ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по проведению лабораторных работ
для дисциплины «Основы криптографии»

Направление подготовки: 09.03.01 Информатика и вычислительная техника
Профиль: Вычислительные машины, комплексы, системы и сети

Ростов на Дону
2019

Рыбалко И.П. МЕТОДИЧЕСКИЕ УКАЗАНИЯ по проведению лабораторных работ по дисциплине «Основы криптографии»/ Рыбалко И.П. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019. – 59 с.: ил.

Методические указания соответствуют направлению подготовки 09.03.01 Информатика и вычислительная техника, Профиль: Вычислительные машины, комплексы, системы и сети.

В указаниях приведены общие сведения о криптографии. Рассмотрены основные методы симметричного и асимметричного шифрования. Приведены задания на выполнение лабораторных работ и даны рекомендации по их выполнению.

Указания предназначены для студентов любых форм обучения, изучающих информационную безопасность и защиту информации, а также специалистов, ведущим проектирование, разработку и эксплуатацию информационных систем.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На современном этапе развития общества ключевая роль во всех сферах человеческой деятельности отводиться информации. Тезис «кто владеет информацией, тот владеет миром» становиться все более актуальным. В настоящее время основная доля информационных ресурсов храниться в системах, основанных на компьютерных технологиях. Процесс подключения компьютеров к локальным сетям и глобальной сети Internet носит повсеместный характер. Это приводит к значительному повышению доступности информации, в т.ч. и конфиденциальной.

В связи с этим вопросам защиты компьютерной информации в последнее время уделяется повышенное внимание. При этом под **защитой информации** понимается комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе ее сбора, хранения, обработки и передачи в информационных системах.

Одним из самых распространенных средств защиты компьютерной информации является шифрование, которое широко используется для обеспечения конфиденциальности как хранимой, так и передаваемой по сетям информации.

Настоящие методические указания предназначены для изучения основ шифрования информации. В первой главе даны основные криптографические понятия, а также приведена классификация шифров. В остальных главах рассмотрены особенности шифрования, присущие каждому классу шифров, и приведены примеры конкретных алгоритмов шифрования.

Целью данных указаний является первоначальное ознакомление с основами шифрования и дешифрования информации. В них не рассматриваются теоретические основы криптографии, криптографические протоколы и т.д. Для этих целей рекомендуется воспользоваться [1, 2, 3].

Программа практических занятий разбита на пять лабораторных работ. Каждая из них рассчитана на срок от двух до трех занятий и посвящена изучению одного класса шифров. В течение первых трех лабораторных работ студент дол-

жен освоить базовые алгоритмы симметричного шифрования (шифры замены, перестановки и гаммирования). В четвертой лабораторной работе он должен изучить основы блочного шифрования на примере бывшего американского стандарта шифрования DES. В пятой лабораторной работе приводится описание трех алгоритмов асимметричного шифрования.

В течение этих занятий студент должен практически освоить весь материал по каждой лабораторной работе, выполнить задание, оформить отчет и защитить работу. При защите студент должен продемонстрировать степень усвоения материала, а также ответить на вопросы, связанные с темами текущей и уже пройденных лабораторных работ.

1. ОСНОВЫ КРИПТОГРАФИИ

Разработкой методов преобразования информации с целью обеспечения ее конфиденциальности и целостности занимается криптография (в переводе с греческого означает «тайнопись»). О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. С широким распространением письменности криптография стала формироваться как самостоятельная наука.

Одно из основных понятий криптографии - шифр (от араб. صِفْر , *ṣifr* «ноль», откуда фр. *chiffre* «цифра» - родственно слову цифра; арабы первыми стали заменять буквы на цифры с целью защиты исходного текста).

Под **шифром** понимается совокупность методов и способов обратимого преобразования информации с целью ее защиты от НСД.

Шифрование (зашифрование) — процесс применения шифра к защищаемой информации, т.е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, шифрограмму, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование - процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Алгоритм криптографического преобразования - набор математических правил, определяющих содержание и последовательность операций, зависящих от ключа шифрования, по шифрованию и дешифрованию информации.

Для шифрования и дешифрования, кроме алгоритма преобразования, необходимо, как правило, знание некоторой секретной информации, которая называется ключом. **Ключ шифра (секретный ключ)** – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозмож-

ных для данного алгоритма. В общем случае, **ключ** – это минимально необходимая информация (за исключением сообщения и алгоритма), необходимая для шифрования и дешифрования сообщений.

Используя понятие ключа, процессы шифрования и дешифрования можно описать в виде соотношений:

$$\mathbf{F(P, k_1) = C,} \quad (1)$$

$$\mathbf{G(C, k_2) = P,} \quad (2)$$

где **P** (англ. public - открытый) - открытое сообщение;

C (англ. cipher - шифрованный) - шифрованное сообщение;

F - правило шифрования;

G - правило расшифрования;

$\mathbf{k_1}$ – ключ зашифрования, известный отправителю;

$\mathbf{k_2}$ – ключ расшифрования, известный адресату.

В зависимости от особенностей алгоритма криптографического преобразования шифры можно разделить на следующие **классы**.

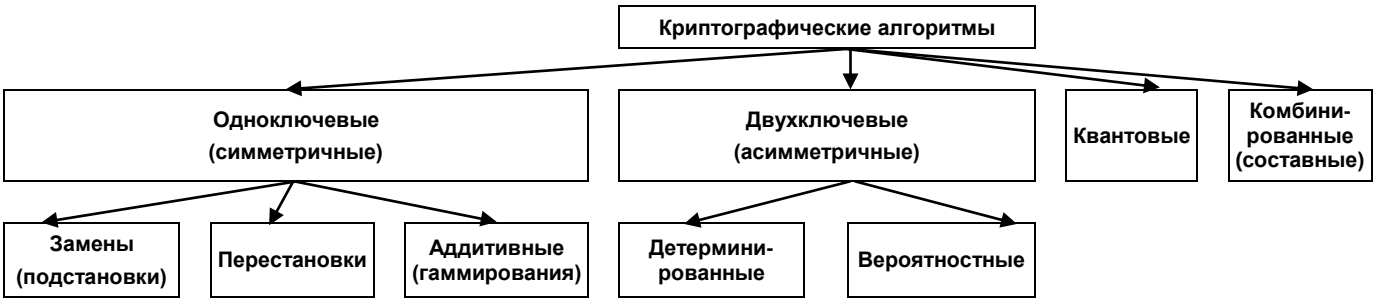


Рис.1. Классификация криптографических алгоритмов

В **одноключевых** системах для шифрования и дешифрования используется один и тот же ключ.

В шифрах **перестановки** все буквы открытого текста остаются в зашифрованном сообщении, но меняют свои позиции. В шифрах **замены** наоборот, позиции букв в шифровке остаются теми же, что и у открытого текста, но символы открытого текста заменяются символами другого алфавита.

В **аддитивных** шифрах буквы алфавита заменяются числами, к которым затем добавляются числа секретной случайной (псевдослучайной) числовой последовательности (гаммы). Состав гаммы меняется в зависимости от используемого ключа. Обычно для шифрования используется логическая операция «Исключающее ИЛИ» (XOR). При дешифровании та же гамма накладывается на зашифрованные данные. Гаммирование широко используется в военных криптографических системах.

В **двухключевых** системах для шифрования и дешифрования используется два совершено разных ключа. При использовании **детерминированного** алгоритма шифрование и расшифрование посредством соответствующей пары ключей возможно только единственным способом. **Вероятностный** алгоритм при шифровании одного и того же исходного сообщения с одним и тем же ключом может давать разные шифртексты, которые при расшифровке дают один и тот же результат.

Квантовая криптография вносит в процесс шифрования естественную неопределенность квантового мира. Процесс отправки и приёма информации выполняется посредством объектов квантовой механики, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. Самым ценным свойством этого вида шифрования является то, что при посылке сообщения отправляющая и принимающая сторона с достаточно большой вероятностью (99.99…%) могут установить факт перехвата зашифрованного сообщения.

Комбинированные (составные) методы предполагают использование для шифрования сообщения сразу нескольких методов (например, сначала замена символов, а затем их перестановка).

Все шифры по алгоритму преобразования также делят на потоковые и блочные. В **потоковых** шифрах преобразование выполняется отдельно над каждым символом исходного сообщения. Для **блочных** шифров информация разбивается на блоки фиксированной длины, каждый из которых шифруется и расшифровывается отдельно.

Кроме приведенной на рис.1 классификации, шифры в зависимости от особенностей алгоритма делят также на потоковые и блочные. В **потоковых шифрах** одна и та же процедура преобразования выполняется над каждым символом независимо от других. В **блочных шифрах** исходное сообщение разбивается на блоки фиксированной длины, каждый из которых шифруется и расшифровывается отдельно.

Одним из ключевых понятий в криптографии является **стойкость шифра (криптостойкость)** - способность шифра противостоять всевозможным атакам на него. Под **атакой на шифр** понимают попытку вскрытия этого шифра [2].

Среди наиболее важных **показателей криптостойкости**: количество всех возможных ключей шифра и среднее время, необходимое для криптоанализа (вскрытия).

Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра – проблема нерешенная. Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации криптоаналитиков, атакующих шифр. Такую процедуру иногда называют **проверкой стойкости** [2].

В зависимости от стойкости шифры делятся на три группы:

- совершенные шифры – шифры, заведомо неподдающиеся вскрытию (при правильном использовании);

- шифры, допускающие неоднозначное вскрытие (при попытке вскрытия противником конкретной шифрограммы он может получить несколько правдоподобных вариантов исходного сообщения);

- шифры, допускающие однозначное вскрытие (основная масса шифров).

2. ЛАБОРАТОРНАЯ РАБОТА № 1. ШИФРЫ ЗАМЕНЫ.

Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) **МА**, **Б** – **МБ**, …, **Я** – **МЯ**. Шифрозамены выбираются таким образом, чтобы любые два множества (**MI** и **MJ**, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{MI} \cap \mathbf{MJ} = \varnothing$).

Таблица, приведенная на рис.2, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.

А	Б	…	Я
$М_А$	$М_Б$	…	$М_Я$

Рис.2. Таблица шифрозамен

При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_A}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_A}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения.

Так как множества $\mathbf{M_A}$, $\mathbf{M_Б}$, ..., $\mathbf{M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом.

Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»).

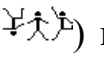
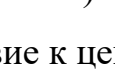
Шифры замены можно разделить на следующие **подклассы**:

- шифры однозначной замены (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 ($|\mathbf{M_i}|=1$ для одного символа);

- полиграммные шифры. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения ($|\mathbf{M_i}|=1$ для блока символов);

- омофонические шифры (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 ($|\mathbf{M_i}|\geq 1$ для одного символа);

- полиалфавитные шифры (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования ($|\mathbf{M_i}|>1$ для одного символа).

Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли».

I. Шифры однозначной замены.

Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа n значение **n!** растет очень быстро (1!=1, 5!=120, 10!=3628800, 15!=1307674368000). При больших **n** для приближенного вычисления n! можно воспользоваться формулой Стирлинга

$$n! \approx \sqrt{2\pi n} * \left(\frac{n}{e}\right)^n \quad (3).$$

Шифр Цезаря. Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю	Я	А	Б	В

Рис.3. Таблица шифрозамен для шифра Цезаря

При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть **«ГДУГПСЕ»**. Получатель сообщения **«ГДУГПСЕ»** ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение **«АБРАМОВ»**.

Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр.

Лозунговый шифр. Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю	Я
Д	Я	И	Н	А	Б	В	Г	Е	Ё	Ж	З	Й	К	Л	М	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю

Рис.4. Таблица шифрозамен для лозунгового шифра

При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ».

В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$).

Полибианский квадрат. Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Рис.5. Таблица шифрозамен для полибианского квадрата

Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца.

Шифрующая система Трисемуса (Тритемия). В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфа-

вита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».

Д	**Я**	**И**	**Н**	**А**	**Б**	**В**	**Г**
Е	**Ё**	**Ж**	**З**	**И**	**Й**	**К**	**Л**
М	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**
Х	**Ш**	**Щ**	**Ъ**	**Ы**	**Э**	**Ю**	

Рис.6. Таблица шифрозамен для шифра Трисемуса

Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК».

Одним из существенных **недостатков шифров однозначной замены** является их легкая вскрываемость. При вскрытии шифрограмм используются различные приемы, которые даже при отсутствии мощных вычислительных средств позволяют добиться положительного результата. Один из таких приемов базируется на том, что в шифрограммах остается информация о частоте встречаемости букв исходного текста. Если в открытом сообщении часто встречается какая-либо буква, то в шифрованном сообщении также часто будет встречаться соответствующий ей символ. Еще в 1412 году Шихаба ал-Калкашанди в своем труде «Субх ал-Ааша» привел таблицу частоты появления арабских букв в тексте на основе анализа текста Корана. Для разных языков мира существуют подобные таблицы. Так, например, для русского языка такая таблица выглядит следующим образом [7].

Таблица 1

Вероятности появления букв русского языка в текстах*

Буква (символ)	Вероятность	Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
Пробел	0.146	Р	0.042	Я	0.017	Ж	0.007
О	0.094	Л	0.039	З	0.016	Ш	0.006
Е	0.071	В	0.038	Ы	0.015	Ц, Ю	0.005
А	0.069	К	0.029	Г	0.014	Щ	0.004
И	0.064	М	0.027	Ь, Б	0.013	Ф	0.003
Н	0.057	П	0.026	Ч	0.012	Э	0.002
Т	0.054	Д	0.024	Й	0.010	Ъ	0.001
С	0.046	У	0.023	Х	0.008		

*) В таблице приведены оценки вероятностей появления букв русского языка и пробела, полученные на основе анализа научно-технических и художественных текстов общим объемом более 1000000 символов.

Существуют подобные таблицы для пар букв (биграмм). Например, часто встречаемыми биграммами являются «то», «но», «ст», «по», «ен» и т.д. Другой прием вскрытия шифрограмм основан на исключении возможных сочетаний букв. Например, в текстах (если они написаны без орфографических ошибок) нельзя встретить сочетания «чя», «щы», «ьъ» и т.п.

Для усложнения задачи вскрытия шифров однозначной замены еще в древности перед шифрованием из исходных сообщений исключали пробелы и/или гласные буквы. Другим способом, затрудняющим вскрытие, является шифрование **биграммами** (парами букв).

II. Полиграммные шифры.

Полиграммные шифры замены - это шифры, которые шифруют сразу группы (блоки) символов.

Шифр Playfair ("Честная игра"). Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с

шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26x26=676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **«X»**, для русского алфавита - «Я»). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг **«ДЯДИНА»**

Д	**Я**	**И**	**Н**	**А**	**Б**
В	**Г**	**Е**	**Ё**	**Ж**	**З**
Й	**К**	**Л**	**М**	**О**	**П**
Р	**С**	**Т**	**У**	**Ф**	**Х**
Ц	**Ч**	**Ш**	**Щ**	**Ы**	**Ь**
Ъ	**Э**	**Ю**	**-**	**-**	**-**

Рис.7. Ключевая таблица для шифра Playfair

Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

1. Если символы биграммы 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 биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Пример шифрования.

- биграмма «за» формирует прямоугольник – заменяется на «жб»;
- биграмма «ши» находятся в одном столбце – заменяется на «юе»;
- биграмма «фр» находятся в одной строке – заменяется на «хс»;
- биграмма «ов» формирует прямоугольник – заменяется на «йж»;
- биграмма «ан» находятся в одной строке – заменяется на «ба»;
- биграмма «но» формирует прямоугольник – заменяется на «ам»;
- биграмма «ес» формирует прямоугольник – заменяется на «гт»;
- биграмма «оя» формирует прямоугольник – заменяется на «ка»;
- биграмма «об» формирует прямоугольник – заменяется на «па»;
- биграмма «ще» формирует прямоугольник – заменяется на «шё»;
- биграмма «ни» формирует прямоугольник – заменяется на «ан»;
- биграмма «ея» формирует прямоугольник – заменяется на «ги».

Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги».

Для расшифровки необходимо использовать инверсию этих правил, откидывая символы «Я» (или «Х»), если они не несут смысла в исходном сообщении.

III. Омофонические шифры.

Другое направление повышения стойкости шифров замены состоит в том, чтобы каждое множество шифрообозначений $\mathbf{M_i}$ содержало более одного элемента. При использовании такого шифра одну и ту же букву (если она встречается несколько раз в сообщении) заменяют на разные шифрозамены из $\mathbf{M_i}$. Это позволяет скрыть истинную частоту встречаемости букв открытого сообщения.

Система омофонов. В 1401 г. Симеоне де Крема стал использовать таблицы омофонов для сокрытия частоты появления гласных букв в тексте при помощи

более чем одной шифрозамены. Такие шифры позже стали называться шифрами многозначной замены или омофонами[1]. Они получили развитие в XV веке. В книге «Трактат о шифрах» Леона Баттисты Альберти (итальянский ученый, архитектор, теоретик искусства, секретарь папы Климентия XII), опубликованной в 1466 г., приводится описание шифра замены, в котором каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости буквы в открытом тексте. Так, если ориентироваться на табл.1, то число шифрозамен для буквы **О** должно составлять 94, для буквы **Е** – 71 и т.д. При этом каждая шифрозамена должна состоять из 3 цифр и их общее количество равно 1000. На рис.8 представлен фрагмент таблицы шифрозамен.

№ п/п	Пробел	А	Б	В	…	М	…	О	…	Р	…	Я
1	012	311	128	175	…	037	…	248	…	064	…	266
2	042	357	950	194	…	149	…	267	…	189	…	333
…	…	…	…	…	…	…	…	…	…	…	…	…
13	278	495	990	199	…	349	…	303	…	374	…	749
…	…	…		…	…	…	…	…	…	…	…	…
17	342	519		427	…	760	…	306	…	469	…	845
…	…	…		…	…	…	…	…	…	…		
27	437	637		524	…	777	…	432	…	554		
…	…	…		…				…	…	…		
38	457	678		644				824	…	721		
…	…	…						…	…	…		
42	628	776						828	…	954		
…	…	…						…				
69	681	901						886				
…	…							…				
94	974							903				
…	…											
146	976											

Рис.8. Фрагмент таблицы шифрозамен для системы омофонов

При шифровании символ исходного сообщения заменяется на любую шифрозамену из своего столбца. Если символ встречается повторно, то, как правило,

[1] **Омофоны** (греч. ὁμός - одинаковый + φωνή - звук) - слова, которые звучат одинаково, но пишутся по-разному и имеют разное значение.

используют разные шифрозамены. Например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «357 990 374 678 037 828 175».

Книжный шифр. Заметным вкладом греческого ученого Энея Тактика в криптографию является предложенный им так называемый книжный шифр, описанный в сочинении «Об обороне укреплённых мест». Эней предложил прокалывать малозаметные дырки в книге или в другом документе над буквами секретного сообщения. Интересно отметить, что в первой мировой войне германские шпионы использовали аналогичный шифр, заменив дырки на точки, наносимые симпатическими чернилами[2] на буквы газетного текста.

После первой мировой войны книжный шифр приобрел иной вид. Шифрозамена для каждой буквы определялась набором цифр, которые указывали на номер страницы, строки и позиции в строке. Количество книг, изданных за всю историю человечества, является величиной ограниченной (по крайней мере, явно меньше, чем 15!). Однако отсутствие полной электронной базы по изданиям делает процедуру вскрытия шифрограмм почти не выполнимой. В связи с этим книжный шифр относят к категории совершенных.

IV. Полиалфавитные шифры.

Полиалфавитные шифры состоят из нескольких шифров однозначной замены и отличаются друг от друга способом выбор варианта алфавита для зашифрования одного символа.

Диск Альберти. В «Трактате о шифрах» Альберти приводит также первое точное описание многоалфавитного шифра на основе шифровального диска.

[2] **Симпатические (невидимые) чернила** — это чернила, записи которыми являются изначально невидимыми и становятся видимыми только при определенных условиях (нагрев, освещение, химический проявитель и т. д.).

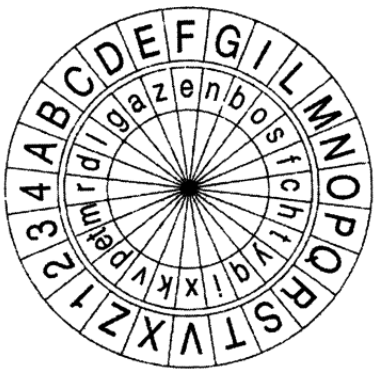


Рис.9. Диск Альберти

Он состоял из двух дисков – внешнего неподвижного (на нем были нанесены буквы в алфавитном порядке и цифры 1,2,3,4) и подвижного внутреннего диска на котором буквы были переставлены. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по новому шифралфавиту. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

Таблица Трисемуса. Одним из шифров, придуманных немецким аббатом Трисемусом, стал многоалфавитный шифр, основанный на так называемой «таблице Трисемуса» - таблице со стороной равной **n**, где **n** – количество символов в алфавите. В первой строке матрицы записываются буквы в порядке их очередности в алфавите, во второй – та же последовательность букв, но с циклическим сдвигом на одну позицию влево, в третьей – с циклическим сдвигом на две позиции влево и т.д.

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Рис.10. Таблица Трисемуса

Здесь первая строка является одновременно и строкой букв открытого текста. Первая буква текста шифруется по первой строке, вторая буква по второй и так далее после использования последней строки вновь возвращаются к первой. Так сообщение «АБРАМОВ» приобретет вид «АВТГРУИ».

Система шифрования Виженера. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

Перед шифрованием выбирается ключ из символов алфавита. Сама процедура шифрования заключается в следующем. По i-ому символу открытого сообщения в первой строке определяется столбец, а по i-ому символу ключа в крайнем левом столбце – строка. На пересечении строки и столбца будет находиться i-ый

символ, помещаемый в шифрограмму. Если длина ключа меньше сообщения, то он используется повторно. Например, исходное сообщение **«АБРАМОВ»**, ключ – **«ДЯДИНА»**, шифрограмма – **«ДАФИЩОЖ»**.

Справедливости ради, следует отметить, что авторство данного шифра принадлежит итальянцу Джованни Батиста Беллазо, который описал его в 1553 г. История «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания» (Давид Канн, «Взломщики кодов»). Беллазо предложил называть секретное слово или фразу **паролем** (ит. password; фр. parole - слово).

Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- шифра Цезаря;
- лозунгового шифра;
- полибианского квадрата;
- шифрующей системы Трисемуса;
- шифра Playfair;
- системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
- шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.

3. ЛАБОРАТОРНАЯ РАБОТА № 2. ШИФРЫ ПЕРЕСТАНОВКИ

Все шифры перестановки делятся на два **подкласса**:

- шифры одинарной (простой) перестановки. При шифровании символы перемещаются с исходных позиций в новые один раз;

- шифры множественной (сложной) перестановки. При шифровании символы перемещаются с исходных позиций в новые несколько раз.

I. Шифры одинарной перестановки.

В общем случае для данного класса шифров при шифровании и дешифровании используется таблица перестановок.

1	**2**	**3**	**…**	**n**
l_1	l_2	l_3	…	l_n

Рис.11. Таблица перестановок

В первой строке данной таблицы указывается позиция символа в исходном сообщении, а во второй – его позиция в шифрограмме. Таким образом, максимальное количество ключей для шифров перестановки равно **n!**, где **n** – длина сообщения.

Шифр простой одинарной перестановки. Для шифрования и дешифрования используется таблица перестановок, аналогичная показанной на рис.12.

1	2	3	4	5	6	7
2	4	1	7	6	5	3

Рис.12. Таблица перестановок

Например, если для шифрования исходного сообщения «АБРАМОВ» использовать таблицу, представленную на рис.12, то шифрограммой будет «РАВБОМА». Для использования на практике такой шифр не удобен, так как при больших значениях **n** приходится работать с длинными таблицами и для сообщений разной длины необходимо иметь свою таблицу перестановок.

Шифр блочной одинарной перестановки. При использовании этого шифра задается таблица перестановки блока символов, которая последовательно применяется до тех пор, пока исходное сообщение не закончится. Если исходное сообщение не кратно размеру блока, тогда оно при шифровании дополняется произвольными символами.

1	**2**	**3**
2	**3**	**1**

Рис.13. Таблица перестановок

Для примера выберем размер блока, равный 3, и примем таблицу перестановок, показанную на рис.13. Дополним исходное сообщение **«АБРАМОВ»** буквами **Ь** и **Э**, чтобы его длина была кратна 3. В результате шифрования получим **«РАБОАМЭВЬ»**.

Количество ключей для данного шифра при фиксированном размере блока равно **m!**, где **m** – размер блока.

Шифры маршрутной перестановки. Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что в фигуру исходный текст вписывается по ходу одного маршрута, а выписывается по другому. Один из таких шифров – шифр «Сцитала» - упоминался ранее. Некоторые из них приводятся ниже.

Шифр табличной маршрутной перестановки. Наибольшее распространение получили шифры маршрутной перестановки, основанные на таблицах. При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) - по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

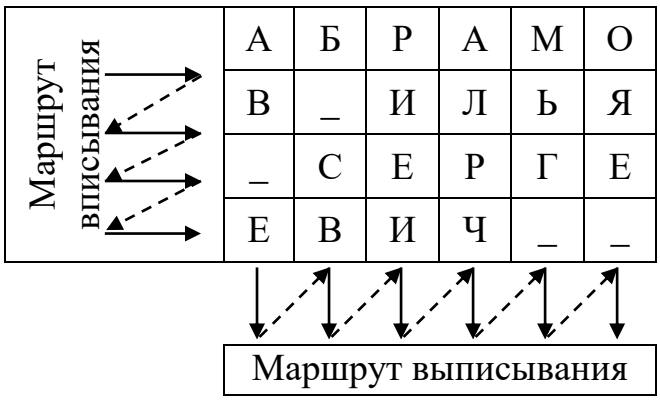


Рис.14. Пример использования шифра маршрутной перестановки

Например, исходное сообщения **«АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ»** вписывается в прямоугольную таблицу размерами 4х6, маршрут вписывания – слева-направо сверху-вниз, маршрут выписывания – сверху-вниз слева-направо. Шифрограмма в этом случае выглядит **«АВ_ЕБ_СВРИЕИАЛР ЧМЫГ_ОЯЕ_».**

Шифр вертикальной перестановки. Является разновидностью предыдущего шифра. К особенностям шифра можно отнести следующие:

- количество столбцов в таблице фиксируется и определяется длиной ключа;

- маршрут вписывания строго соответствует маршруту, показанному на рис.14;

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

Ключ	**Д**	**Я**	**Д**	**И**	**Н**	**А**
	2	**6**	**3**	**4**	**5**	**1**
Текст	**А**	**Б**	**Р**	**А**	**М**	**О**
	В	**_**	**И**	**Л**	**Ь**	**Я**
	_	**С**	**Е**	**Р**	**Г**	**Е**
	Е	**В**	**И**	**Ч**	**_**	**_**

Рис.15. Пример использования шифра вертикальной перестановки

В качестве ключа можно использовать слово или фразу. Тогда порядок выписывания столбцов соответствует алфавитному порядку букв в ключе. Напри-

мер, если ключевым словом будет **«ДЯДИНА»**, то присутствующая в нем буква **А** получает номер 1, **Д** – 2 и т.д. Если какая-то буква входит в слово несколько раз, то ее появления нумеруются последовательно слева направо. В примере первая буква **Д** получает номер 2, вторая **Д** – 3.

При шифровании сообщения **«АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ»** результат будет **«ОЯЕ_АВ_ЕРИЕИАЛРЧМЬГ_Б_СВ»**.

Шифр «Поворотная решетка». В 1550 году итальянский математик Джероламо Кардано[3], состоящий на службе у папы Римского, в книге «О тонкостях» предложил новую технику шифрования - решётку Кардано. Ее считают первым **транспозиционным** шифром, или, как ещё называют, геометрическим шифром, основанным на положении букв в шифртексте.

Для шифрования и дешифрования изготовляется прямоугольный трафарет с четным количеством строк и столбцов. В трафарете вырезаются клетки таким образом, чтобы при наложении его на таблицу того же размера четырьмя возможными способами, его вырезы полностью покрывали все ячейки таблицы ровно по одному разу.

При шифровании трафарет накладывается на таблицу. В видимые ячейки таблицы выписываются буквы исходного текста слева-направо сверху-вниз. Далее трафарет поворачивается и вписывается следующая часть букв. Эта операция повторяется еще два раза. Шифрограмму выписывают из итоговой таблицы по определенному маршруту.

Таким образом, ключом при шифровании является трафарет, порядок его поворотов и маршрут выписывания.

Пример шифрования сообщения **«АБРАМОВ+ДЯДИНА»** показан на рис.16. Результат шифрования – **«АДВ_МНРДБЯ+_ОААИ».**

[3] Джелорамо Кардано (1501 – 1576 гг.) - итальянский математик, инженер, философ, медик и астролог. В его честь названы открытые Сципионом дель Ферро формулы решения кубического уравнения (Кардано первым их опубликовал) и карданный вал (известного ещё Леонардо да Винчи).

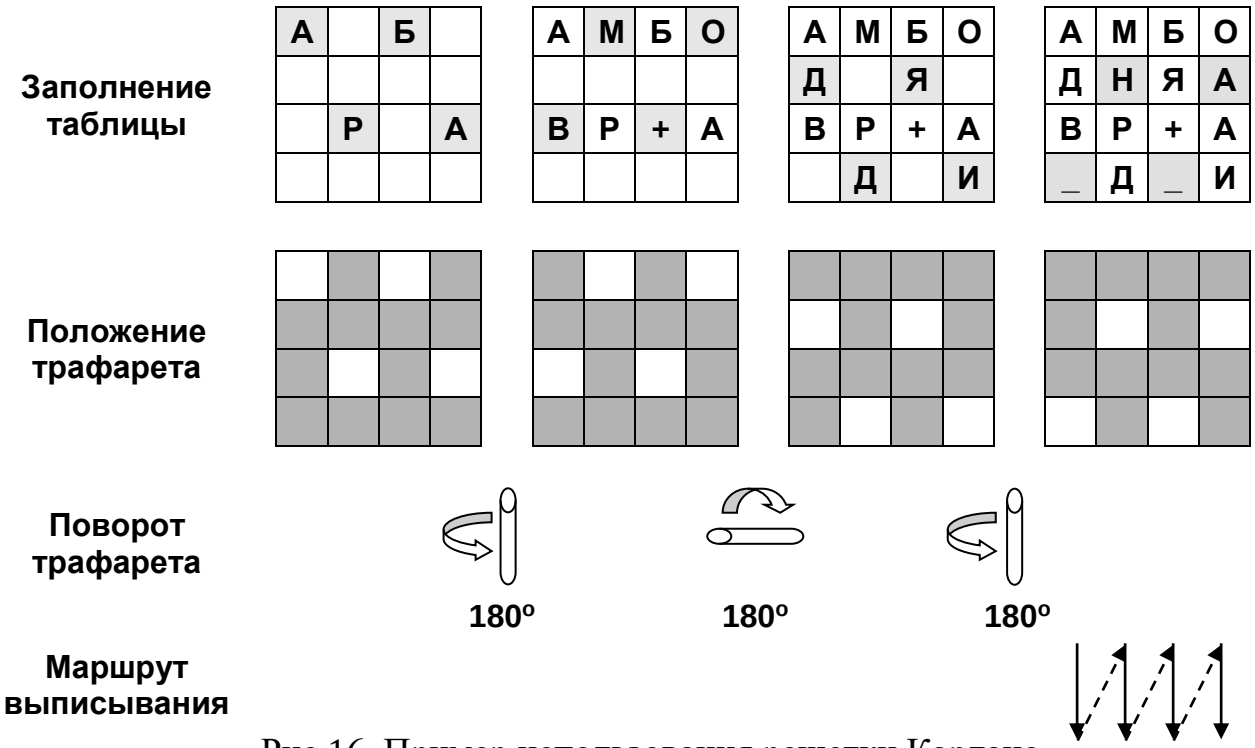
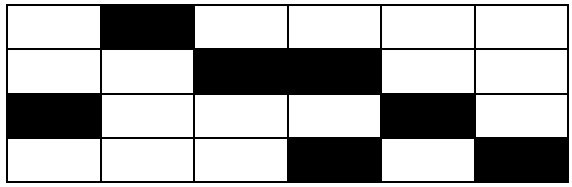


Рис.16. Пример использования решетки Кардано

Шифр Ришелье. В основу шифра положена решетка Карадно. Обычная решетка представляла собой лист из твердого материала, в котором через неправильные интервалы сделаны прямоугольные вырезы высотой для одной строчки и различной длины. Накладывая эту решетку на лист писчей бумаги, можно было записывать в вырезы секретное сообщение (букву, слог или целое слово). После этого, сняв решетку, нужно было заполнить оставшиеся свободные места на листе бумаги неким текстом, маскирующим секретное сообщение.



	А				
		Б	**Р**		
А				**М**	
			О		**В**

П	**А**	О	И	Ы	П
А	О	**Б**	**Р**	Л	Ь
А	М	И	Я	**М**	Г
В	Ц	Д	**О**	Ж	**В**

Рис.17. Пример использования шифра Ришелье

При переписке Ришелье использовал прямоугольник размера 7x10. Для длинных сообщений прямоугольник использовался несколько раз. Подобным методом маскировки сообщения пользовался известный русский писатель, общественный деятель и дипломат А. С. Грибоедов. Будучи послом в Персии, он писал своей жене «невинные» послания, которые, попав в руки жандармерии, для которой и были предназначены, расшифровывались по соответствующей «решетке» и передавались царскому правительству уже как секретные сведения. Пример использования решетки Ришелье можно было также видеть в титрах легендарного советского сериала о Шерлоке Холмсе.

Следует отметить, что данный способ шифрования относится к стеганографии, нежели криптографии.

Магические квадраты. Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые в сумме по каждому столбцу, каждой строке и каждой диагонали дают одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 x 3, если не принимать во внимание его повороты. Магических квадратов 4 x 4 насчитывается уже 880, а число магических квадратов размером 5 x 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

Рассмотри квадрат размером 4 x 4. В него вписываются числа от 1 до 16. Его магия состоит в том, что сумма чисел по строкам, столбцам и полным

диагоналям равняется одному и тому же числу - 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Рис.18. Магический квадрат 4 х 4

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: «АБРАМОВДЯДИНА...». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу. В пустые клетки ставится точка или любая буква.

16 .	3 Р	2 Б	13 А
5 М	10 Д	11 И	8 Д
9 Я	6 О	7 В	12 Н
4 А	15 .	14 .	1 А

Рис.19. Пример шифрования с помощью магического квадрата

После этого шифрованный текст записывается в строку (считывание производится слева-направо сверху-вниз, построчно) – «.РБАМДИДЯОВНА..А».

II. Шифры множественной перестановки.

В данном подклассе шифров используется идея повторного шифрования уже зашифрованного сообщения.

Шифр двойной перестановки. В таблицу по определенному маршруту записывается текст сообщения, затем переставляются столбцы, а потом переставляются строки. Шифрограмма выписывается по определенному маршруту.

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на рис.20. Результат шифрования – «ОАБЯ+_АИВ_РДМНАД».

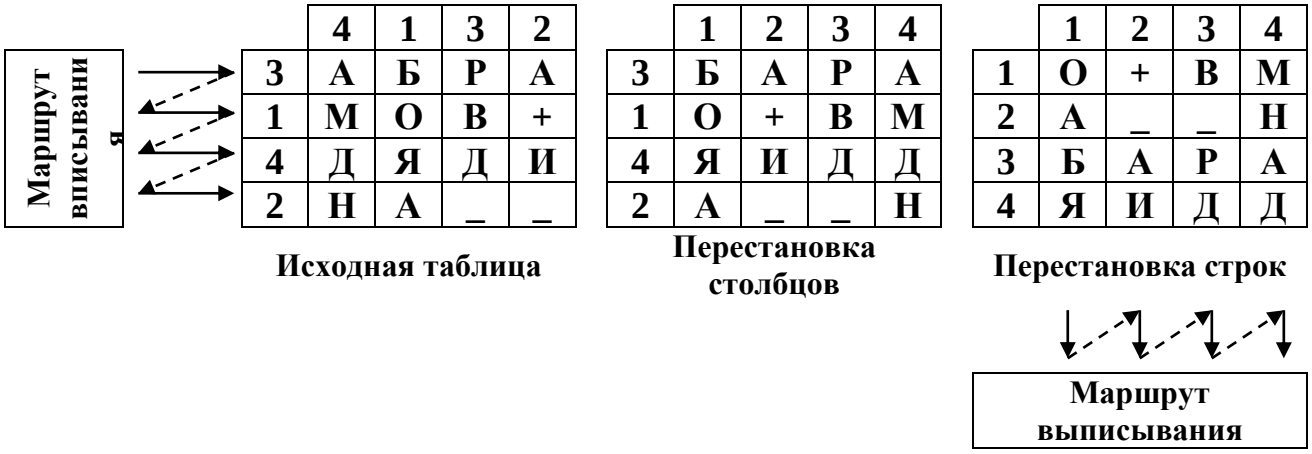


Рис.20. Пример использования шифра двойной перестановки

Ключом к шифру являются размеры таблицы, маршруты вписывания и выписывания, а также порядки перестановки столбцов и строк. Если маршруты являются фиксированными величинами, то количество ключей равно **n!*m!**, **n** и **m** – количество столбцов и строк в таблице.

Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию (для первых двух шифров) или фамилию и имя (для остальных) с помощью следующих шифров:

- простой одинарной перестановки;
- блочной одинарной перестановки;
- табличной маршрутной перестановки;
- вертикальной перестановки;
- поворотной решетки;
- магический квадрат (размер квадрата - 4x4);
- двойной перестановки.

При оформлении отчета необходимо привести исходное сообщение (фамилию или фамилию и имя), таблицы, ключевые слова (выбираются произвольно), маршруты вписывания и выписывания, повороты решетки и зашифрованное сообщение.

4. ЛАБОРАТОРНАЯ РАБОТА № 3. АДДИТИВНЫЕ ШИФРЫ

В аддитивных шифрах используется сложение по модулю (**mod**) исходного сообщения с гаммой, представленных в числовом виде. Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, 5+10 mod 4 = 15 mod 4 = 3).

В литературе шифры этого класса часто называют **потоковыми**. Стойкость закрытия этими шифрами определяется, главным образом, качеством гаммы, которое зависит от длины периода и случайности распределения по периоду [1].

Длиною периода гаммы называется минимальное количество символов, после которого последовательность начинает повторяться. **Случайность распределения символов** по периоду означает отсутствие закономерностей между появлением различных символов в пределах периода.

По длине периода различаются гаммы с **конечным и бесконечным периодом**. Если длина периода гаммы превышает длину шифруемого текста, гамма является истинно случайной и не используется для шифрования других сообщений, то такое преобразование является абсолютно стойким (совершенный шифр). Такой шифр нельзя вскрыть на основе статистической обработки шифрограммы.

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы

$$\mathbf{C_i = (P_i + K_i) \bmod N,} \qquad (4)$$

$$\mathbf{P_i = (C_i + N - K_i) \bmod N,} \qquad (5)$$

где $\mathbf{P_i, C_i}$ - i-ый символ открытого и шифрованного сообщения;

N - количество символов в алфавите;

$\mathbf{K_i}$ - i-ый символ гаммы (ключа). Если длина гаммы меньше, чем длина сообщения, то она используется повторно.

Данный метод шифрования воспроизводит зашифрование / расшифрование по Виженеру при замене букв алфавита числами согласно следующей таблице (применительно к русскому алфавиту):

А	Б	В	Г	Д	Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ъ	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Рис.21. Таблица кодирования символов

Например, для шифрования используется русский алфавит (**N = 32,** буква **Ё** эквивалентна **Е** и не учитывается), открытое сообщение – **«АБРАМОВ»**, гамма – **«ЖУРИХИН».** При замене символов на числа буква **А** будет представлена как 0, **Б** – 1, …, **Я** – 31. Результат шифрования показан в следующей таблице.

Таблица 2

Пример аддитивного шифрования по модулю N

Символ								
	открытого сообщения, P_i	А	Б	Р	А	М	О	В
		0	1	16	0	12	14	2
	гаммы, K_i	Ж	У	Р	И	Х	И	Н
		6	19	16	8	21	8	13
	шифрограммы, C_i	Ж	Ф	А	И	Б	Ц	П
		6	20	0	8	1	22	15

Сложение по модулю 2. Является частным случаем предыдущего шифра и используется при шифровании в автоматизированных системах. Символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по модулю 2 (⊕, для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»). Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C_i = P_i \oplus K_i, \quad (6)$$

$$P_i = C_i \oplus K_i. \quad (7)$$

Перед иллюстрацией использования шифра приведем таблицу кодов символов Windows 1251 и их двоичное представление.

Таблица 3

Коды символов Windows 1251 и их двоичное представление

Буква	Dec-код	Bin-код	Буква	Dec-код	Bin-код	Буква	Dec-код	Bin-код
А	192	1100 0000	Л	203	1100 1011	Ц	214	1101 0110
Б	193	1100 0001	М	204	1100 1100	Ч	215	1101 0111
В	194	1100 0010	Н	205	1100 1101	Ш	216	1101 1000
Г	195	1100 0011	О	206	1100 1110	Щ	217	1101 1001
Д	196	1100 0100	П	207	1100 1111	Ъ	218	1101 1010
Е	197	1100 0101	Р	208	1101 0000	Ы	219	1101 1011
Ж	198	1100 0110	С	209	1101 0001	Ь	220	1101 1100
З	199	1100 0111	Т	210	1101 0010	Э	221	1101 1101
И	200	1100 1000	У	211	1101 0011	Ю	222	1101 1110
Й	201	1100 1001	Ф	212	1101 0100	Я	223	1101 1111
К	202	1100 1010	Х	213	1101 0101			

Примечание. Dec-код – десятичный код символа, Bin-код – двоичный код символа.

Пример шифрования сообщения «ВОВА» с помощью гаммы «ЮЛЯ» показан в следующей таблице.

Таблица 4

Пример аддитивного шифрования по модулю 2

Открытое сообщение	Буква	В	О	В	А
	Dec-код	194	206	194	192
	Bin-код	1100 0010	1100 1110	1100 0010	1100 0000
Гамма	Буква	Ю	Л	Я	Ю
	Dec-код	222	203	223	222
	Bin-код	1101 1110	1100 1011	1101 1111	1101 1110
Шифрограмма	Dec-код	28	5	29	30
	Bin-код	0001 1100	0000 0101	0001 1101	0001 1110

Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию двумя рассмотренными выше способами. При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы шифрования (см. табл.2 и 4).

5. ЛАБОРАТОРНАЯ РАБОТА № 4. КОМБИНИРОВАННЫЕ ШИФРЫ

Среди комбинированных методов шифрования наиболее распространенными являются методы блочного шифрования. Блочное шифрование предполагает разбиение исходного открытого текста на равные блоки, к которым применяется однотипная процедура шифрования. В настоящее время блочные шифры широко используются на практике. Российский и американский стандарты шифрования относятся именно к этому классу шифров.

DES (Data Encryption Standard, стандарт шифрования данных) - федеральный стандарт шифрования США в 1977-2001 годах [5] **для использования во всех несекретных правительственных каналах связи** (FIPS PUB 46 «Data Encryption Standard»). Несмотря на то, что в настоящий момент федеральным стандартом шифрования США является Rijndael (AES - Advanced Encryption Standard, расширенный стандарт шифрования; тип – подстановочно - перестановочная сеть), рассмотрение DES позволяет понять основные принципы блочного шифрования.

В алгоритме, лежащем в основе DES, используются методы замены, перестановки и гаммирования (сложение по модулю 2).

Открытое сообщение разбивается на блоки длиной 64 бита. Если длина сообщения не кратна 64, оно дополняется справа недостающим количеством битов.

Данные шифруются ключом длиной 56 бит. На самом деле ключ имеет размер 64 бита, однако реально для выработки ключевых элементов используются только 56 из них. Самые младшие биты каждого байта ключа (8-ой, 16-ый, …, 64-ый) не попадают в ключевые элементы и служат исключительно для контроля четности. Требуется, чтобы сумма битов каждого байта ключа, включая контрольный, была четной.

Для решения разнообразных криптографических задач, разработаны четыре рабочих режима, реализующих DES:

- электронная кодовая книга ECB (Electronic Code Book);

- сцепление блоков шифра CBC (Cipher Block Chaining);

- обратная связь по шифртексту CPB (Cipher Feed Back);

- обратная связь по выходу OFB (Output Feed Back).

Режим ECB (электронная кодовая книга - Electronic Code Book).

Открытое сообщение разбивают на 64-битовые блоки. Каждый из них шифруют независимо с использованием одного и того же ключа шифрования.

Общая схема шифрования блока изображена на рис.22 [6].

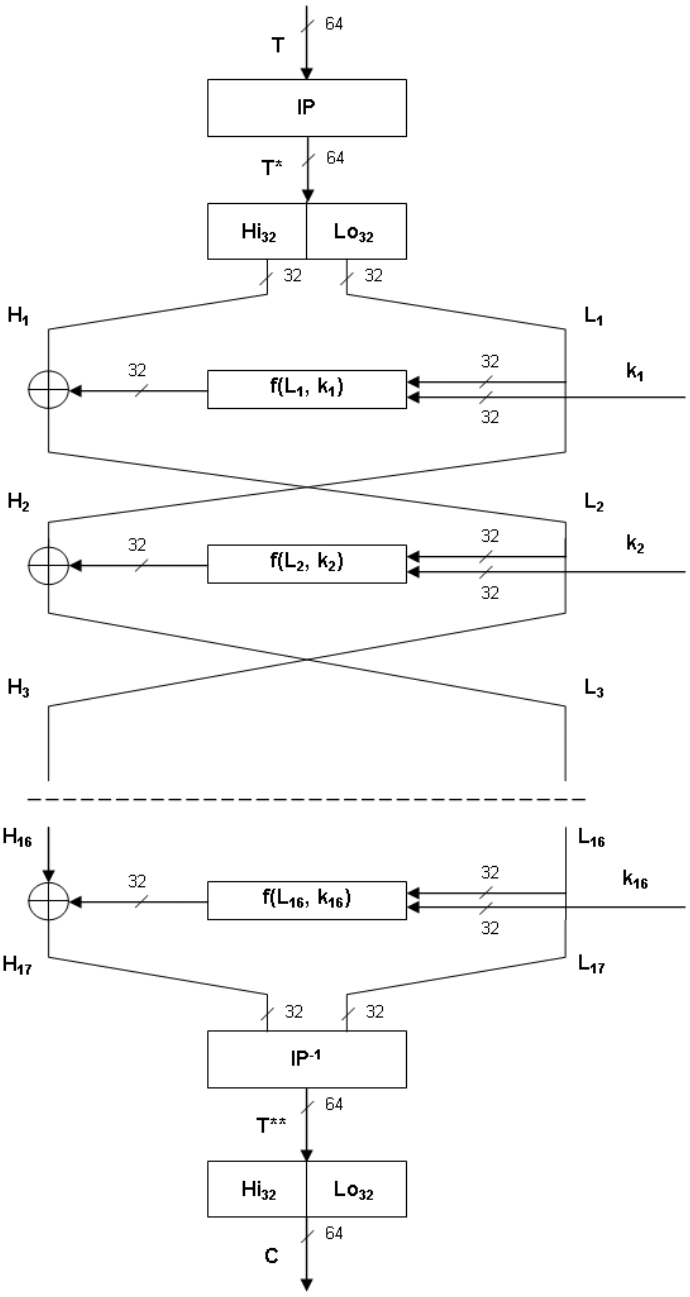


Рис.22. Схема шифрования блока

1. Шифрование 64-битового блока данных **T** начинается с начальной перестановки битов **IP** (табл. 5). В таблице указывается новое положение соответствующего бита. Таким образом, при выполнении начальной перестановки 58-ый бит станет 1-ым, 50-ый – 2-ым, 42-ой – 3-им и т.д.

Таблица 5

Начальная перестановка IP

58	**50**	**42**	**34**	**26**	**18**	**10**	**2**
60	**52**	**44**	**36**	**28**	**20**	**12**	**4**
62	**54**	**46**	**38**	**30**	**22**	**14**	**6**
64	**56**	**48**	**40**	**32**	**24**	**16**	**8**
57	**49**	**41**	**33**	**25**	**17**	**9**	**1**
59	**51**	**43**	**35**	**27**	**19**	**11**	**3**
61	**53**	**45**	**37**	**29**	**21**	**13**	**5**
63	**55**	**47**	**39**	**31**	**23**	**15**	**7**

2. Результат перестановки **T*** разделяется на две 32-битовые части $\mathbf{H_0}$ и $\mathbf{L_0}$, с которыми выполняются 16 раундов преобразования.

3. В каждом раунде **i** старшая половина $\mathbf{H_{i-1}}$ блока модифицируется путем побитового прибавления к ней по модулю 2 ($\oplus$) результата вычисления функции шифрования **f**, зависящей от младшей половины блока $\mathbf{L_{i-1}}$ и 48-битового ключевого элемента $\mathbf{k_i}$. Ключевой элемент $\mathbf{k_i}$ вырабатывается из ключа шифрования. Между раундами старшая и младшая половины блока меняются местами. В последнем раунде происходит то же самое за исключением обмена значениями половинок блока.

4. Полублоки $\mathbf{H_{16}}$ и $\mathbf{L_{16}}$ объединяются в полный блок **T****, в котором выполняется конечная битовая перестановка $\mathbf{IP^{-1}}$, обратная начальной. Результат последней операции и является выходным значением цикла шифрования – зашифрованным блоком **C**.

Таблица 6

Конечная перестановка IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Все перестановки в таблицах **IP** и $\mathbf{IP^{-1}}$ подобраны разработчиками таким образом, чтобы максимально затруднить процесс расшифровки путём подбора ключа.

Схема функции шифрования **f** приведена на рис.23.

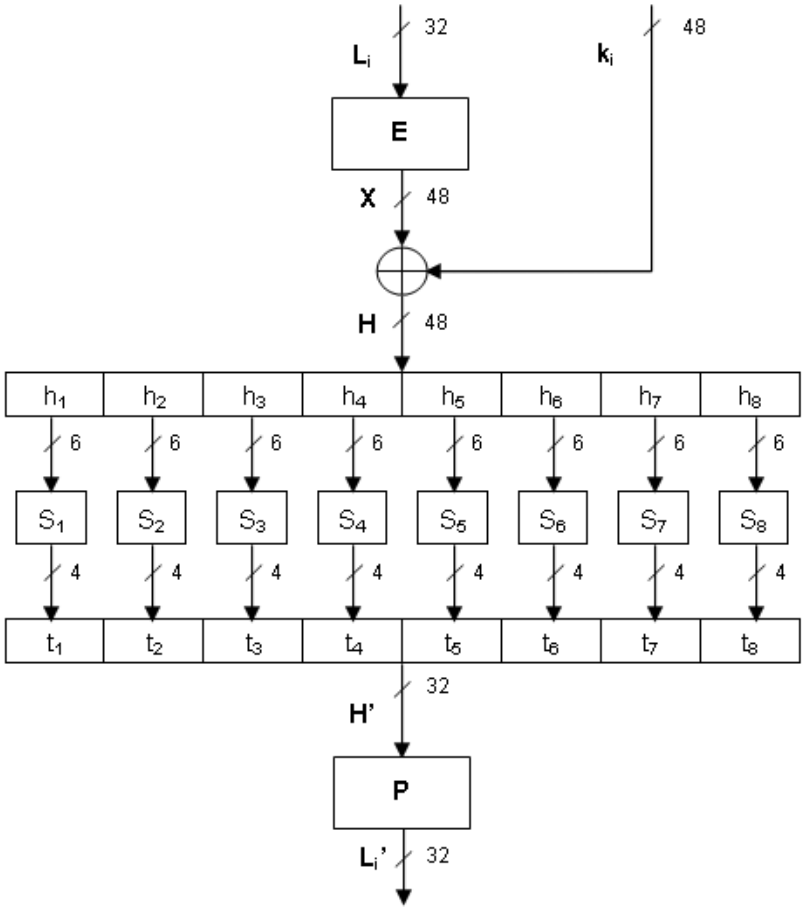


Рис.23. Схема функции шифрования

1. На вход поступает 32-битовая половина шифруемого блока $\mathbf{L_{i-1}}$ и 48-битовый ключевой элемент $\mathbf{k_i}$.

2. $\mathbf{L_{i-1}}$ разбивается на 8 тетрад по 4 бита. Каждая тетрада по циклическому закону дополняется крайними битами из соседних тетрад до 6-битного слова (функция расширения **E**). Цикличность означает, что первый бит L_{i-1} добавляется последним в последнее слово, а последний бит L_{i-1} добавляется первым в первое слово. Далее выполняется объединение тетрад в 48-битный блок **X**. Например, L_{i-1}=0111 0110 1… …0 1101, тогда X=101110 101101 … 011010.

3. **X** побитово суммируется по модулю 2 (⊕) с ключевым элементом $\mathbf{k_i}$.

4. 48-битовый блок данных **H** разделяется на восемь 6-битовых элементов, обозначенных $\mathbf{h_1, h_2, …, h_8}$.

5. Каждое из значений $\mathbf{h_j}$ преобразуется в новое 4-битовое значение $\mathbf{t_j}$ с помощью соответствующего узла замены $\mathbf{S_j}$.

Если на вход $\mathbf{S_j}$ поступает блок $\mathbf{h_j=b_1b_2b_3b_4b_5b_6}$, то двухбитовое число $\mathbf{b_1b_6}$ указывает номер строки матрицы, а четырёхбитовое число $\mathbf{b_2b_3b_4b_5}$ - номер столбца в таблице узлов замен. В результате применения узла замены $\mathbf{S_i}$ к блоку $\mathbf{h_i}$ получается число (от 0 до 15), которое преобразуется в $\mathbf{t_i}$. Например, в узел замены S_3 поступает h_3=101011. Тогда, номер строки равен 3 (b_1b_6=11), номер столбца – 5 ($b_2b_3b_4b_5$=0101), t_3=1001 (9).

6. Полученные восемь элементов $\mathbf{t_i}$ вновь объединяются в 32-битовый блок **H'**.

7. В **H'** выполняется перестановка битов **P**.

Таблица 7

Узлы замен

Номер строки \ Номер столбца	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Таблица 8

Перестановка P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Результат последней операции и является выходным значением функции шифрования $\mathbf{L}_{i-1}'$.

Ключевые элементы вырабатываются из ключа с использованием сдвигов и битовых выборок-перестановок. Таким образом, ключевые элементы состоят исключительно из битов исходного ключа, «перетасованных» в различном порядке. Схема выработки ключевых элементов показана на рис.24.

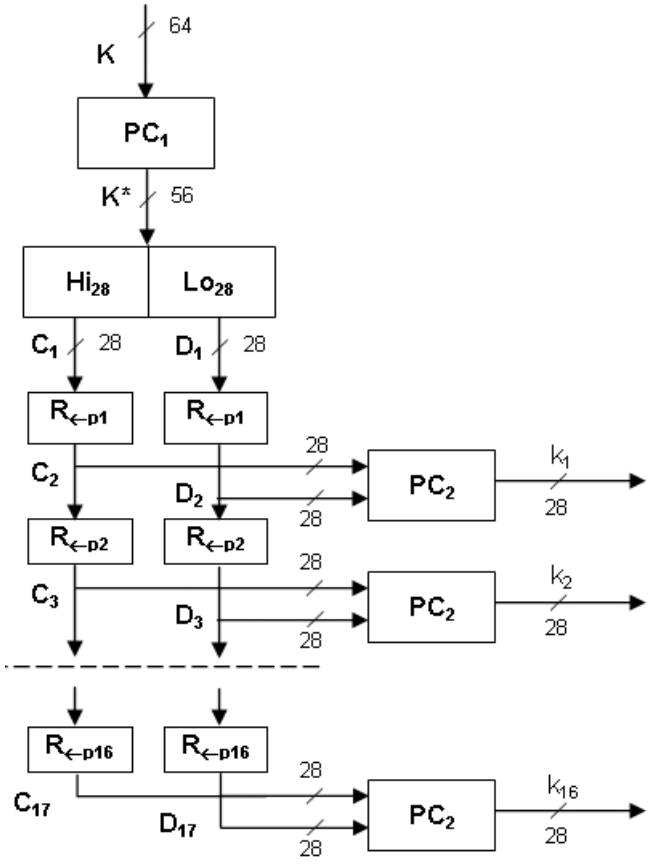


Рис.24. Схема выработки ключевых элементов

1. Выработка ключевых элементов из ключа **K** начинается со входной выборки-перестановки битов $\mathbf{PC_1}$ (табл.9), которая отбирает 56 из 64 битов ключа и располагает их в другом порядке.

Таблица 9

Перестановка $\mathbf{PC_1}$

57	**49**	**41**	**33**	**25**	**17**	**9**
1	**58**	**50**	**42**	**34**	**26**	**18**
10	**2**	**59**	**51**	**43**	**35**	**27**
19	**11**	**3**	**60**	**52**	**44**	**36**
63	**55**	**47**	**39**	**31**	**23**	**15**
7	**62**	**54**	**46**	**38**	**30**	**22**
14	**6**	**61**	**53**	**45**	**37**	**29**
21	**13**	**5**	**28**	**20**	**12**	**4**

2. Результат выборки-перестановки **K*** разделяется на две 28-битовые части: старшую $\mathbf{C_0}$ и младшую $\mathbf{D_0}$.

3. 16 раз выполняется процедура.

3а. В зависимости от номера итерации обе части циклически сдвигаются на 1 или 2 бита влево.

Таблица 10

Циклический сдвиг

Номер итерации	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Сдвиг (бит)	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**1**

3б. Из полученных блоков с помощью выходной битовой выборки-перестановки $\mathbf{PC_2}$ отбираются первые 48 битов, которые и формируют очередной ключевой элемент.

Таблица 11

Перестановка $\mathbf{PC_2}$

14	**17**	**11**	**24**	**1**	**5**
3	**28**	**15**	**6**	**21**	**10**
23	**19**	**12**	**4**	**26**	**8**

16	**7**	**27**	**20**	**13**	**2**
41	**52**	**31**	**37**	**47**	**55**
30	**40**	**51**	**45**	**33**	**48**
44	**49**	**39**	**56**	**34**	**53**
46	**42**	**50**	**36**	**29**	**32**

Алгоритмы шифрования и расшифрования DES-ECB в общем виде выражаются следующими схемами

$$\mathbf{C = DES(T) = IP(T) \rightarrow H_0 \oplus f(L_0, k_1), L_0 \rightarrow \ldots \rightarrow H_{15} \oplus f(L_{15}, k_{16}), L_{15} \rightarrow IP^{-1}(2^{32} * L_{16} + H_{16}),} \quad (8)$$

$$\mathbf{T = DES^{-1}(C) = IP(C) \rightarrow H_0 \oplus f(L_0, k_{16}), L_0 \rightarrow \ldots \rightarrow H_{15} \oplus f(L_{15}, k_1), L_{15} \rightarrow IP^{-1}(2^{32} * L_{16} + H_{16}).} \quad (9)$$

Таким образом, для расшифрования необходимо «прогнать» DES с тем же ключом в обратном направлении.

Использование различных методов шифрования:

- замена - функция расширения **E**, узлы замены **S**;
- перестановка – перестановки **IP**, $\mathbf{IP^{-1}}$, **P**, $\mathbf{PC_1}$, $\mathbf{PC_2}$, чередование $\mathbf{L_i}$ и $\mathbf{H_i}$, циклический сдвиг;
- гаммирование – $\oplus$.

Из-за небольшого числа возможных ключей (всего 2^{56}), появляется возможность их полного перебора на быстродействующей вычислительной технике за реальное время. В 1998 году Electronic Frontier Foundation используя специальный компьютер DES-Cracker, удалось взломать DES за 3 дня. По неподтвержденным данным, Агентство национальной безопасности США уже в 1996 г. могло вскрывать ключ DES за 3-15 мин. с помощью устройства стоимостью 50000 долларов.

Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать по алгоритму DES-ECB сообщение, состоящее из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв шифруемого сообщения.

При оформлении отчета необходимо привести:

- шифруемое сообщение (8 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251 (табл.3).;

- ключ (7 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251 (табл.3).;

- ключ в битовом представлении с учетом битов контроля четности;

- ключевые элементы $\mathbf{k_i}$;

- результат начальной перестановки **IP**;

- полублоки $\mathbf{H_i}$ и $\mathbf{L_i}$, $\mathbf{f(k_i, L_i)}$, $\mathbf{H_i \oplus f(k_i, L_i)}$;

- результат конечной перестановки IP^{-1}.

6. ЛАБОРАТОРНАЯ РАБОТА № 5. ШИФРОВАНИЕ С ОТКРЫТЫМ КЛЮЧОМ

Главная проблема использования одноключевых (симметричных) криптосистем заключается в распределении ключей. Для того чтобы был возможен обмен информацией между двумя сторонами, ключ должен быть сгенерирован одной из них, а затем в конфиденциальном порядке передан другой. Особую остроту данная проблема приобрела в наши дни, когда криптография стала общедоступной, вследствие чего количество пользователей больших криптосистем может исчисляться сотнями и тысячами.

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уитфилда Диффи и Мартина Хеллмана, опубликованной в 1976 году. Находясь под влиянием работы Ральфа Меркле (Ralph Merkle) о распространении открытого ключа, они предложили метод получения секретных ключей для симметричного шифрования, используя открытый канал. В 2002 году Хеллман предложил называть данный алгоритм «Диффи - Хеллмана - Меркле», признавая вклад Меркле в изобретение криптографии с открытым ключом.

Хотя работа Диффи-Хеллмана создала большой теоретический задел для открытой криптографии, первой реальной криптосистемой с открытым ключом считают алгоритм RSA (названный по имени авторов - Рон Ривест (Ronald Linn Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman) из Массачусетского Технологического Института (MIT)).

Справедливости ради следует отметить, что в декабре 1997 года была обнародована информация, согласно которой британский математик Клиффорд Кокс (Clifford Cocks), работавший в центре правительственной связи (GCHQ) Великобритании, описал систему, аналогичную RSA, в 1973 году, а несколькими месяцами позже в 1974 году Малькольм Вильямсон изобрел математический алгоритм, аналогичный алгоритму Диффи – Хеллмана - Меркле.

Суть шифрования с открытым ключом заключается в том, что для шифрования данных используется один ключ, а для расшифрования другой (поэтому такие системы часто называют **ассиметричными**).

Основная предпосылка, которая привела к появлению шифрования с открытым ключом, заключалось в том, что отправитель сообщения (тот, кто зашифровывает сообщение), не обязательно должен быть способен его расшифровывать. Т.е. даже имея исходное сообщение, ключ, с помощью которого оно шифровалось, и зная алгоритм шифрования, он не может расшифровать закрытое сообщение без знания ключа расшифрования.

Первый ключ, которым шифруется исходное сообщение, называется **открытым** и может быть опубликован для использования всеми пользователями системы. Расшифрование с помощью этого ключа невозможно. Второй ключ, с помощью которого дешифруется сообщение, называется **секретным** и должен быть известен только законному получателю закрытого сообщения.

Алгоритмы шифрования с открытым ключом используют так называемые необратимые или односторонние функции. Эти функции обладают следующим свойством: при заданном значении аргумента **x** относительно просто вычислить значение функции **f(x)**, однако, если известно значение функции **y = f(x)**, то нет простого пути для вычисления значения аргумента **x**. Например, функция **SIN**. Зная **x**, легко найти значение **SIN(x)** (например, **x = π - SIN(π) = 0**). Однако, если **SIN(x)=0**, однозначно определить **x** нельзя, т.к. в этом случае **x** может быть любым числом, определяемым по формуле **i*π**, где **i** – целое число.

Однако не всякая необратимая функция годится для использования в реальных криптосистемах. В их числе и функция **SIN**. Следует также отметить, что в самом определении необратимости функции присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к криптосистемам с открытым ключом предъявляются два важных и очевидных **требования**.

1. Преобразование исходного текста должно быть условно необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне.

Все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих **типов односторонних преобразований**.

1. Разложение больших чисел на простые множители (алгоритм RSA).

2. Вычисление дискретного логарифма или дискретное возведение в степень (алгоритм Диффи-Хелмана, схема Эль-Гамаля).

3. Задача об укладке рюкзака (ранца) (авторы Хелман и Меркл).

4. Вычисление корней алгебраических уравнений.

5. Использование конечных автоматов (автор Тао Ренжи).

6. Использование кодовых конструкций.

7. Использование свойств эллиптических кривых.

Алгоритм RSA. Стойкость RSA основывается на большой вычислительной сложности известных алгоритмов разложения произведения простых чисел на сомножители. Например, легко найти произведение двух простых чисел 7 и 13 даже в уме – 91. Попробуйте в уме найти два простых числа, произведение которых равно 323 (числа 17 и 19). Конечно, для современной вычислительной техники найти два простых числа, произведение которых равно 323, не проблема. Поэтому для надежного шифрования алгоритмом RSA, как правило, выбираются простые числа, количество двоичных разрядов которых равно нескольким сотням.

Описание RSA было опубликовано в августе 1977 года в журнале Scientific American. Авторы RSA поддерживали идею её активного распространения. В свою очередь, Агентство национальной безопасности (США), опасаясь использования этого алгоритма в негосударственных структурах, на протяжении нескольких лет безуспешно требовало прекращения распространения системы. Ситуация

порой доходила до абсурда. Например, когда программист Адам Бек (Adam Back) описал на языке Perl алгоритм RSA, состоящий из пяти строк, правительство США запретило распространение этой программы за пределами страны. Люди, недовольные подобным ограничением, в знак протеста напечатали текст этой программы на своих футболках.

Первым этапом любого асимметричного алгоритма является создание получателем шифрограмм пары ключей: открытого и секретного. Для алгоритма RSA этап создания ключей состоит из следующих операций.

Таблица 12

Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбираются два простых числа **p** и **q**.	p=7, q=13
2	Вычисляется произведение **n** = p * q.	n=91
3	Вычисляется **функция Эйлера**, равная **φ(n)**=(p-1)(q-1)=n-p-q+1. Результат расчета данной функции равен количеству положительных чисел, не превосходящих **n** и взаимно простым с **n**.	φ(n)=(7-1)(13-1)= 91-7-13+1 = 72
4	Выбирается произвольное число **e** (0<e<n), взаимно простое с результатом функции Эйлера (e ⊥ φ(n)). Число **e** называется открытой экспонентой.	e=5
5	Вычисляется секретный ключ **d** из соотношения (d*e) mod φ(n) = 1. Число **d** называется закрытой экспонентой. Обычно пользуются выражением de = 1 + kφ(n), где k - некоторое целое число.	(d*5) mod 72 = 1, d = 29
6	Публикуются открытые ключи **e** и **n** в специальном хранилище, где исключается возможность его подмены (**общедоступном сертифицированном справочнике**).	

Примечания. **Простое число** – натуральное число, большее единицы и не имеющее других делителей, кроме самого себя и единицы. **Взаимно простые числа** – числа, не имеющие общих делителей, кроме 1 (например, p=3, q=5, n=15, φ(n)=8 – взаимно простые с 15 – 1, 2, 4, 7, 8, 11, 13, 14).

Процедуры шифрования и дешифрования выполняются по следующим формулам

$$\mathbf{C = T^e \bmod n,} \quad (10)$$

$$\mathbf{T = C^d \bmod n.} \quad (11)$$

где **T, C** - числовые эквиваленты символов открытого и шифрованного сообщения.

Пример шифрования по алгоритму RSA приведен в следующей таблице. Коды букв соответствуют их положению в русском алфавите.

Таблица 13

Пример шифрования по алгоритму RSA

Открытое сообщение, T	**Символ**	**А**	**Б**	**Р**	**А**	**М**	**О**	**В**
	Код	**1**	**2**	**18**	**1**	**14**	**16**	**3**
Шифрограмма, $C = T^5 \bmod 91$		**1**	**32**	**44**	**1**	**14**	**74**	**61**
Открытое сообщение, $T = C^{29} \bmod 91$		**1**	**2**	**18**	**1**	**14**	**16**	**3**

Следует отметить, что **p** и **q** выбираются таким образом, чтобы **n** было больше кода любого символа открытого сообщения. В автоматизированных системах исходное сообщение переводиться в двоичное представление, после чего шифрование выполняется над блоками бит, равной длины. При этом длина блока должна быть меньше, чем длина двоичного представления **n**.

В заключении следует отметить стойкость данного алгоритма. В 2003 г. Ади Шамир и Эран Тромер разработали схему устройства TWIRL, которое при стоимости $ 10 000 может дешифровать 512-битный ключ за 10 минут, а при стоимости $ 10 000 000 – 1024-битный ключ меньше, чем за год. В настоящее время Лаборатория RSA рекомендует использовать ключи размером 2048 битов.

Алгоритм на основе задачи об укладке ранца [1]. В 1978 г. Меркль и Хеллман предложили использовать задача об укладке ранца (рюкзака) для асимметричного шифрования. Она относится к классу NP-полных задач и формулиру-

ется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений $\mathbf{M_1, M_2, ..., M_n}$ и суммарное значение **S**; требуется вычислить значения $\mathbf{b_i}$ такие что

$$\mathbf{S = b_1M_1+b_2M_2 + ... + b_nM_n,} \qquad (12)$$

где **n** – количество предметов;

$\mathbf{b_i}$ - бинарный множитель. Значение $\mathbf{b_i}$ = 1 означает, что предмет i кладут в рюкзак, $\mathbf{b_i}$ = 0 - не кладут.

Например, веса предметов имеют значения 1, 5, 6, 11, 14, 20, 32 и 43. При этом можно упаковать рюкзак так, чтобы его вес стал равен 22, использовав предметы весом 5, 6 и 11. Невозможно упаковать рюкзак так, чтобы его вес стал равен 24.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям **b**, а текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

Таблица 14

Пример шифрования на основе задачи об укладке ранца

Открытый текст	1 1 1 0 0 1 0 0	0 1 0 1 1 0 0 1	0 0 0 0 0 0 0 0
Рюкзак (ключ)	1 5 6 11 14 20 32 43	1 5 6 11 14 20 32 43	1 5 6 11 14 20 32 43
Шифрограмма	32 (1+5+6+20)	73 (5+11+14+43)	0

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них реша-

ется легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа **трудный** для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить **легкий** для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность. **Сверхвозрастающей** называется **последовательность**, в которой каждый последующий член больше суммы всех предыдущих. Например, последовательность {2, 3, 6, 13, 27, 52, 105, 210} является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} - нет.

Решение для сверхвозрастающего ранца найти легко. В качестве текущего выбирается полный вес, который надо получить, и сравнивается с весом самого тяжелого предмета в ранце. Если текущий вес меньше веса данного предмета, то его в рюкзак не кладут, в противном случае его укладывают в рюкзак. Уменьшают текущий вес на вес положенного предмета и переходят к следующему по весу предмету в последовательности. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля, то решение найдено. В противном случае, нет.

Например, пусть полный вес рюкзака равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в рюкзак. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в рюкзак не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак. Аналогично проходят процедуру укладки в рюкзак предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот рюкзак был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число **n** по модулю **m**. Значение модуля **m** должно быть больше суммы всех чисел последовательности, например, 420 (2+3+6+13+27+52+105+210=418). Множитель **n** должен быть взаимно простым числом с модулем **m**, например, 31. Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

Таблица 15

Пример получения открытого ключа

Закрытый ключ, k_i	**2**	**3**	**6**	**13**	**27**	**52**	**105**	**210**
Открытый ключ, $(k_i*n) \bmod m = (k_i*31) \bmod 420$	**62**	**93**	**186**	**403**	**417**	**352**	**315**	**210**

Для шифрования сообщение сначала разбивается на блоки, по размерам равные числу элементов последовательности в рюкзаке. Затем, считая, что единица указывает на присутствие элемента последовательности в рюкзаке, а ноль — на его отсутствие, вычисляются полные веса рюкзаков – по одному рюкзаку для каждого блока сообщения.

В качестве примера возьмем открытое сообщение **«АБРАМОВ»,** символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {**62, 93, 186, 403, 417, 352, 315, 210**} представлен в следующей таблице.

Таблица 16

Пример шифрования

Открытое сообщение		Сумма весов	Шифрограмма (рюкзак), c_i
Символ	Bin-код		
А	1100 0000	62+93	155
Б	1100 0001	62+93+210	365
Р	1101 0000	62+93+403	558
А	1100 0000	62+93	155
М	1100 1100	62+93+417+352	924
О	1100 1110	62+93+417+352+315	1239
В	1100 0010	62+93+315	470

Для расшифрования сообщения получатель должен сначала определить обратное число $\mathbf{n^{-1}}$, такое что $\mathbf{(n * n^{-1}) \bmod m = 1}$. В математике **обратное число** $\mathbf{n^{-1}}$ (обратное значение, обратная величина) - число, на которое надо умножить данное число n, чтобы получить единицу ($\mathbf{n * n^{-1} = 1}$). Пара чисел, произведение которых равно единице, называются **взаимно обратными**. Например: **5 и 1/5**, **−6/7** и **−7/6**. **Обратными числами по модулю m** называются такие числа **n** и $\mathbf{n^{-1}}$, для которых справедливо выражение ($\mathbf{n * n^{-1}}$) **mod m = 1**. Для вычисления обратных чисел по модулю обычно используется расширенный алгоритм Евклида. После определения обратного числа каждое значение шифрограммы умножается на $\mathbf{n^{-1}}$ по модулю **m** и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна {**2, 3, 6, 13, 27, 52, 105, 210**}, **m = 420, n = 31**. Значение $\mathbf{n^{-1}}$ равно **271 (31*271 mod 420 = 1**).

Таблица 17

Пример расшифрования

Шифрограмма (рюкзак), c_i	$(c_i*n^{-1}) \bmod m = (c_i*271) \bmod 420$	Сумма весов	Открытое сообщение	
			Bin-код	Символ
155	5	2+3	1100 0000	А
365	215	2+3+210	1100 0001	Б
558	18	2+3+13	1101 0000	Р
155	5	2+3	1100 0000	А
924	84	2+3+27+52	1100 1100	М
1239	189	2+3+27+52+105	1100 1110	О
470	110	2+3+105	1100 0010	В

В своей работе авторы рекомендовали брать длину ключа, равную 100 (количество элементов последовательности). В заключении следует отметить, что задача вскрытия данного способа шифрования успешно решена Шамиром и Циппелом в 1982 г.

Алгоритм шифрования Эль-Гамаля. Схема была предложена Тахером Эль-Гамалем в 1984 году. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и обеспечения аутентификации. Стойкость данного алгоритма базируется на сложности решения задачи дискретного логарифмирования.

Суть задачи заключается в следующем. Имеется уравнение

$$g^x = y \bmod p. \qquad (13)$$

Требуется по известным g, y и p найти целое неотрицательное число x (дискретный логарифм).

Порядок создания ключей приводится в следующей таблице.

Таблица 18

Процедура создания ключей

№ п/п	Описание операции	Пример
1	Выбираются простое число **p** и два любых произвольных числа **g** и **x** меньше **p** (**g** - первообразный корень по модулю **p**).	p=23, g=3, x=5
2	Вычисляется $\mathbf{y = g^x \bmod p}$	$y = 3^5 \bmod 23 = 243 \bmod 23 = 13$
3	Открытый ключ - **y, g** и **p**. Причем g и p можно сделать общими для группы пользователей. Закрытый ключ - **x**.	

Для шифрования каждого отдельного блока исходного сообщения должно выбираться случайное число **k** ($1 < k < p - 1$). После чего шифрограмма генерируется по следующим формулам

$$\mathbf{a = g^k \bmod p,} \qquad (14)$$

$$\mathbf{b = (y^k\, T) \bmod p,} \qquad (15)$$

где **T** – исходное сообщение;

(a, b) – зашифрованное сообщение.

Дешифрование сообщения выполняется по следующей формуле

$$\mathbf{T = (b\,(a^x)^{-1}) \bmod p} \qquad (16)$$

или

$$\mathbf{T = (b\, a^{p-1-x}) \bmod p,} \qquad (17)$$

где $\mathbf{(a^x)^{-1}}$ – обратное значение числа a^x по модулю p.

Пример шифрования и дешифрования по алгоритму Эль-Гамаля при **k=7** приведен в таблице, хотя для шифрования каждого блока (в нашем случае буквы) исходного сообщения надо использовать свое случайное число k.

Первая часть шифрованного сообщения – $\mathbf{a = 3^7 \bmod 23 = 2.}$

$\mathbf{a^x = 2^5 = 32, (a^x)^{-1} = 18 (32 * 18 \bmod 23 = 1)}$ **или** $\mathbf{a^{p-1-x} = a^{23-1-5} = 131072.}$

Таблица 19

Пример шифрования по алгоритму Эль-Гамаля при (k = const)

Открытое сообщение, T	Символ	А	Б	Р	А	М	О	В
	Код	1	2	18	1	14	16	3
Вторая часть шифрограммы, $b = (13^7 * T) \bmod 23$		9	18	1	9	11	6	4
Открытое сообщение, $T = (b * 18) \bmod 23$		1	2	18	1	14	16	3

Ввиду того, что число k является произвольным, то такую схему еще называют схемой **вероятностного шифрования**. Вероятностный характер шифрования является преимуществом для схемы Эль-Гамаля, т.к. у схем вероятностного шифрования наблюдается большая стойкость по сравнению со схемами с определенным процессом шифрования. Недостатком схемы шифрования Эль-Гамаля является удвоение длины зашифрованного текста по сравнению с начальным текстом. Для схемы вероятностного шифрования само сообщение T и ключ не определяют шифртекст однозначно. В схеме Эль-Гамаля необходимо использовать различные значения случайной величины k для шифровки различных сообщений T и T’. Если использовать одинаковые k, то для соответствующих шифртекстов (a, b) и (a’, b’) выполняется соотношение $\mathbf{b\,(b')^{-1} = T\,(T')^{-1}\ (mod\ p)}$. Из этого выражения можно легко вычислить T, если известно T’.

Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;

- алгоритма на основе задачи об укладке ранца;

- алгоритма шифрования Эль-Гамаля.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251 (табл.3).

СПИСОК ЛИТЕРАТУРЫ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – М.: ТРИУМФ, 2002. – 816 с.

2. Введение в криптографию / Под. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.

3. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Иващко. – М.: Горячая линия - Телеком, 2000. – 452 с.

4. Яковлев В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д. транспорта / В.В. Яковлев, А.А. Корниенко. – М.: УМК МПС России, 2002. – 328 с.

5. National Institute of Standards and Technology (NIST). FIPS Pub 46-3 (Federal information processing standards publication): Data Encryption Standard (DES). Oct. 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

6. Винокуров А.Ю. Традиционные криптографические алгоритмы. http://www.enlight.ru/crypto/algorithms/algs.htm

7. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазинин, Н.С. Погожин. – М.: Горячая линия - Телеком, 2001. – 148 с.