Лабораторная работа №10. Шифр Цезаря (шифр простого сдвига).

Цель работы

Выполнить шифрование заданного сообщения шифром циклического сдвига (частный случай шифра замен) и выполнить подбор ключа для дешифрования простого шифра.

Теоретическая часть

Шифр (cipher) – совокупность алгоритмов или отображений открытой информации, представленной в формализованном виде, в недоступный для восприятия шифрованный текст (также представленный в формализованном виде), который зависит от внешнего параметра (ключа).

Не зная ключа, невозможно по шифрованной информации определить открытую информацию, а по шифрованной и открытой информации – ключ.

Ключ (key) – некоторый неизвестный параметр шифра, позволяющий выбрать для шифрования и расшифрования конкретное преобразование из всего множества преобразований, составляющих шифр.

Открытый текст (plain text) – массив незашифрованных данных.

Шифртекст (ciphertext) – массив зашифрованных данных.

Шифр блочный (block cipher) – данные шифруются порциями одинакового размера, называемыми блоками, и результат зашифрования очередного блока зависит только от значения этого блока и от значения ключа шифрования, и не зависит от расположения блока в шифруемом массиве и от других блоков массива.

Шифр перестановок (P – permutation) – заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр.

Шифр перестановок

Шифр замен (S – substitution) – заключается в замене одних значений на другие по индексной таблице, замене подвергаются группы элементов шифруемого блока – битов или символов.

Шифр замен является одним из простейших блочных шифров. Символы исходного сообщения (открытый текст) заменяются на символы шифра в соответствии с таблицей замен, играющей роль ключа шифра. В общем случае алфавиты открытого текста и шифртекста не обязательно должны совпадать. В частном (но распространенном) случае символы в таблице замен берутся из алфавита открытого текста. Ключом к шифру замен является таблица замен символов (кодовых слов) в блоке открытого текста.

Например, при использовании такой таблицы замен (рис. справа), открытому тексту "1234ABCD" будет соответствовать шифртекст "!@#$%^&*". Операция шифрования с использованием таблицы замен (если алфавиты открытого текста и шифртекста разные) очень похожа на операцию кодирования (переход от одной кодировки к другой), однако при кодировании таблица кодов (замен) не является секретной.

вместо	подставить
1	!
2	@
3	#
4	$
A	%
B	^
C	&
D	*

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке.

При шифровании исходного текста каждая буква заменяется другой буквой того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту к концу от исходной буквы на k букв. При достижении конца алфавита выполняется циклический переход к его началу.

Например: пусть A – используемый алфавит: $A=\{a_1, a_2,\ldots,a_i,\ldots,a_N\}$,

где $a_1, a_2,\ldots,a_i,\ldots,a_N$ – символы алфавита; N – размер алфавита.

Пусть k – число позиций сдвига символов алфавита при шифровании, $0<k<N$.

При шифровании каждый символ алфавита с номером i из кодируемого текста заменяется на символ этого же алфавита с номером i+k: $\text{cod: } a_i \rightarrow a_{i+k}$

Если $m+k>N$, номер символа в алфавите A определяется как m+k-N.

Для дешифрования текстовой информации номер позиции символа восстанавливаемого текста определяется как m-k. Если $m-k<0$, то вычисление этого номера производится как m-k+N.

Достоинством этой системы является простота шифрования и дешифрования.

К недостаткам системы Цезаря следует отнести:
- подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного и отрытого текста;
- сохраняется алфавитный порядок в последовательности заменяющих букв; при изменении значения k изменяются только начальные позиции такой последовательности;
- число возможных ключей k мало;
- шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифре.

Пример использования шифра Цезаря

Исходное сообщение "МАМА_МЫЛА_РАМУ"

Алфавит A = { _, А, Л, М, Р, У, Ы}

Ключ k = 1

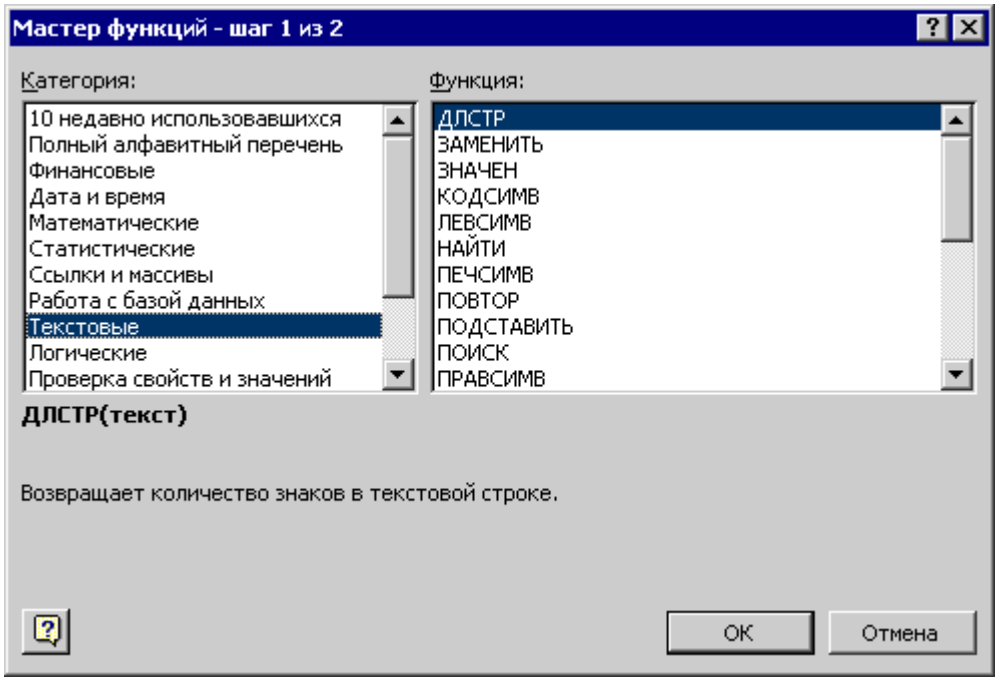
Таблица замен

(Позиция символа в алфавите)	Вместо	Подставить	(Позиция символа в алфавите)
1	_	А	2
2	А	Л	3
3	Л	М	4
4	М	Р	5
5	Р	У	6
6	У	Ы	7
7	Ы	_	1

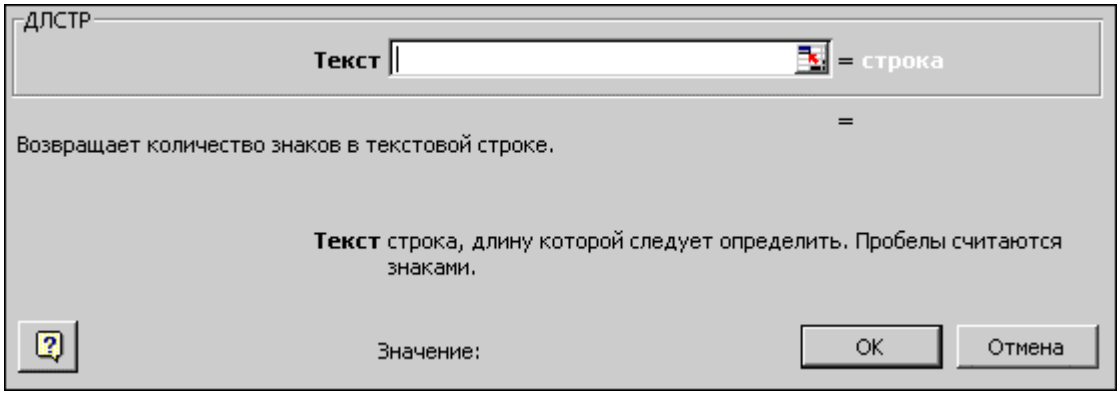
Шифртекст «РЛРЛАР_МЛАУЛРЫ»

Мастер функций MS Excel

Для обработки текстовых значений ячеек в MS Excel используются специальные функции, сгруппированные в категории "Текстовые". Вызов мастера функций осуществляется при помощи кнопки  на панели инструментов. Для каждой функции показывается краткое описание назначения функции и ее аргументы.



После выбора функции мастер предлагает ввести ее аргументы, для каждого из которых также есть небольшая подсказка.



В приведенном примере показана функция ДЛСТР, определяющая длину строки, которая имеет один аргумент – адрес ячейки со строкой текста. Возвращаемое значение зависит от вида функции и может быть числом, текстовой строкой или сообщением об ошибке.

Краткое описание используемых в работе функций

ДЛСТР(текст)

Категория – текстовые функции

Возвращает длину строки текста, заданного первым и единственным аргументом.

ПСТР(текст;начальный_номер;количество_символов)

Категория – текстовые

Извлекает из строки текста, заданной первым аргументом, начиная с позиции, заданной вторым аргументом, столько символов, сколько указано в третьем аргументе.

ТЕКСТ	ДЛСТР()		ТЕКСТ	НАЧ	КОЛ	ПСТР()
Я	1		ПОБЕДА	1	1	П
ДОМ	3		ПОБЕДА	1	2	ПО
МАМА	4		ПОБЕДА	2	3	ОБЕ
ВЕРТОЛЕТ	8		ПОБЕДА	3	4	БЕДА
КТО ЗДЕСЬ?	10		ПОБЕДА	4	3	ЕДА

При определении длины строки учитываются все символы, включая буквы, цифры, пробелы, знаки препинания и прочие символы.

Как и любые аргументы любых функций, номер начальной позиции в строке символов и количество символов для извлечения могут быть не только константами (как изображено на рисунке выше), но и результатами вычислений по формулам.

СЦЕПИТЬ(текст1;текст2;…)

Категория – текстовые

Объединяет несколько (от одного до тридцати) текстовых аргументов в один текст.

НАЙТИ(найти_текст;внутри_текста;начальный_номер)

Категория – текстовые

Ищет первый текстовый аргумент внутри второго текстового аргумента, начиная с позиции, указанной в третьем аргументе. Если текст найден, возвращается номер позиции, с которой начинается найденный текст, иначе возвращается сообщение об ошибке #ЗНАЧ!.

ТЕКСТ1	ТЕКСТ2	СЦЕПИТЬ()		ТЕКСТ1	ТЕКСТ2	НАЧ	НАЙТИ()
ДА		ДА		К	КОЛОКОЛ	1	1
	НЕТ	НЕТ		К	КОЛОКОЛ	2	5
ДА	НЕТ	ДАНЕТ		К	КОЛОКОЛ	5	5
ДА И	НЕТ	ДА ИНЕТ		К	КОЛОКОЛ	6	#ЗНАЧ!
ДА И	НЕТ	ДА И НЕТ		К	КОЛОКОЛ	8	#ЗНАЧ!

Если одна из объединяемых ячеек является пустой, т.е. не содержит никаких символов, то она рассматривается как пустая строка длины 0.

При слиянии строк пробелы между строками не добавляются автоматически. При необходимости пробелы должны добавляться вручную либо в самих строках (как изображено на рисунке выше), либо непосредственно в списке аргументов в функции, например, так: =СЦЕПИТЬ(B3; " ";C3).

ЕОШИБКА(проверяемое_значение)

Категория – проверка свойств и значений

Возвращает значение ИСТИНА, если проверяемое значение является любым сообщением об ошибке, например #Н/Д, #ССЫЛКА, #ИМЯ?, #ЗНАЧ! и т.д.

Если проверяемое значение не является ошибкой (т.е. является числом или текстом), то возвращается значение ЛОЖЬ.

Сообщение об ошибке не всегда является признаком неправильного результата. В некоторых случаях (в том числе – при выполнении данной работы), сообщение об ошибке текстовой функции, полученное в одних ячейках, используется для выполнения определенных действий с другими ячейками, т.е. является ожидаемым событием.

ЕСЛИ(проверяемое_условие;значение_если_истина;значение_если_ложь)

Категория – логические функции

Проверяет условие или логическое значение, заданное первым аргументом, и возвращает второй либо третий аргумент в зависимости от результата проверки.

Функции НАЙТИ(), ЕОШИБКА() и ЕСЛИ() могут эффективно применяться совместно. В зависимости от того, был ли найден искомый текст функцией НАЙТИ() в одной ячейке, в другой ячейке появится либо число, либо сообщение об ошибке, которое может быть

Этапы выполнения работы

1. Составить алфавит для заданного сообщения (т.е. определить множество неповторяющихся символов).

2. Составить расчетную таблицу для шифрования сообщения с заданным ключом;

3. Сравнить алфавиты и частоты появления символов открытого текста и шифртекста. Сделать вывод о наличии или отсутствии статистической связи открытого текста и шифртекста;

4. Для заданного шифртекста вручную подобрать ключ. Выписать полученный ключ и открытый текст.

1. Составление алфавита сообщения

Для составления алфавита предлагается использовать следующий алгоритм:

- разбить сообщение на отдельные символы;

- найти уникальные (неповторяющиеся) символы;

- составить из найденных символов строку алфавита.

В качестве примера используется сообщение МАМА_МЫЛА_РАМУ

В отдельную ячейку вводится исходное сообщение. Для наглядности рекомендуется использовать заглавные буквы, а пробелы заменить символом подчеркивания.

В следующей строке находим длину сообщения, которая потребуется для определения количества ячеек в расчетах.

Следующие две строки оставляем для будущих вычислений.

	A	B	C	D
1	**Сообщение**	МАМА_МЫЛА_РАМУ		
2	**Длина сообщения**	14		
3	Алфавит сообщения			
4	Размер алфавита			

Далее с использованием простейшей формулы (A8=A7+1) заполняем первый столбец числами от 1 до найденной длины сообщения.

В следующем столбце при помощи функции **ПСТР( )** извлекаем по одному символу из исходного сообщения (номер позиции символа берется из первого столбца).

Перед копированием формулы по строкам вниз следует убедиться, что в формуле использована абсолютная ссылка на ячейку с исходным сообщением (B1). Для наглядности результата рекомендуется установить для полученных символов выравнивание по центру ячейки.

	A	B	C	D
1	**Сообщение**	МАМА_МЫЛА_РАМУ		
2	**Длина сообщения**	14		
3	Алфавит сообщения			
4	Размер алфавита			
5				
6	**Номер**	**Символ**		
7	1	М		
8	2	А		
9	3	М		
10	4	А		
11	5	_		
12	6	М		
13	7	Ы		
14	8	Л		
15	9	А		
16	10	_		
17	11	Р		
18	12	А		
19	13	М		
20	14	У		
21				

Для каждого символа в столбце B известна его позиция в сообщении (столбец A), однако пока неизвестно, встречается ли такой символ только один раз только в этой позиции, или он есть где-то еще в сообщении в другой позиции.

Попробуем найти следующее вхождение заданного символа в строку исходного сообщения. В следующем столбце (начиная с ячейки C7) при помощи функции **НАЙТИ()** будем искать в сообщении (B1) поочередно отдельные символы со следующей позиции по отношению к известной (в столбце A).

Если символ будет найден, в ячейке появится позиция повторного появления данного символа в сообщении.

Если символ в сообщении больше не встречается, будет получено сообщение об ошибке.

	A	B	C	D
1	**Сообщение**	МАМА_МЫЛА_РАМУ		
2	**Длина сообщения**	14		
3	Алфавит сообщения			
4	Размер алфавита			
5				
6	**Номер**	**Символ**	**Повтор**	
7	1	М	=НАЙТИ(B7;B1;A7+1)	
8	2	А	4	
9	3	М	6	
10	4	А	9	
11	5	_	10	
12	6	М	13	
13	7	Ы	#ЗНАЧ!	
14	8	Л	#ЗНАЧ!	
15	9	А	12	
16	10	_	#ЗНАЧ!	
17	11	Р	#ЗНАЧ!	
18	12	А	#ЗНАЧ!	
19	13	М	#ЗНАЧ!	
20	14	У	#ЗНАЧ!	

Таким образом, в алфавит следует включать только те символы, для которых в столбце «Повтор» имеется сообщение об ошибке (т.е. они больше не повторяются).

Для составления строки алфавита испльзуется сложная формула, включающая в себя три функции из трех разных категорий (логическая, проверка, текстовая).

Для правильной работы этой формулы в ячейку D6 необходимо ввести пустую строку "" (две кавычки без пробела), которая будет являться заготовкой для получения алфавита сообщения, иначе пустая ячейка интерпретируется как число 0.

Символ	Повтор	=""
М	3	=ЕСЛИ(ЕОШИБКА(C7);СЦЕПИТЬ(D6;B7);D6)

Если в текущей строке в столбце C есть сообщение об ошибке, значит, в столбце B есть символ, который больше не повторяется в сообщении, поэтому его следует дописать в столбце D к строке алфавита из предыдущей строки.

Если в столбце C ошибки нет, предыдущая строка алфавита остается без изменений.

После копирования формулы в последней строке будет получен алфавит сообщения.

Используя относительную ссылку на ячейку в последней строке алфавита, скопируем полученный результат в ячейку B3 и рассчитаем размер алфавита в ячейке B4.

	A	B	C	D
1	**Сообщение**	МАМА_МЫЛА_РАМУ		
2	**Длина сообщения**	14		
3	**Алфавит сообщения**	ЫЛ_РАМУ		
4	**Размер алфавита**	7		
5				
6	**Номер**	**Символ**	**Повтор**	
7	1	М	3	
8	2	А	4	
9	3	М	6	
10	4	А	9	
11	5	_	10	
12	6	М	13	
13	7	Ы	#ЗНАЧ!	Ы
14	8	Л	#ЗНАЧ!	ЫЛ
15	9	А	12	ЫЛ
16	10	_	#ЗНАЧ!	ЫЛ_
17	11	Р	#ЗНАЧ!	ЫЛ_Р
18	12	А	#ЗНАЧ!	ЫЛ_РА
19	13	М	#ЗНАЧ!	ЫЛ_РАМ
20	14	У	#ЗНАЧ!	ЫЛ_РАМУ

2. Шифрование сообщения

Рассмотрим шифрование открытого текста простым шифром циклического сдвига на следующем примере: открытый текст "МАМА_МЫЛА_РАМУ", ключ k=1.

Для выполнения операции шифрования потребуется открытый текст сообщения, алфавит сообщения и размер алфавита.

Размер алфавита нужен для проверки и коррекции величины сдвига при выполнении циклического сдвига.

Кроме того, вставим пару новых пустых строк для ключа и шифртекста.

	A	B	C	D
1	**Открытый текст**	МАМА_МЫЛА_РАМУ		
2	**Длина сообщения**	14		
3	**Алфавит сообщения**	ЫЛ_РАМУ		
4	**Размер алфавита**	7		
5	**Ключ сдвига**	1		
6	**Шифртекст**			
7				
8	**Номер**	**Символ**	**Повтор**	
9	1	М	3	
10	2	А	4	
11	3	М	6	
12	4	А	9	
13	5	_	10	
14	6	М	13	
15	7	Ы	#ЗНАЧ!	Ы
16	8	Л	#ЗНАЧ!	ЫЛ
17	9	А	12	ЫЛ
18	10	_	#ЗНАЧ!	ЫЛ_
19	11	Р	#ЗНАЧ!	ЫЛ_Р
20	12	А	#ЗНАЧ!	ЫЛ_РА
21	13	М	#ЗНАЧ!	ЫЛ_РАМ
22	14	У	#ЗНАЧ!	ЫЛ_РАМУ

Далее при помощи функции НАЙТИ() необходимо определить, какую позицию занимает текущий символ открытого текста в алфавите сообщения.

В рассматриваемом примере символы в строке алфавита не упорядочены, а появляются в том порядке, в котором они были найдены в столбцах C и D.

Обратите внимание: одни и те же буквы сообщения занимают одни и те же позиции в алфавите: буква М всегда на позиции 6, буква А всегда на позиции 5 и т.д.

Номера позиций находятся в диапазоне от 1 до размера алфавита (в ячейке B4).

НАЙТИ | =НАЙТИ(B9;B3;1)

	A	B	C	D	E	F	G
1	**Открытый текст**	МАМА_МЫЛА_РАМУ					
2	**Длина сообщения**	14					
3	**Алфавит сообщения**	ЫЛ_РАМУ					
4	**Размер алфавита**	7					
5	Ключ сдвига	1					
6	Шифртекст						
7							
8	**Номер**	**Символ**	**Повтор**			**Позиция**	
9	1	М	3			=НАЙТИ(B9;B3;1)	
10	2	А	4			5	
11	3	М	6			6	
12	4	А	9			5	
13	5	_	10			3	
14	6	М	13			6	
15	7	Ы	#ЗНАЧ!	Ы		1	
16	8	Л	#ЗНАЧ!	ЫЛ		2	
17	9	А	12	ЫЛ		5	
18	10	_	#ЗНАЧ!	ЫЛ_		3	
19	11	Р	#ЗНАЧ!	ЫЛ_Р		4	
20	12	А	#ЗНАЧ!	ЫЛ_РА		5	
21	13	М	#ЗНАЧ!	ЫЛ_РАМ		6	
22	14	У	#ЗНАЧ!	ЫЛ_РАМУ		7	

В следующем столбце рассчитывается позиция в алфавите нового символа, который будет использован в шифртексте вместо исходного символа открытого текста после выполнения сдвига.

Расчетная формула для столбца G очевидна – к текущей позиции прибавляется с использованием абсолютной ссылки на соответствующую ячейку величина сдвига (ключ шифра).

В столбце H для всех ячеек выполняется проверка: если величина сдвига (столбец G) больше размера алфавита (B4), то возвращаемся циклически к начальным символам алфавита.

H9 | =ЕСЛИ(G9>B4;G9-B4;G9)

	A	B	C	D	E	F	G	H
1	**Открытый текст**	МАМА_МЫЛА_РАМУ						
2	**Длина сообщения**	14						
3	**Алфавит сообщения**	ЫЛ_РАМУ						
4	**Размер алфавита**	7						
5	**Ключ сдвига**	1						
6	Шифртекст							
7								
8	**Номер**	**Символ**	**Повтор**			**Позиция**	**Сдвиг**	**Коррекция**
9	1	М	3			6	7	7
10	2	А	4			5	6	6
11	3	М	6			6	7	7
12	4	А	9			5	6	6
13	5	_	10			3	4	4
14	6	М	13			6	7	7
15	7	Ы	#ЗНАЧ!	Ы		1	2	2
16	8	Л	#ЗНАЧ!	ЫЛ		2	3	3
17	9	А	12	ЫЛ		5	6	6
18	10	_	#ЗНАЧ!	ЫЛ_		3	4	4
19	11	Р	#ЗНАЧ!	ЫЛ_Р		4	5	5
20	12	А	#ЗНАЧ!	ЫЛ_РА		5	6	6
21	13	М	#ЗНАЧ!	ЫЛ_РАМ		6	7	7
22	14	У	#ЗНАЧ!	ЫЛ_РАМУ		7	8	1

В рассматриваемом примере в последней строке символ У занимает в алфавите позицию 7, при величине сдвига 1 необходима коррекция, таким образом, вместо символа У в шифртексте будет использован символ, занимающий в алфавите позицию 1 (т.е. буква Ы).

Далее при помощи функции ПСТР() извлекаем по очереди символы шифртекста из строки алфавита (по одному символу в скорректированных позициях) и составляем из них при помощи функции СЦЕПИТЬ() строку шифртекста (начиная с пустой строки =””).

B6 = УМУМРУЛ_МРАМУЫ

	A	B	C	D	E	F	G	H	I	J
1	**Открытый текст**	МАМА_МЫЛА_РАМУ								
2	**Длина сообщения**	14								
3	**Алфавит сообщения**	ЫЛ_РАМУ								
4	**Размер алфавита**	7								
5	**Ключ сдвига**	1								
6	**Шифртекст**	УМУМРУЛ_МРАМУЫ								
7										
8	**Номер**	**Символ**	**Повтор**			**Позиция**	**Сдвиг**	**Коррекция**	**Шифр**	
9	1	М	3			6	7	7	У	У
10	2	А	4			5	6	6	М	УМ
11	3	М	6			6	7	7	У	УМУ
12	4	А	9			5	6	6	М	УМУМ
13	5	_	10			3	4	4	Р	УМУМР
14	6	М	13			6	7	7	У	УМУМРУ
15	7	Ы	#ЗНАЧ!	Ы		1	2	2	Л	УМУМРУЛ
16	8	Л	#ЗНАЧ!	ЫЛ		2	3	3	_	УМУМРУЛ_
17	9	А	12	ЫЛ		5	6	6	М	УМУМРУЛ_М
18	10	_	#ЗНАЧ!	ЫЛ_		3	4	4	Р	УМУМРУЛ_МР
19	11	Р	#ЗНАЧ!	ЫЛ_Р		4	5	5	А	УМУМРУЛ_МРА
20	12	А	#ЗНАЧ!	ЫЛ_РА		5	6	6	М	УМУМРУЛ_МРАМ
21	13	М	#ЗНАЧ!	ЫЛ_РАМ		6	7	7	У	УМУМРУЛ_МРАМУ
22	14	У	#ЗНАЧ!	ЫЛ_РАМУ		7	8	1	Ы	УМУМРУЛ_МРАМУЫ

Результат заносим в ячейку шифртекста при помощи относительной ссылки на последнюю ячейку.

3. Статистический анализ открытого текста и шифртекста

Создадим заготовку расчетной таблицы. По вертикали (столбец G) извлечем отдельные символы из сообщения, а по горизонтали (строка 3) – символы алфавита.

Выделим символы жирным шрифтом.

Далее в полученной матрице (в данном примере – в диапазоне ячеек H4:N17) проверим, какой из сиволов алфавита совпадает с текущим символом сообщения.

H3 = =ПСТР(B3;H2;1)

	F	G	H	I	J	K	L	M	N
1		Количество							
2	**Номер**		1	2	3	4	5	6	7
3		**Символ**	**Ы**	**Л**	**_**	**Р**	**А**	**М**	**У**
4	1	**М**							
5	2	**А**							
6	3	**М**							
7	4	**А**							
8	5	**_**							
9	6	**М**							
10	7	**Ы**							
11	8	**Л**							
12	9	**А**							
13	10	**_**							
14	11	**Р**							
15	12	**А**							
16	13	**М**							
17	14	**У**							

При составлении формулы необходимо использовать абсолютные ссылки на столбец символов сообщения и строку символов алфавита. В таком случае формулу из ячейки H3 можно скопировать на все ячейки матрицы.

Логическая функция ЕСЛИ проверяет совпадение символов. В пределах каждой из строк должна быть только одна единица (все символы алфавита разные, поэтому в строке совпадение только одно).

Количество единиц в столбце дает частоту повторения символов алфавита во всем сообщении.

H4 = =ЕСЛИ($G4=H$3;1;0)

	F	G	H	I	J	K	L	M	N
1		**Количество**	**1**	**1**	**2**	**1**	**4**	**4**	**1**
2	**Номер**		1	2	3	4	5	6	7
3		**Символ**	**Ы**	**Л**	**_**	**Р**	**А**	**М**	**У**
4	1	**М**	0	0	0	0	0	1	0
5	2	**А**	0	0	0	0	1	0	0
6	3	**М**	0	0	0	0	0	1	0
7	4	**А**	0	0	0	0	1	0	0
8	5	**_**	0	0	1	0	0	0	0
9	6	**М**	0	0	0	0	0	1	0
10	7	**Ы**	1	0	0	0	0	0	0
11	8	**Л**	0	1	0	0	0	0	0
12	9	**А**	0	0	0	0	1	0	0
13	10	**_**	0	0	1	0	0	0	0
14	11	**Р**	0	0	0	1	0	0	0
15	12	**А**	0	0	0	0	1	0	0
16	13	**М**	0	0	0	0	0	1	0
17	14	**У**	0	0	0	0	0	0	1

Количество повторений символов алфаавита в сообщении получено в первой строке при помощи функции математической функции СУММ( ).

Повторим расчет частот появления символов дважды: 1) для открытого текста; 2) для шифртекста.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	**Сообщение**	УМУМРУЛ_МРАМУЫ					**Количество**	**1**	**1**	**2**	**1**	**4**	**4**	**1**
2	**Длина сообщения**	14				**Номер**		1	2	3	4	5	6	7
3	**Алфавит сообщения**	Л_РАМУЫ					**Символ**	**Л**	**_**	**Р**	**А**	**М**	**У**	**Ы**
4	**Размер алфавита**	7				1	**У**	0	0	0	0	0	1	0
5						2	**М**	0	0	0	0	1	0	0
6	**Номер**	**Символ**	**Повтор**			3	**У**	0	0	0	0	0	1	0
7	1	У	3			4	**М**	0	0	0	0	1	0	0
8	2	М	4			5	**Р**	0	0	1	0	0	0	0
9	3	У	6			6	**У**	0	0	0	0	0	1	0
10	4	М	9			7	**Л**	1	0	0	0	0	0	0
11	5	Р	10			8	**_**	0	1	0	0	0	0	0
12	6	У	13			9	**М**	0	0	0	0	1	0	0
13	7	Л	#ЗНАЧ!	Л		10	**Р**	0	0	1	0	0	0	0
14	8	_	#ЗНАЧ!	Л_		11	**А**	0	0	0	1	0	0	0
15	9	М	12	Л_		12	**М**	0	0	0	0	1	0	0
16	10	Р	#ЗНАЧ!	Л_Р		13	**У**	0	0	0	0	0	1	0
17	11	А	#ЗНАЧ!	Л_РА		14	**Ы**	0	0	0	0	0	0	1
18	12	М	#ЗНАЧ!	Л_РАМ										
19	13	У	#ЗНАЧ!	Л_РАМУ										
20	14	Ы	#ЗНАЧ!	Л_РАМУЫ										

При помощи специальной вставки скопируем (только значения) результаты расчетов частот появления символов открытого текста и шифртекста на новый рабочий лист. Сравните положение символов в алфавитах и их частоты.

	A	B	C	D	E	F	G	H	I	J	K
1	**Открытый текст**	**МАМА_МЫЛА_РАМУ**									
2	**Символ**	Ы	Л	_	Р	А	М	У			
3	**Количество**	1	1	2	1	4	4	1			
4											
5	**Шифртекст**	**АМАМЛЫМ_АР_А__УМ**									
6	**Символ**	Л	_	Р	А	М	У	Ы			
7	**Количество**	1	1	2	1	4	4	1			
8											
9	**Вывод**	Статистическая связь между символами открытого текста и шифртекста ?????									

Сделайте вывод о наличии или отсутствии статистической связи между символами открытого текста и шифртекста (написать вместо знаков вопроса ?????).

4. Подбор неизвестного ключа для заданного шифртекста

Заключительная часть работы посвящена вскрытию шифра циклического сдвига.

В предлагаемых заданиях в качестве шифртекстов для взлома шифра Цезаря использованы афоризмы Марка Твена. Алфавиты открытых текстов сообщений имеют размер около 20-30 символов, что определяет максимальное количество вариантов шифрования (и, соответственно, глубину перебора).

Для дешифрования сообщения следует скопировать расчетную таблицу шифрования на отдельный рабочий лист. Взлом шифра осуществляется перебором возможных значений ключа.

	A	B	C	D	E	F	G	H	I	J
1	**Открытый текст**	ЕУДО,НРУ_ПМГ,МКМРАВНДУГУЫКМНСЬ,ГОИТ								
2	**Длина сообщения**	36								
3	**Алфавит сообщения**	Е_ПРАВДУЫКМНСЬ,ГОИТ								
4	**Размер алфавита**	19								
5	**Ключ сдвига**	9								
6	**Шифртекст**	КОГДА_СОМНЕВАЕТЕСЬ,_ГОВОРИТЕ_ПРАВДУ!								
7										
8	**Номер**	**Символ**	**Повтор**			**Позиция**	**Сдвиг**	**Коррекция**	**Шифр**	
9	1	Е	#ЗНАЧ!	Е		1	10	10	К	К
10	2	У	8	Е		8	17	17	О	КО
11	3	Д	21	Е		7	16	16	Г	КОГ
12	4	О	34	Е		17	26	7	Д	КОГД
13	5	,	13	Е		15	24	5	А	КОГДА
14	6	Н	20	Е		12	21	2	_	КОГДА_

Содержание отчета о лабораторной работе:

- номер группы, ФИО, дата выполнения работы;
- открытый текст сообщения и его длина;
- ключ (сумма цифр номера варианта плюс пять);
- шифртекст;
- алфавит открытого текста и частоты появления символов;
- алфавит шифртекста и частоты появления символов;
- вывод о наличии или отсутствии статистической связи между символами открытого текста и шифртекста;
- открытый текст афоризма;
- подобранный ключ шифрования афоризма.

Варианты ключа простого сдвига

Вар.	1	2	3	4	5	6	7	8	9	10
Ключ	5	2	3	4	5	3	6	4	2	3

Вар.	11	12	13	14	15	16	17	18	19	20
Ключ	4	2	3	5	4	6	3	2	4	5

Вар.	21	22	23	24	25	26	27	28	29	30
Ключ	3	4	2	5	3	5	4	6	2	4

Варианты открытого текста сообщений

1. ВЕСЕЛО_И_ЛАСКОВО_СЛОВО_СОКОЛА
2. АЛЕН_ДЕЛОН_НЕ_ПИЛ_ОДЕКОЛОН
3. НЕТУ_СИЛ_У_ЛИСЫ_ПЛЕСТИ_СЕТИ
4. ТУРОК_СТЕРЕГ_СУРКА_У_СТОГА
5. ТАРАКАН_ИСКАЛ_КАРАВАН_РИСА
6. КАРЛ_У_КЛАРЫ_НЕ_КРАЛ_КОРАЛЛЫ
7. РАНО_МОНАРХ_НАХАМИЛ_МОНАХУ
8. КЛАРА_У_КАРЛА_УКРАЛА_КЛАРНЕТ
9. РАД_КОНОКРАД_ДАРЕНОЙ_КОРОВЕ
10. КАЗАК_ЗАКАЗАЛ_ФАЗАНА_В_КАЗАНЕ
11. ТАРАКАН_УВОЛОК_ВОРОНУ_У_РАКА
12. СОКОЛ_ЛАСКЕ_РАССКАЗАЛ_СКАЗКУ
13. НАПОЛЕОН_ПОЛОЛ_НА_ПОЛЕ_ЛУК
14. НЕДАРОМ_МНОГО_МАРОДЕРОВ_В_МОРЕ
15. ПЛАКАЛА_ВОРОНА_НА_КАРНАВАЛЕ
16. САВАННА_ПОЛНА_КАРАВАНОВ_КОРОВ
17. ЛОСОСЬ_НАСЫПАЛ_СОЛЬ_НА_САЛО
18. ПОСОЛ_ПОД_СТОЛ_ПОЛОЖИЛ_ТОПОР
19. В_МОРГЕ_ГАРЕМА_ГРОМКО_ГРЕМЕЛО
20. ВАРАН_НАПАЛ_НА_КАРАВАН_ВАНИЛИ
21. РЕВИЗОР_ВЕЗ_ТЕЛЕВИЗОР_ЗВЕРЮ
22. В_САЛАКЕ_МАЛО_САЛА_И_МАСЛА
23. КАБАН_И_БАРАН_КУРИЛИ_ТАБАК
24. УЛИТКА_ЗАПОЛЗЛА_ЗА_КАЛИТКУ
25. ВОБЛА_БЫЛА_В_КАБАЛЕ_У_ВОЛОВ
26. РИС_С_БАРБАРИСОМ_И_РЕДИСОМ
27. ЛОСЬ_И_ОСА_ЕЛИ_СОЛЬ_И_ФАСОЛЬ
28. МАЛ_КОЛОКОЛ_ИЗ_ВОЛОКОЛАМСКА
29. ОСА_ПОКУСАЛА_ОСЛИКУ_ЛОПАТКУ
30. ВАССАЛ_ПОСЛАЛ_ПИСЬМО_В_ЛАОС

Шифртексты

Вариант	Шифртекст	Вариант	Шифртекст
1	ЦРЯ:ЛХОЗКЕНБИЯЙЧЯУБЬАХЯ:КХ.ЗХРЯЖЦВ.ХЬАБЖЧРД:ЕЯЖЯ.ЖЗСЯ:КЗ_ЧЕСТЯХ:КБЯЗЯЖЧ:ЯЙХРЯ:ЬХ.:РЖПЯБЯХ:КБЯЦЙБЯЗЯЖЧ:ЯХ:РД,	16	ЗЖП-УЬЗСЬ.УКЛОЛС-Ь-ЛВАЬВЛВЬПЙИУАЬМЬКЛЮ,СЬ-УТНВУЬЗЛЖ,ЗУ_-НАЬ_ЬВУ-УКУЕЬСРУЬ.КЖЗЖЧЛД-ЬЗЛЬ,СКЙГ
2	НИЫЧ.ЬБЛИ.ЬБИЗГИЬЛИКДЛЬМИЧ.ВДЬКИБТУК_МРЧЛЗИТНКОИЬПВНТЮНЛЬЬКТЮМСИЕИНКТЕПЛТЛЬМОИКЬВИНТЛА.ВИЮПЛЫЧЛЮИПЛЗКЬЮВС	17	ЧЬСУСП-ПОМТ.П_ЧЛЙ,П-ПЧЬ_ЕСБ!ИЧЖДЗПЙОВ!ЧЖУЙ!!ИЙ.ПЕЖИП!СОЙН!ИП–ОЙЧДП!СП–ЙТЬЙ.ПЫПХЙ–УЙЧЖ!ИЧЖДА
3	ГН!НЫНБ_ШЯНБЧЕЧИЬРБДЖЯМБДИЬБЖЯЬАЧЯНЖУБЬЕЧАОНБЖНЖ,!М,УТБНОБИНХБ_Ш,УБЬ.Д!ДОТБА,НБОДБКН.,Н!ЛД,БАЬСМГБЫЬ,НПВ	18	ЙЭАУ.ВЬНЫЭГХНВДЬНКВЙЮРСЕЫМЬТГЫЬ.ЫЭГВЙЮГЬХ.ЫЙЫРСЭГЙЮАЬЕА_ЫГЫКПИЬРО.ЧИЬЮЬХ.ЮЙЮГЬЙЭАЯЬНКЫЛЮЯМ
4	В.ЮКИ.ВЮСНТК,НПЮВНЮБЕКБКДНВЮЕКВРЯЛ_ЮСЯКЮЯОПКНЮВОБЯКРЧОРЮТЬДК,Л_ЮЕКПОЮВНЮЕЩКА.,НЯЮ,ЮДЩОПНЮСНЯ,НЩЯЛЮ,НПОЖ	19	Н_ЕВЧУТЫКЯНМРШЯПДУРУМЯ.ЯПД,АУЬ_ИЯМЫКСУЕЧКУЫПМИОПДУИЫПУРУЫМЫЛЕЯПЧНДЛЫУИЯ.ШЧАПДУ,ЫКЛЧЛРАЗ
5	ХЕЩИЬТГХПЕАЬКЬХМВЛГПГТБГРЬБГЬ-ГУВДЕЙВЩИЬТП,Л.АОЬУВУЬХЕЩИЬТГХПЕАОЬКЬЗ_ЗЬХМВЛГПГТБЗНОЬ.ЬБЗЬЩВУЬЫМГ-ГЩБГР	20	ХЛАЫ,СДЫ,.Л,ЧЗЮДЮ,ХЫШЮД,ЧУЛЗ.ЬДИЧЙ,ЧЫ,ЧПРПЫЯ_,ПЫДЫУРЕ,ЗОВОЗЛЮД,З,.ЛЧ,МЫУЫЖЬЯ,КЮУЮЗЫТН
6	ЕТБСЬБЙ:И.Ж_ЭБО:ИИЙС_Ч_ПНБМЙС_Ч_ПИНЙЬ.НЛИ:ЙЕТДЬИТЛДСБ,УПРЙЕТБСЬ.Е.Ь.ЖДРАЙБЙЕТБСЬБЙСЙЯ,.ЧЙ:ИЙ:ЫЛЬБИ,ПРВ	21	ЛТПЕАЛЬ_КОКУЬАКЛАВДАЬЭ-ЕПХЭПКЛЬД,М.КЭКИАХЬДАЕ_КХ,СКЛЬД,МАТРК,КХПКАЬЛ.ЬЛЬ-ЭПКЛЬД,М,Н
7	ЧДКЗЯ,ЯЗИ_ЕЯВШЗИЯЗАШТРОС.РЯЙЦЗЫШЮШЛЗТДЮ_ЩРЗМИЯМЯЙЗПЛЩШУЗРЗТДАРНЕЯЙЗЙРТУЗМ:Ш.ИШЗМИЯМ:РЗЩЯ:ДГЗЫ:РИЯЙДХ	22	СМЕЧЛЬПМОЬЯЮЕМЬЖКЬМЯЮГРЬЧМ_ЕМЬ.ЧЮЖОЬГЛСМГЮИЬДАЫНМЧЫПОЬМГМЬСЛ.ЮПЦТЬГЮМ.ЫЧЛГГМЦПРХ,
8	ДШОАЧ_ШУОВШКШЕВЧКОТКР,ШКШ_ИР,ХЫОИЧВМШОРУШСПОЕСЖКХШОТЬ_ШКНЖДДХШОАКРИИРЖДСХ.ОВШУОДШОРУШСПОДРБЖБРЛЫ	23	ИДЫАРДЯЖМЖДСВ_Г-РД__АДЖЛВРА-_АДЕЖЯА-АЭАДЖОАЛД-ЖЯЭТГ_Д-ПЖВЖВОДД-ЖСЫ.ЖЧ-А,АЖКАРАСНЬ
9	ЭЛЬ,ТСО;Ч;З.ЛЬ,ЬЕ;У-Г;,Г.:,С;ДСРИЕ;,С;_Г.ЬЕ;,С;,ЛЬЫЗ.ЫГ,,ФЗ.СН;Ы;ФЗ.Ь_К,ФР;АГ;Й.Ф;ЦЯ-ГЗ,ИМ;ВЛЬМЖ	24	Й_ПЫЦШЙ-ПУВКВАП.НЧПШЛВШНЬНЫОТВЕП.ЙПЬВАЬНК.ЦДНЛВИНЬН_РВАЬНВЬЙШВ-ПВЕП.Й.ЦВЫЙ-Б,ПМ
10	ИХИРЖ_ХЛКВЯСРВЬЕЗЧРШХ,ВЬПКНУРЖЯЕЧ,НКРКРТЧРЖЯВЬЕКНУРКАСРЕЧ.РЖЯВУШЯЛХНУ,ОРЖЯЕЧ,НО.КРТЧШХ,ВЬПЧТТЯМ	25	УИОНЖО-М-РОБЧЗ-СЗ,,ЧЗ-ХД-.ЧВЧА-Т.Ч-_-,ОР-ЗР.ПЬ-Ц_ЖЗБ-ГЗ-ИОРЕЧЖЧНО.П-ЗЗ-ЦЗИЗГ,Ч;
11	ХЛЬКОЬБЙХЬОЬЛАЙЬКТЧСЛ,ДЙГКЛЙАЧЙХЬДДЮМКРЛ,ЙОДРАКВЫЙЧИКДЬКЧИ_ЙЛ,НЕКИКТЙЧЬГКДИКДЬ.ЬЛИУКВЫЙЧИКДЬ,Г	26	ЫБИГРКАЖВНЯЕ.УНИНГРПРВ_НТРУЯБНГЙНЫЩНДЕБС,НТРУЯБНГЙНДЕБС_НТБОЯЙВНП.ЯЩГНИНГРПРВ,
12	ЩЯ,ЛЕАЗЛБВПЛК_ГЛБЫРКЫЛМБЕЗХЗОБАЛНЗ.ЗКЛХ_ЧСЫБРЛПСБДП_ЕМ_СА_АСТБЯБ.ЗМЗПЗУЗБАСБПЯ.СДБЩЛМЙПЛБМЯВСИ	27	ЗЮКЬУПЯШЧЮКАЮЛПД,ПВЗВЕЮМРП.БЮНПЬЮОУПВ_КБАЮДЧКЗРЬЗЮНАОЧВЬЮНПАНИЮП.ГЧДП,ЧКЬЫТ
13	ЭИ,_ЛОРЛМБШЭЫ_,_ТЛЬЫЯЛОРЛВБЛИЫЯ.ЯВЭЛГЯ,ЙЧ_ВИЫОБТЛПЫЯЛОЭ.ВРАЛС._МВБЕЛЫЯНЯТЛЬЫЯЛСЯ.БЛШЭВЗЫЙИЗК	28	_ЯКЙГЙШЗБТЕЯКШОЙВБАКЛЯОБЕМКЛС-ДСКЬКЯШОПКИЕСК_ЯКУДСЩПЕКРБЭК-СОМ.ПЭКЙЧЯД-СЭН
14	Р,ЛГ.ВЗС,.ГУБЛВЫЛУНЮГВ.АТЩЛГУБЛМГ,ЛИЛАТПГСУ.ВЗГЕ.ИО.У.ШЬУТГВАЛНУЮ_ЫДГЬРЕБ.ШЬЧЬБ.ШХ,,ЫДГБЛСТЯ	29	ХОУРЖЛТЯ,П,УГОУПВГОМУНАДАЛА.ОЕУ.АУЮП_УГАПММУЬМЯМПОДУСАЛИМЯСЬУ.МУКАЮ,П,ЯБЫ
15	МДЭЛПМТЭСЬ.МРЬ-ЬЭКЮРЬ,ПЧМЭПМ.З-МВЭСПМЭМЧЭЧЬЭ,КОЬ.ЭРЭП_ИЗТЬВЭЧМЭЕМСЬТНЭЧЬЭ,КОЬ.ЭБЭЧЬКЮРЬ,ПЧМУ	30	Г-;,И;Д_ТГЧБ,_СДЫЙЧК-ДХД,ВДОДК-ЮЧТГ_МД-ДОДРКАТГ_НД,-Д,ВЕВТ-.ДЫЙЧК-Д,ВГУ

Контрольные вопросы

- Чем отличается алфавит сообщения от самого сообщения?
- Может ли размер алфавита быть равен размеру сообщения?
- Может ли размер алфавита быть больше размера сообщения?
- Какие символы могут входить в алфавит сообщения?
- Что означают единицы и нули в прямоугольной матрице в диапазоне ячеек H4:N17 (диапазон ячеек указан для примера, приведенного в задании)?
- Чему равна сумма всех единиц в этом диапазоне ячеек?
- Что означает сообщение об ошибке #ЗНАЧ! текстовой функции НАЙТИ()?
- Является ли сообщение об ошибке #ЗНАЧ! текстовой функции НАЙТИ() признаком неправильности выполнения вычислений?
- Является ли для логических функций значение ЛОЖЬ признаком неправильности выполнения вычислений?
- Чем шифрование отличается от кодирования?
- Должен ли быть секретным шифр (алгоритм шифрования)?
- Должен ли быть секретным ключ шифра?
- Кто может знать алгоритм шифрования?
- Кто должен знать ключ шифра?
- Что делать, если размер ключа меньше размера текста?
- В чем заключается идея шифра простого сдвига?
- Сколько уникальных вариантов ключа можно получить для заданного сообщения?
- Легко ли подобрать ключ шифра простого сдвига?
- Алфавиты открытого текста и шифртекста совпадают или отличаются?
- Видно ли из сравнения алфавитов, что сдвиг символов – циклический?
- Частоты появления символов открытого текста и шифртекста совпадают или отличаются?
- Как изменяются частоты появления символов шифртекста по сравнению с открытым текстом в шифре простого сдвига?
- Можно ли по сдвигу частот появления символов определить неизвестную величину циклического сдвига?