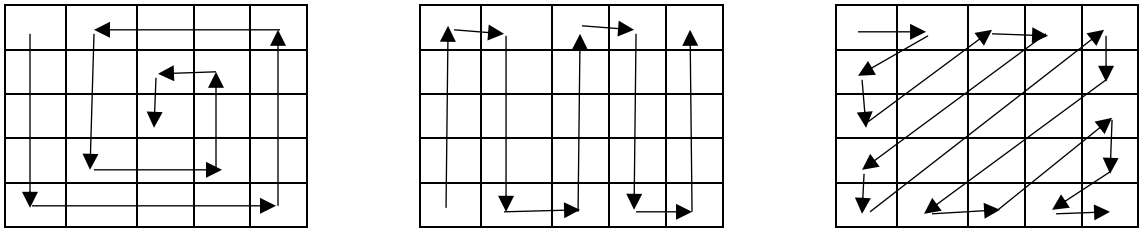
$$k = [(n - 1)/s] + 1. \qquad (3.1)$$

При этом слагаемое в квадратных скобках должно быть целым числом [15].

Нетрудно себе представить аналогию между Скитала и таблицей, которая «намотана» на цилиндр.

При использовании шифра Скитала для формирования шифртекста сначала выбирается 1-ая буква открытого текста, затем (k+1)-буква, (2k+1)-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 (см. рис. 3.2). Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.



а) б) в)

Рисунок 3.2 – Графическое представление методов маршрутной перестановки

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 х 4.

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.

3.1.1.4. 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: слева-направо, сверху-вниз;
- шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

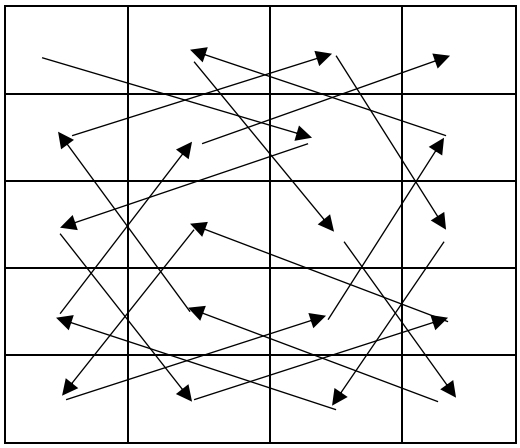


Рисунок 3.3 – Пример маршрута «обход конем»

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

Пример 4. Например, ключом является слово «крипто». Во-первых, это означает, что количество столбцов k в таблице должно быть равно длине ключа, т. е. – 6. Если вспомним порядок букв из ключевого слова в алфавите, то последовательность считывания столбцов будет следующим: 2, 5, 1, 4, 6, 3.

Необходимо зашифровать сообщение M_i = «шифр вертикальной перестановки»; n = 30.

Строим основную таблицу 5x6 (табл. 3.7), в которую по стокам будет записано исходное сообщение.

Считывая информацию из таблицы по столбцам в соответствии с ключом, получим шифрограмму C_i = «фтнрошелпава тириоевирьен кйск».

Таблица 3.7

к	*р*	*и*	*п*	*т*	*о*
2	5	1	4	6	3
ш	и	ф	р		в

е	р	т	и	к	а
л	ь	н	о	й	
п	е	р	е	с	т
а	н	о	в	к	и

3.1.2. Шифры множественной перестановки

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем 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.

Пример 5. Предположим, что (в продолжение к последнему примеру) вторым ключом будет «слово» или 5, 2, 3, 1, 4 (одинаковым буквам «о» мы присвоили последовательные числа).

Предыдущая таблица несколько видоизменится и примет следующий вид (табл. 3.8).

Таблица 3.8

ключи		*к*	*р*	*и*	*п*	*т*	*о*
		2	5	1	4	6	3
с	5	ш	и	ф	р		в
л	2	е	р	т	и	к	а
о	3	л	ь	н	о	й	
в	1	п	е	р	е	с	т
о	4	а	н	о	в	к	и

Для удобства отсортируем последовательно строки в соответствии с ключом (табл. 3.9).

Таблица 3.9

ключи	*к*	*р*	*и*	*п*	*т*	*о*
	2	5	1	4	6	3

в	1	п	е	р	е	с	т
л	2	е	р	т	и	к	а
о	3	л	ь	н	о	й	
о	4	а	н	о	в	к	и
с	5	ш	и	ф	р		в

И столбцы – в соответствии с ключевым словом «слово».

Таблица 3.10

ключи		*и*	*к*	*о*	*п*	*р*	*т*
		1	2	3	4	5	6
в	1	е	т	р	е	с	п
л	2	и	а	т	р	к	е
о	3	о		н	ь	й	л
о	4	в	и	о	н	к	а
с	5	р	в	ф	и		ш

Получим итоговую шифрограмму C_i = «еиоврта ивртноферьнискйк пелаш».

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 на другие.

Полезную информацию о классе рассмотренных шифров можно найти в [16, 17].

3.2 ПРАКТИЧЕСКОЕ ЗАДАНИЕ

Рекомендация! Перед выполнением практического задания целесообразно освежить практические навыки использования и особенностями функционирования программного средства *L_LUX*, реализующего перестановочные (и другие) методы зашифрования/расшифрования текстовой информации и являющегося приложением на компакт-диске к [5].

Обратим внимание на использование «горячих» клавиш для реализации некоторых операций:

Ctrl + F3 – зашифрование на основе простой перестановки,

Shift + F3 – расшифрование на основе простой перестановки,

Shift + Ctrl + F1 – вывод гистограмм (частотных параметров символов) исходного и зашифрованного сообщений,

Shift + Ctrl + F2 – вывод гистограмм (частотных параметров символов) зашифрованного и расшифрованного сообщений.

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;

Варианты задания

Вариант	алфавит	шифр
1	белорусский	1. Маршрутная перестановка (маршрут: запись – по строкам, считывание – по столбцам таблицы; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия
2	русский	1. Маршрутная перестановка (маршрут: по спирали; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия
3	английский	1. Маршрутная перестановка (маршрут: зигзагом; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия
4	немецкий	1. Маршрутная перестановка (маршрут: змейкой; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия
5	польский	1. Маршрутная перестановка (маршрут запись – по столбцам, считывание – по строкам таблицы; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия

- 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).*

Ниже представлен (Листинг 3.1) пример кода программы (класса *Encryption*) для зашифрования сообщения на основе табличного представления сообщений.

```
class Encryption{
{
        private int[] key = null;
        public void SetKey(string[] _key)
        {
            key=new int[_key.Length];
            for(int i=0;i<_key.Length;i++)
              key[i] = Convert.ToInt32(_key[i]);
        }
        public string Encrypt(string input)
        {
            for(int i=0;i<input.Length % key.Length;i++) input +=
input[i];

            string result = "";
            for(int i=0;i<input.Length;i+=key.Length)
            {
                char[] transposition = new char[key.Length];
                for(int j=0;j<key.Length;j++)
                        transposition[key[j]-1]=input[i+j];
                for(int j=0;j<key.Length;j++)
                        result += transposition[j];
            }
            return result;
        }
        public string Decrypt(string input)
        {
            string result = "";
            for(int i=0;i<input.Length;i+=key.Length)
            {
                char[] transposition = new char[key.Length];
                for(int j=0;j<key.Length;j++)
```

```
                        transposition[j] = input[i + key[j] - 1];
                for(int j=0;j<key.Length;j++) result += transposi-
tion[j];
            }
            return result;
        }
}
```

Листинг 3.1. Пример кода программы для зашифрования сообщения на основе табличного представления сообщений

При анализе полученных гистограмм можно сопоставить полученные данные с аналогичными результатами выполнения лабораторной работы №2 из [1] и лабораторной работы №2 настоящего пособия.

Если указанный в таблице язык исходного текста не известен разработчику программного средства, можно взять документ на требуемом языке и воспользоваться доступным электронным переводчиком (возникающие при этом отдельные семантические неточности не следует считать существенным недостатком выполняемого анализа).

2. Результаты оформить в виде отчета по установленным правилам.

ВОПРОСЫ ДЛЯ КОНТРОЛЯ И САМОКОНТРОЛЯ

1. В чем заключается основная идея криптографических преобразований на основе шифров перестановки?

2. Привести классификационные признаки и дать сравнительную характеристику разновидностям перестановочных шифров.

3. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?

4. Охарактеризовать криптостойкость перестановочных и подстановочных шифров.

5. Привести примеры дать характеристику перестановочным шифрам, не рассмотренным в материалах к данной лабораторной работе.

6. Имеются ли предпочтения в выборе размеров используемой таблицы для перестановочных шифров?

7. Охарактеризовать основные методы взлома перестановочных шифров.