ЛАБОРАТОРНАЯ РАБОТА № 2

Часть 1. ШИФРЫ ЗАМЕНЫ

Сущность шифрования методом замены заключается в следующем. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$**, Б -** $\mathbf{M_Б}$**, Я -** $\mathbf{M_Я}$**.** Шифрозамены выбираются таким образом, чтобы любые два множества не содержали одинаковых элементов.

Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.

А	Б		Я
$M_А$	$M_Б$		Мя

Рис.1. Таблица шифрозамен

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

Так как множества $\mathbf{M_А}$**,** $\mathbf{M_Б}$**, ... ,** $\mathbf{M_Я}$ 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;
- полиграммные шифры. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения;
-омофонические шифры (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1;
- полиалфавитные шифры (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

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, 101=3628800, 15!=1307674368000).

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

Рис.3. 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! ($>10^{35}$).

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.4. 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 алфавита 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	И	К	Л
М	О	П	Р	С	Т	У	Ф
Х	Ш	Щ	Ъ	Ы	Э	Ю	

Рис.5. 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.

Таблица 1

Вероятности появления букв русского языка в текстах*

Буква (символ)	Вероят-ность	Буква	Вероят-ность	Буква	Вероят-ность	Буква	Вероят-ность
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	И	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», «ъъ» 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 оЯ об ще ни еЯ». 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
и	К	Л	М	О	П
р	С	Т	У	Ф	Х
Ц	Ч	Ш	Щ	Ы	Ь
Ъ	Э	Ю		-	-

Рис.6. 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.7 представлен фрагмент таблицы шифрозамен.

---

[1] **Омофоны** (греч. 6J6((- одинаковый + cpwvn - звук) - слова, которые звучат одинаково, но пишутся по-разному и имеют разное значение.

№ 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.7. 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, 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

[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.).

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.

Рис.8. 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	И	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	И	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	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
Г	Д	Е	Ж	З	И	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
Д	Е	Ж	З	И	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
Е	Ж	З	И	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
Ж	З	И	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
З	И	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
И	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	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	И
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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	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	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Рис.9. 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).

Часть 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
11	I2	I3		In

Рис.10. 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. 11

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

Рис.11. Таблица перестановок

Например, если для шифрования исходного сообщения «АБРАМОВ» использовать таблицу, представленную на рис.11, 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.12. Таблица перестановок

Для примера выберем размер блока, равный 3, и примем таблицу перестановок, показанную на рис.12. 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.

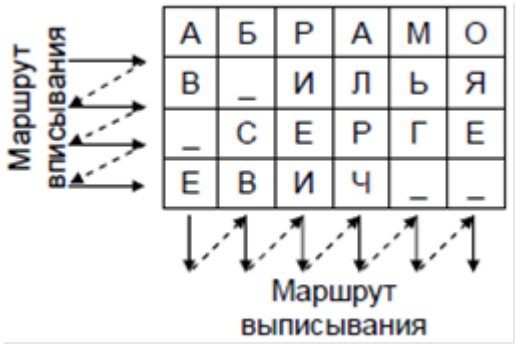

Рис.13. Пример использования шифра маршрутной перестановки

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 ЧМЬГ_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.13;
- 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.14. Пример использования шифра вертикальной перестановки

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

---

[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).

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

Пример шифрования сообщения «АБРАМОВ+ДЯДИНА» показан на рис.15. Результат шифрования - «АДВ_МНРДБЯ+_ОААИ».

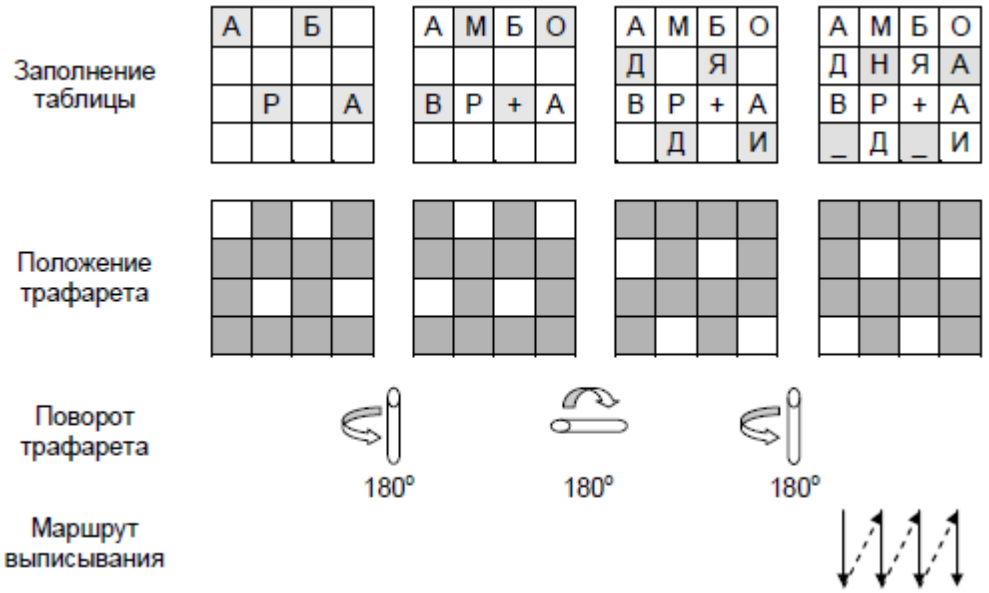

Рис.15. Пример использования решетки Кардано

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.

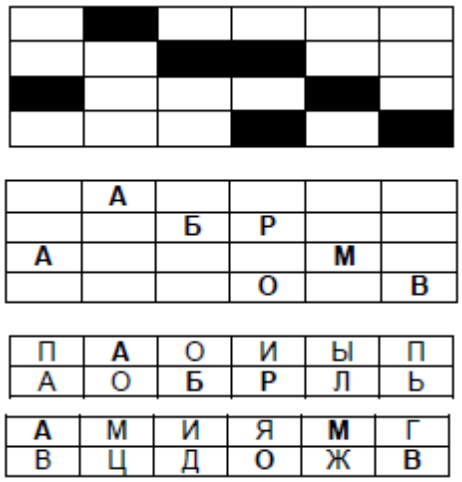

Рис.16. Пример использования шифра Ришелье

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.17. Магический квадрат 4 x 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.18. 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.19. Результат шифрования - «ОАБЯ+_АИВ_рДмНАД».

Рис.19. 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.

Часть 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.

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

$d = (P_i + K_i) \bmod N,$

$P_i = (C_i + N - K_i) \bmod N,$

где P_i, C_i - i-ый символ открытого и шифрованного сообщения;

N - количество символов в алфавите;

К - 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	И	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.20. 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 (0, для булевых величин аналог этой операции - XOR, «Исключающее ИЛИ»). Процедуры шифрования и дешифрования выполняются по следующим формулам

$$C_i = P_i \oplus K_i,$$
$$P_i = C_i \oplus K_i.$$

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.

Задание 1.

1) Зашифруйте сообщение методом Цезаря: "Умный человек знает все; мудрый - всех".

2) Расшифруйте сообщение методом Цезаря: "ЖЛТМОКЮФЖЭВАЖЕСЧЮЭ ПЖЙЮ ОЮЁАЖРЖЭ МЯЧГПРАЮ"

3) Зашифруйте сообщение методом Полибия: ""Умный человек знает все; мудрый - всех"

4) Расшифруйте сообщение методом Полибия: "УК ЗСЁЙКШЕ РФТХЕБШКЦФТ - ЖДШЕ ЖКНИЦЁТФШУДТ"

5) Зашифруйте сообщение методом Виженера, используя своё ключевое слово: "Умный человек знает все; мудрый - всех"

6) Расшифруйте сообщение методом Виженера, используя ключевое слово ИНФОРМАТИКА: "ЦУ ЭЬЕЫСЯЙБЙИ БЦФЧСБШЫ, Л ЙЦАГЬСГЙТ"

Задание 2.

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.

Задание 3.

Необходимо зашифровать свою фамилию (для первых двух шифров), 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.

Задание 4.

Необходимо зашифровать свою фамилию двумя способами: сложение по модулю N, сложение по модулю 2. При оформлении отчета необходимо привести исходное сообщение (фамилию), гамму и таблицы шифрования (см. табл.2 и 4).