Лабораторная работа №9

«Программная реализация простых шифров»

Введение

История человечества неразрывно связана с криптографией. С самого появления письменности люди уже начали использовать криптографию при записи рецептов производства и ведении учетных записей. Само слово криптография не означает непосредственно шифрование как таковое, слово *криптография* произошло от древне греческих слов κρυπτός – «тайный» и γράφω – «писать». Таким образом, криптография это наука о методах тайного письма или тайнописи. В текстах Индии, Египта, Месопотамии, Китая встречаются зашифрованные фрагменты, и даже описания самих методов шифрования. Наиболее древние свидетельства относят к третьему тысячелетию до н.э., по сути, ко времени появления самой письменности. В древних индийских текстах использовалось множество различных способов записи информации, часть из которых можно уверенно рассматривать как тайнопись. Например, известен способ письма, при котором гласные буквы заменялись согласными и наоборот. Из наиболее известных древних текстов, в которых использовались элементы криптографии, можно назвать Библию. Отдельные фрагменты в ней были зашифрованы шифром *Атбаш*.

В более позднее время различные методы шифрования сообщений стали применяться уже повсеместно. Средние века и эпоха Возрождения считаются периодом расцвета криптографии и криптоанализа. В это время шифры становятся популярны не только у военных, политиков и дипломатов, но и среди обычных граждан, появляется множество различных шифров и их описаний. Первая европейская книга, в которой описываются различные шифры, появляется в XIII веке - «Послание монаха Роджера Бэкона о тайных действиях искусства и природы и ничтожестве магии». Несколько позже в XV веке публикуется работа Габриэля де Левинда «Трактат о шифрах».

Если рассматривать простые способы тайнописи (простые шифры), то их можно разделить на два основных типа: *шифры замены* (подстановки) и *шифры перестановки*. В первом случае символы исходного алфавита заменяются символами другого алфавита или просто непонятными

символами, во втором символы исходного текста меняются местами – переставляются. Известным примером шифров замены является шифр «Пляшущие Человечки» из одноименного рассказа Артура Конан Дойла о легендарном сыщике Шерлоке Холмсе. В этом шифре символы текста заменялись фигурками пляшущих человечков.

Параллельно с развитием криптографии во все времена развивались и совершенствовались методы дешифрования – криптоанализа. Хотя термин «криптоанализ» и был введён лишь в 1920 году американским криптографом Уильямом Ф. Фридманом, как таковой криптоанализ существовал уже давно. Так первым письменным упоминанием можно считать «Манускрипт о дешифровке криптографических сообщений», написанный арабским учёным Ал-Кинди в IX веке. В работе приводится первое описание частотного криптоанализа зашифрованных сообщений. В XV веке данный метод анализа стали использовать и в Европе. Появление первых эффективных методов криптоанализа подтолкнуло развитее криптографии и привело к усложнению алгоритмов шифрования. Так на место *моноалфавитных* шифров замены, использовавшим для замены символов сообщения один алфавит, пришли более сложные – *полиалфавитные* шифры, в которых уже использовалось несколько различных алфавитов. Использование большего количества алфавитов позволило повысить стойкость шифров к частотному криптоанализу, но в тоже время значительно усложнило сами шифры.

С начала XX века на место простых шифров пришли специальные механические шифровальные устройства. С конца 70-х годов в основу криптографии были положены математические методы и для шифрования сообщений стали применять электронные вычислительные машины.

1. Шифры простой замены

Шифр простой замены, шифр однозначной замены – шифр, в котором каждому символу алфавита открытого текста ставится в соответствие один символ алфавита шифротекста. Правило шифрования/расшифрования может быть представлено в виде простой таблицы замены символов. Первая строка такой таблицы содержит алфавит открытого текста, вторая символы из алфавита шифротекста. В большинстве случаев алфавиты открытого текста и шифротекста совпадают и отличаются лишь перестановкой символов.

Шифр Цезаря. Сегодня считается одним из типичных представителей шифров простой замены. В свое время именно этот шифр использовал Гай Юлий Цезарь. Согласно дошедшим до нас описаниям для того, чтобы расшифровать сообщение необходимо вместо первой буквы читать четвертую букву алфавита, вместо второй пятую и т.д. В табличном виде правило шифрования можно представить следующим образом: выписывается алфавит в обычном виде, а под ним выписывался тот же алфавит, но смещенный на 3 буквы влево. Применительно к русскому алфавиту, таблица шифрования выглядит следующим образом:

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

В процессе шифрования буква «А» меняется на «Г», буква «Б» меняется на «Д» и т. д. Например, слово «РИМ» превращается в «УЛП».

В качестве ключа шифрования k в шифре Цезаря можно считать величину сдвига алфавита в нижней строке таблицы. Так в приведенном примере величина сдвига равна трем ($k = 3$). Если пронумеровать символы алфавита с нуля, то для произвольного ключа k правило шифрования можно представить в следующем виде: $j = (i + k) \bmod n$, где i – номер буквы в исходном алфавите, j – номер буквы зашифрованного текста в исходном алфавите, n – число символов в алфавите. Правило расшифрования в этом случае будет выглядеть следующим образом: $i = (j – k + n) \bmod n$.

Шифр Атбаш. Название шифра состоит из четырех букв «алеф», «тае», «бет», «шин». Эти буквы являются соответственно первой, последней, второй и предпоследней буквами древнесемитского алфавита. Эта последовательность букв в названии шифра выбрана не случайно и определяет правило шифрования: для алфавита, состоящего из n символов, i-ая буква заменяется буквой с номером $n - i + 1$.

Аффинная перестановка. В классическом шифре Цезаря использовалась только одна операция – сложение. Добавлением операции умножения можно получить новый шифр – аффинную перестановку. Возьмет два взаимно простых числа a и b таких, что $0 \le a, b \le n - 1$, где n – мощность алфавита. Тогда правило перестановки символов в исходном алфавите можно описать следующим выражением: $j = (a \cdot i + b) \bmod n$. Правило перестановки для расшифрования сообщения: $i = (j - b)\ a^{-1} \bmod n$, где a^{-1} – обратное к a по модулю n, т.е.: $a \cdot a^{-1} \bmod n = 1$.

Шифр подстановки. В рассмотренных выше примерах шифров простой замены использовались определенные правила позволяющие запомнить правило замены и порядок следования символов в алфавите шифрования. Помимо правила шифрования шифр подстановки может быть задан просто таблице подстановки. Как было отмечено ранее, такая таблица состоит из двух строк. Первая строка таблиц содержит символы исходного алфавита, вторая – некоторую их перестановку (или перестановку символов другого алфавита). Когда правило выбора символов из алфавита замены не задано или не известно используют непосредственно только таблицу замены.

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

Процесс шифрования состоит в том, чтобы найти букву исходного слова в верхней строке таблицы и выписать соответствующую ей букву из

нижней строки. Так, используя приведенную выше таблицу подстановки слов «ПОНЕДЕЛЬНИК» можно зашифровать как «ШФЩПСПЦЖЩГЗ».

Квадрат Полибия. Греческий историк, известный государственный деятель и военачальник Полибий предложил использовать специальную сигнальную систему для передачи сообщений с помощью факелов или даже просто «на пальцах». Для кодирования текста использовалась простая табличка представлявшая собой квадрат из пяти строк и пяти столбцов. В ячейках квадрата были записаны символы используемого алфавита.

	1	2	3	4	*5*
1	A	B	C	D	*E*
2	F	G	H	I, J	*K*
3	L	M	N	O	*P*
4	Q	R	S	T	*U*
5	*V*	*W*	*X*	*Y*	*Z*

В процессе кодирования каждому символу сообщения ставилась в соответствие пара чисел: номер строки и номер столбца. В результате шифрования сообщение «WAR» превращается в строку чисел: 52 11 42. Имея таблицу, расшифровать данное сообщение не составит труда.

Несмотря на то, что данный метод кодирования сообщений изначально был предложен для использования в сигнальных системах, более широкое применение квадрат Полибия нашел именно в криптографии. В данную систему шифрования можно добавить и ключ шифрования – особый порядок следования символов в таблице.

Тюремный шифр. Одна из модификаций шифра на основе квадрата Полибия получила название – «*тюремный шифр*». Способ кодирования сообщений предложенный Полибием оказался очень удобным для передачи их стуком через стены. Так, для того, чтобы передать букву «Н» нужно было стукнуть по стене два раза, и с небольшой паузой еще три раза. Но такой

способ кодирования был известен и охранникам. Для того чтобы усложнить шифр использовали произвольный порядок расположения букв. Но запомнить его было сложно, а передать таблицу на бумажке тоже было нельзя. Поэтому в качестве ключа использовали не целую таблицу, а некоторое простое и легко запоминаемое слово. Если в слове встречались повторы букв, они удалялись. Например, возьмем слов «PRISON». Выбранное слово записывается в начальные клетки квадрата. Затем, в оставшиеся клетки в обычном порядке записываются все остальные буквы.

	1	2	3	4	*5*
1	P	R	I, J	S	*O*
2	N	A	B	C	*D*
3	E	F	G	H	*K*
4	L	M	Q	T	*U*
5	*V*	*W*	*X*	*Y*	*Z*

Вместо короткого слова может быть использована целая фраза. Использование фразы позволяет лучше перемешать буквы в таблице, а запомнить её также легко, как и одно слово.

2. Шифры перестановки

Шифры, которые меняют только порядок следования символов сообщения, но не меняет сами символы, называют шифрами перестановки. Эти шифры не использую дополнительный алфавит шифрования и замену символов. Большинство шифров перестановки построено на основе использования таблиц перестановки. Открытое сообщение разбивается на блоки, длина которых равна количеству ячеек в таблице. Если последний фрагмент сообщения оказывается короче необходимой длины, он дополняется до нужной длины случайными символами. Каждый фрагмент

(блок) сообщения записывается в такую таблицу перестановки в прямом порядке, а затем считывается из нее в соответствии с заданным правилом.

Одиночная перестановка. Простая перестановка осуществляется по квадратной или прямоугольной таблице с фиксированными размерами. Ключом шифра является пара чисел: количество строк и столбцов. Например, используя таблицу размером 3×3 можно закодировать сообщение «ПОСЛАНИЕ СКРЫТО В ТЕКСТЕ ЗАПИСКИ» следующим образом:

П	О	С
Л	А	Н
И	Е	_

С	К	Р
Ы	Т	О
_	В	_

Т	Е	К
С	Т	Е
_	З	А

П	И	С
К	И	*Н*
Г	*Ш*	*Ц*

Если выписать сообщение по столбцам, то получим зашифрованное сообщение: «ПЛИОАЕСН_СЫ_КТВРО_ТС_ЕТЗКЕАПКГИИШСНЦ».

В случае квадратной таблицы порядок начальной записи фрагмента сообщения в таблицу (по строкам или по столбцам) не имеет значения. Если же используется прямоугольная таблица, то порядок записи сообщения в таблицу необходимо обговорить заранее.

Шифр вертикальной перестановки. В отличие от предыдущего шифра в данном шифре добавляется еще один параметр, который можно менять от сообщения к сообщению – ключевое слов. В качестве ключевого слова выбирается произвольное слово небольшой длины. Например, слов «ВОСХОД». Буквы слова нумеруются в соответствии с порядком их следования в алфавите. Повторяющиеся буквы нумеруются слева направо.

Ключевое слово выписывается в первой строке таблицы, под ним записываются номера упорядоченных букв. Ниже, строка за строкой записывается текст сообщения. После того, как будет записано все сообщение, столбцы таблицы переставляются в соответствии с порядковыми номерами букв сообщения.

В	О	С	Х	О	Д
1	*3*	*5*	*6*	*4*	*2*
П	О	С	Л	А	Н
И	Е	_	С	К	Р
Ы	Т	О	_	В	_
Т	Е	К	С	Т	Е
_	З	А	П	И	С
К	И	*Н*	*Г*	*О*	*К*

В	Д	О	О	С	Х
1	*2*	*3*	*4*	*5*	*6*
П	Н	О	А	С	Л
И	Р	Е	К	_	С
Ы	_	Т	В	О	_
Т	Е	Е	Т	К	С
_	С	З	И	А	П
К	*К*	И	*О*	*Н*	*Г*

Зашифрованное сообщение выписывается из таблицы по столбцам сверху вниз. В нашем примере получаем зашифрованное сообщение: «ПИЫТ_КНР_ЕСКОЕТЕЗИАКВТИОС_ОКАНЛС_СПГ».

Двойная перестановка. Шифр двойной перестановки во многом аналогичен шифру вертикальной перестановки. Основное отличие заключается в том, что вместо прямоугольника, высота которого не фиксирована (для шифра вертикальной перестановки), выбирается квадрат с длиной стороны равной длине ключевого слова. После того, как сообщение (или его фрагмент) будет записано в квадрат, выполняется перестановка столбцов точно также как в шифре вертикальной перестановки. Затем, аналогичным образом переставляются строки. После двух последовательных перестановок зашифрованное сообщение может быть выписано из квадрата либо по столбцам, либо по строкам.

Магический квадрат. Рассмотрим квадратную таблицу с длиной стороны L. В ячейки таблицы можно записать все целые числа от 1 до L^2. Если в результате получается таблица, у которой суммы чисел по всем строка и всем столбцам равны, то такая таблица называется Магическим квадратом. В качестве примера магического квадрата можно привести квадрат с гравюры Альбрехта Дюрера «Меланхолия». Что интересно, так это то, что в двух нижних ячейках квадрата записан год создания гравюры - 1514.

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

В средние века использование магических квадратов для шифрования сообщений было очень популярно. Процесс шифрования заключался в том, что шифруемое сообщение записывалось в ячейки квадрата согласно числам в этих ячейках. Зашифрованное сообщение считывалось по строкам. Считалось, что магический квадрат передает часть своей неведомой силы шифру и от этого взломать его, как тогда казалось, будет гораздо сложнее.

Магический квадрат является ярким примером шифров маршрутной перестановки, когда сообщение записывается или считывается из таблицы по определенному маршруту. В случае магического квадрата этот маршрут задается числами, записанными в его ячейках.

2. Полиалфавитные шифры

Каким бы сложным не был тот или иной алгоритм простой однозначной замены или перестановки все они потенциально обладают существенным недостатком. Зашифрованный текст может быть абсолютно не похож на исходный, но в нем все же остается кое-что от открытого текста. В частности, в тексте сохраняются частоты встречаемости букв и связи между ними. Например, буква «*О*» в русском языке встречается чаще других. В зашифрованном сообщении, тот символ или буква, которая будет встречаться чаще других, скорее всего, окажется буквой «*О*». Зная частоты встречаемости отдельных букв и биграмм в открытом тексте можно легко восстановить достаточно длинное зашифрованное сообщение.

Еще в XIV веке появились работы, посвященные частотному анализу и шифрам многозначной замены. Шифрами *многозначной замены* или

полиалфавитными называют шифры, в которых один и тот же символ открытого текста в зашифрованном сообщении может быть представлен несколькими разными символами.

Простой многоалфавитный шифр. Самым простым вариантом решения задачи многозначной замены символов является использование при шифровании сразу нескольких алфавитов замены. Рассмотрим шифр подстановки, в котором используется два алфавита шифротекста. В процессе шифрования поочередно используются оба алфавита шифрования. Для первой буквы используется первый алфавит, для второй – второй, для третьей снова первый и т.д. В качестве примера с помощью следующей таблицы зашифруем слово «ТРАССА».

Исходн. алф.	А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ш Щ Ы Ь Ъ Э Ю Я
Алфавит шифр. 1	Н З Ц М И Я Т Ю Х Р Щ Ф Ш Э Ч К А Г Ы Ъ Ж Л Е С П В О У Б Ь Д Ё
Алфавит шифр. 2	Р О А Щ У Ю Б Л Ш К Г Е Н В Д Ы Ф Ж Э Ъ Й Х Ц Ь Т И М Ё З Я Ч С

В результате шифрования получим текст «ЪЖНЭЫР». Как видно из примера, не смотря на то, что в исходном слове дважды встречались буквы «А» и «С», в зашифрованном слове парных букв не оказалось.

Шифр Гронсфельда является многоалфавитной модификацией шифра Цезаря. Если в шифре Цезаря величина сдвига фиксирована, то в шифре Гросфельда она меняется в процессе шифрования. Для этого используется числовой ключ, который циклически записывается под сообщением. В процессе шифрования сдвиг происходит на цифру, указанную под шифруемой буквой. Например, возьмем ключ «34152» и слово «Сообщение».

Открытый текст	С	О	О	Б	Щ	Е	Н	И	Е
Ключ	**3**	**4**	**1**	**5**	**2**	3	4	1	5
Зашифрованный текст	О	К	Н	Ъ	Ц	В	Й	З	А

Шифр пропорциональной замены. Частоты встречаемости символов в открытом тексте различны и хорошо прослеживаются даже в зашифрованном с помощью шифра перестановки или простой замены тексте. В таблице ниже представлены относительные частоты встречаемости символов русского алфавита в обычных текстах.

Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
Пробел	0,145	Р	0,041	Я	0,019	Х	0,009
О	0,095	В	0,039	Ы	0,016	Ж	0,008
Е	0,074	Л	0,036	З	0,015	Ю	0,007
А	0,064	К	0,029	Ъ, Ь	0,015	Ш	0,006
И	0,064	М	0,026	Б	0,015	Ц	0,004
Т	0,056	Д	0,026	Г	0,014	Щ	0,003
Н	0,055	П	0,024	Ч	0,013	Э	0,003
С	0,046	У	0,021	Й	0,010	Ф	0,002

Как можно заметить, буква «А» встречается в четыре раза чаще буквы «Б», а буква «Ы» в два раза чаще «Ж». Для того, что бы выровнять частоты встречаемости символов в зашифрованном сообщении, те символы, которые в исходном тексте встречаются чаще всего, заменяются не одним, а несколькими символами. Количество замещающих символов выбирается пропорционально частоте встречаемости символов открытого текста. Так, например символы «Ч», «Й», «Х», «Ж», «Ю», «Ш», «Ц», «Щ», «Э» и «Ф» в процессе шифрования можно заменить одним символом. При шифровании букв «О» и «Е» нужно выбирать один из восьми, девяти символов. Выбор замещающего символа из такого множества осуществляется либо случайным образом, либо циклически. При первом появлении буквы берется первый замещающий символ, при втором – второй и т.д.

Таблица Тритемия. Задача построения алфавита шифрования для шифра пропорциональной замены все же достаточно сложна. Во-первых, необходимо достаточно точно определить частоты встречаемости букв в открытом тексте. Во-вторых, нужно грамотно составить алфавит

шифрования значительно больший по сравнению с исходным алфавитом и при этом обеспечить визуальное единство алфавита. Например, будет неправильно дополнять латинский алфавит символами греческого алфавита. Размер греческого алфавита известен. Если в зашифрованном сообщении будет встречаться только половина символов этого алфавита, то это подтолкнет криптоаналитика на мысль об использовании шифра пропорциональной замены. Еще одной ошибкой будет использовать в качестве первой строки таблицы замены символы только исходного алфавита. Тогда противник будет знать, что те символы, которые не входят в исходный алфавит являются расширяющими. В свою очередь это позволит разбить символы на группы и впоследствии расшифровать сообщение.

Интересное решение задачи выравнивания частот символов в зашифрованном сообщении принадлежит Иоганнесу Тритемию. В своей книге «Полиграфия» вышедшей в 1518 году он предложил использовать квадратную таблицу представленную ниже.

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

В первую строку таблицы записывается обычный алфавит в прямом порядке. Каждая последующая строка таблицы представляет собой тот же алфавит, но сдвинутый относительно алфавита предыдущей строки на одну позицию влево. Первая строка таблицы используется и в качестве алфавита открытого текста и в качестве одного из шифралфавитов.

Принцип шифрования достаточно прост: первая буква сообщения шифруется обычным шифром подстановки с помощью первой строки, вторая с помощью второй и т.д. В результате, алфавит шифрования меняется с каждой буквой сообщения. Если в исходном алфавите 24 буквы, то каждая из них может быть представлена в зашифрованном тексте всеми 24 буквами. При этом алфавиты исходного и зашифрованного сообщений совпадают.

Шифр Виженера. Минусом шифра Тритемия является отсутствие в системе ключа шифрования как такого. В качестве ключа шифрования может быть использована перестановка символов исходного алфавита в первой строке таблицы Тритемия, но такой ключ сложно менять от сообщения к сообщению. Интересное решение этой проблемы было предложено французским дипломатом Блезом де Виженером. В своей книге «Трактат о шифрах» в 1586 году Виженер предложил использовать в качестве ключа шифрования само сообщение – *самоключ*.

Суть идеи Виженера состояла в том, чтобы менять алфавиты шифрования не последовательно, как в шифре Тритемия, а выбирать их в зависимости от букв сообщения или ранее зашифрованного текста. Сам шифр Виженера фактически представляет собой модификацию шифра Тритемия. В основе шифра лежит таблица Тритемия, сверху и слева от которой записан обычный алфавит.

Первая строка таблицы под алфавитом открытого текста может быть представлена как упорядоченным, так и перемешанным алфавитом. Все последующие строки также как и в таблице Тритемя представляют собой предыдущую строку, циклически сдвинутую на одну позицию влево.

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
D	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C
E	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D
F	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E
G	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F
H	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G
I	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K
M	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L
N	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M
O	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N
P	P	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O
Q	Q	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
R	R	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
S	S	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
T	T	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
U	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Дополнительная строка, записанная сверху таблицы, используется в шифре для сопоставления с символами сообщения, а дополнительный столбец служит для выбора нужного алфавита по символам ключа. Известны два варианта реализации шифра Виженера.

В первом варианте в качестве ключа шифрования используется само шифруемое сообщение $M = m_1, m_2,\ldots, m_n$. Для того чтобы обеспечить однозначность расшифрования в начало ключа (перед сообщением) дописывается одна буква k_0 известная как отправителю, так и получателю сообщения $K = k_0, k_1(= m_1), k_2(= m_2),\ldots, k_n(=m_n)$. Обе последовательности символов M и K записываются друг под другом. Ниже выписывается зашифрованное сообщение.

Сообщение	$m_1\ m_2\ \ldots\ m_n$
Ключ	$k_0\ \ m_1\ \ldots\ m_{n-1}$
Зашифрованное сообщение	$s_1\ \ s_2\ \ \ldots\ s_n$

Буквы зашифрованного сообщения $S = s_1, s_2,\ldots, s_n$ выбираются из таблицы шифрования по столбцу, соответствующему букве m_i сообщения M, и строке, соответствующей символу k_i ключа K.

Во втором варианте в качестве ключа шифрования используются уже зашифрованные на символы сообщения $K = k_0, k_1(= s_1), k_2(= s_2),\ldots, k_n(=s_n)$. В результате каждый следующий символ зависит от предыдущего.

Сообщение	$m_1\ m_2\ \ldots\ m_n$
Ключ	$k_0\ \ s_1\ \ldots\ s_{n-1}$
Зашифрованное сообщение	$s_1\ \ s_2\ \ \ldots\ s_n$

Впоследствии идеи Виженера нашли свое продолжение в работе Гильберта Вернама предложившего в 1917 г. последовательно складывать двоичные значения букв сообщения с двоичными значениями символов достаточно длинного ключа шифрования. Фактически им был предложен шифр гаммирования – совершенный шифр, не поддающийся дешифрованию.

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

При выполнении лабораторной работы необходимо программно реализовать алгоритмы шифрования и расшифрования простых шифров (по варинатм). Каждое задание состоит из трех подзадач: сформировать алфавит шифрования и расшифрования; описать алгоритм расшифрования для соответствующего простого шифра; написать программную реализацию шифра на языке высокого уровня Delphi, C++, C# или др.

Необходимо предусмотреть загрузку длинных сообщений и ключа (при необходимости) из файла и запись результатов работы программы в файл. Все программы должны работать с русским алфавитом по возможности дополненным пробелом и знаками препинания. В ряде шифров допускается использование только заглавных букв: аффинная перестановка, квадрат Полибия, тюремный шифр, простой многоалфавитный шифр, шифр пропорциональной замены.

Варианты задания:

1) Шифр Атабаш для русского и английского алфавитов;

2) Квадрат Полибия (для русского и английского алфавитов) – получение шифртекста;

3) Квадрат Полибия со случайным порядком следования символов (для русского и английского алфавитов) получение пары чисел;

4) Тюремный шифр;

5) Маршрутный шифр с задаваемым размером матрицы;

6) Шифр Гронсфельда;

7) Шифр пропорциональной замены;

8) Шифр Тритемия;

9) Шифр пропорциональной замены;

10) Шифровка цифр.