Лабораторная работа №12. Модифицированный шифр Цезаря.

Цель работы

Выполнить шифрование заданного сообщения модифицированным шифром Цезаря (сдвиг по кодовому слову) и выполнить статистический анализ шифртекста.

Модификация циклического сдвига: переменный сдвиг

Шифр Цезаря обладает существенным недостатком – поскольку величина циклического сдвига всегда постояннна, то одна и та же буква открытого текста всегда превращается в одну и ту же букву шифртекста (по таблице циклического сдвига). Это позволяет (зная алгоритм шифрования) легко подобрать неизвестный ключ (величину сдвига).

Для усиления стойкости шифра предлагается использовать несложную модификацию шифра: величина сдвига будет переменной. Например, для нечетных букв открытого текста будем использовать сдвиг k=1, а для четных букв открытого текста – сдвиг k=2.

Открытый текст «ШЛА_САША_ПО_ШОССЕ»

Алфавит А = {_, А, Е, Л, О, П, С, Ш}

Открытый текст	Ш	Л	А	_	С	А	Ш	А	_	П	О	_	Ш	О	С	С	Е
Позиция в алфавите	8	4	2	1	7	2	8	2	1	6	5	1	8	5	7	7	3
Сдвиг	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
Новая позиция	1	6	3	3	8	4	1	4	2	8	6	3	1	7	8	1	4
Шифртекст	_	П	Е	Е	Ш	Л	_	Л	А	Ш	П	Е	_	С	Ш	_	Л

Шифр переменного сдвига обладает свойством перемешивания: нет однозначной связи между символами открытого текста и шифртекста. Действительно, в рассмотренном примере буква А в нечетной позиции (сдвиг k=1) превращается в букву Е, а в четной позиции (сдвиг k=2) превращается в букву Л. Аналогично, пробел превращается с переменным сдвигом либо в букву А, либо в букву Е, а буква С – в букву Ш и пробел.

Открытый текст	Ш	Л	А	_	С	А	Ш	А	_	П	О	_	Ш	О	С	С	Е
Позиция в алфавите	8	4	2	1	7	2	8	2	1	6	5	1	8	5	7	7	3
Сдвиг	1	2	**1**	2	1	**2**	1	2	**1**	2	1	**2**	1	2	**1**	**2**	1
Новая позиция	1	6	3	3	8	4	1	4	2	8	6	3	1	7	8	1	4
Шифртекст	_	П	Е	Е	Ш	Л	_	Л	А	Ш	П	Е	_	С	Ш	_	Л

По тем же причинам одни и те же символы шифртекста образуются из разных символов открытого текста. В рассматриваемом примере показано образование символов Е и Ш и пробела в шифртексте из разных символов открытого текста.

Открытый текст	Ш	Л	А	_	С	А	Ш	А	_	П	О	_	Ш	О	С	С	Е
Позиция в алфавите	8	4	2	1	7	2	8	2	1	6	5	1	8	5	7	7	3
Сдвиг	1	2	**1**	**2**	**1**	2	1	2	1	**2**	1	2	**1**	2	1	**2**	1
Новая позиция	1	6	3	3	8	4	1	4	2	8	6	3	1	7	8	1	4
Шифртекст	_	П	Е	Е	Ш	Л	_	Л	А	Ш	П	Е	_	С	Ш	_	Л

Алфавит шифртекста может отличаться от алфавита открытого текста. В примере алфавит шифртекста А’ = {_, А, Е, Л, П, С, Ш }. Буквы О в алфавите шифртекста нет, так как в нее не превратилось ни одной буквы открытого текста. Эта особенность проявляется преимущественно в коротких текстах. В больших текстах более вероятно совпадение алфавитов, но частоты появления символов в алфавитах будут отличаться.

Переменный сдвиг по кодовому слову

Для упрощения запоминания переменного сдвига можно использовать кодовое слово, состоящее из символов алфавита открытого текста. Тогда для получения шифртекста Т’ из открытого текста Т размером N символов с алфавитом А размером М символов и кодового слова К можно использовать следующий алгоритм:

1. Извлечь очередную букву T_i открытого текста Т (1<i<N).

2. Найти позицию этой буквы j в алфавите А (1<j<M).

3. Извлечь очередную букву кодового слова К. Если буквы в кодовом слове закончились, перейти обратно к первой букве кодового слова.

4. Найти позицию буквы кодового слова k в алфавите А (1<k<M).

5. Сложить позиции буквы открытого текста и буквы кодового слова i’=j+k.

Если j+k>M, то i’=j+k-M (циклический сдвиг).

6. Извлечь из алфавита букву с номером i’.

7. Дописать очередную букву $A_{i'}$ к строке шифртекста Т’.

Этапы выполнения работы

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

2. Сравнить алфавиты и частоты появления символов открытого текста и шифртекста.

3. Выписать три наиболее часто встречающиеся буквы открытого текста и найти, в какие символы шифртекста они превращаются.

4. Выписать три наиболее часто встречающиеся буквы шифртекста и найти, из каких символов открытого текста они образуются.

5. Сделать выводы:

1) о наличии или отсутствии статистической связи открытого текста и шифртекста;

2) о наличии свойства перемешивания у шифра с переменным сдвигом.

1. Шифрование сообщения

Рассмотрим шифрование открытого текста шифром циклического сдвига по кодовому слову на следующем примере: открытый текст "МАМА_МЫЛА_РАМУ", кодовое слово К=»УРА».

Начало работы не отличается от шифра постоянного циклического сдвига: нам потребуется открытый текст сообщения и его размер, а также алфавит сообщения и его размер.

Кроме того, отведем пару строк для кодового слова и шифртекста.

Далее (также как в предыдущих работах) найдем алфавит сообщения и рассчитаем его размер при помощи текстовых функций ПСТР(), НАЙТИ(), ЕОШИБКА(), СЦЕПИТЬ(), ДЛСТР().

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

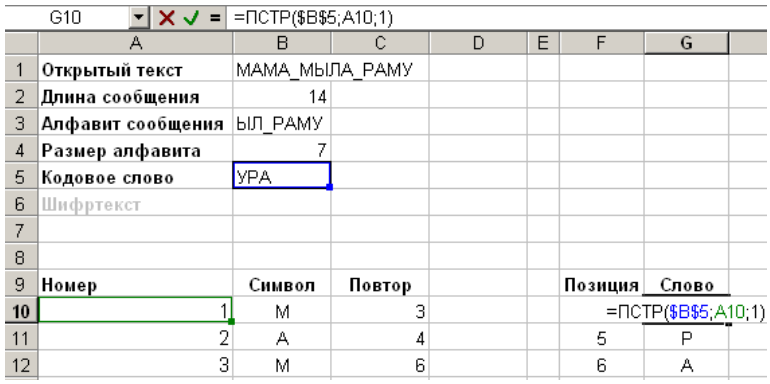
	A	B	C	D
1	**Открытый текст**	МАМА_МЫЛА_РАМУ		
2	**Длина сообщения**	14		
3	**Алфавит сообщения**	ЫЛ_РАМУ		
4	**Размер алфавита**	7		
5	**Кодовое слово**	УРА		
6	**Шифртекст**			
7				
8				
9	**Номер**	**Символ**	**Повтор**	
10	1	М	3	
11	2	А	4	
12	3	М	6	
13	4	А	9	
14	5	_	10	
15	6	М	13	
16	7	Ы	#ЗНАЧ!	Ы
17	8	Л	#ЗНАЧ!	ЫЛ
18	9	А	12	ЫЛ
19	10	_	#ЗНАЧ!	ЫЛ_
20	11	Р	#ЗНАЧ!	ЫЛ_Р
21	12	А	#ЗНАЧ!	ЫЛ_РА
22	13	М	#ЗНАЧ!	ЫЛ_РАМ
23	14	У	#ЗНАЧ!	ЫЛ_РАМУ

Далее в столбце F (Позиция) при помощи функции НАЙТИ() определим, какую позицию занимает текущий символ открытого текста в алфавите сообщения. F10=НАЙТИ(B10;B3;1)

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

Далее в столбце G в первых ячейках запишем кодовое слово при помощи функции ПСТР() со ссылкой на ячейку B5 с кодовым словом.

G10=ПСТР(B5;A10;1)



Далее при помощи относительной ссылки распространяем вниз кодовое слово на оставшиеся расчетные ячейки.

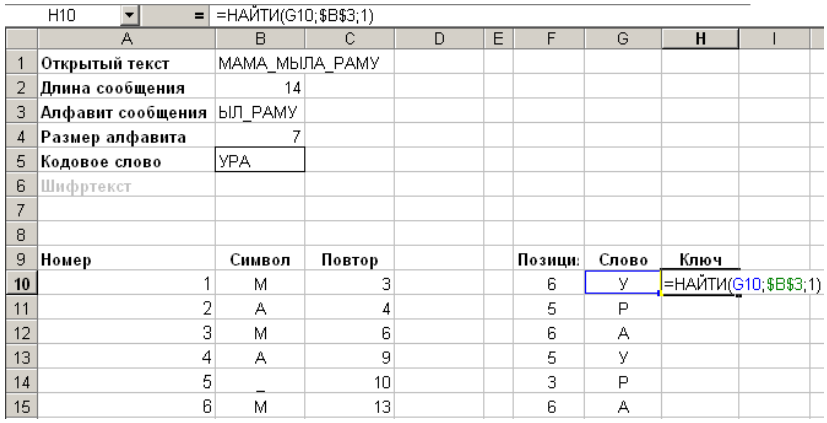
Следующий шаг – перейти от буквы кодового слова к ключу сдвига – номеру буквы в алфавите.

Сравните формулы в столбцах F и H:

H10=НАЙТИ(G10;B3;1)

В обоих случаях мы ищем номер позиции некоторой буквы в алфавите сообщения.

Но сначала (столбец F) буква берется из открытого текста, а затем (столбец H) – из кодового слова.



	A	B	C	D	E	F	G	H	I
H10	=	=НАЙТИ(G10;B3;1)							
1	**Открытый текст**	МАМА_МЫЛА_РАМУ							
2	**Длина сообщения**	14							
3	**Алфавит сообщения**	ЫЛ_РАМУ							
4	**Размер алфавита**	7							
5	**Кодовое слово**	УРА							
6	**Шифртекст**								
7									
8									
9	**Номер**	**Символ**	**Повтор**			**Позиция**	**Слово**	**Ключ**	
10	1	М	3			6	У	=НАЙТИ(G10;B3;1)	
11	2	А	4			5	Р		
12	3	М	6			6	А		
13	4	А	9			5	У		
14	5	_	10			3	Р		
15	6	М	13			6	А		

Построение остальных формул достаточно очевидно. Сдвиг определяется как сумма позиций исходной буквы и ключа. Коррекция нужна для проверки необходимости циклического сдвига. Символы шифртекста извлекаются снова из строки алфавита. Строка шифртекста получается из отдельных символов (начиная с пустой строки в ячейке L9=””) при помощи функции СЦЕПИТЬ().

	A	B	C	D	E	F	G	H	I	J	K	L
1	**Открытый текст**	МАМА_МЫЛА_РАМУ										
2	**Длина сообщения**	14										
3	**Алфавит сообщения**	ЫЛ_РАМУ										
4	**Размер алфавита**	7										
5	**Кодовое слово**	УРА										
6	**Шифртекст**	МЛРАУРЫМ__Ы_МР										
7												
8												
9	**Номер**	**Символ**	**Повтор**			**Позиция**	**Слово**	**Ключ**	**Сдвиг**	**Коррекция**	**Шифр**	
10	1	М	3			6	У	7	13	6	М	М
11	2	А	4			5	Р	4	9	2	Л	МЛ
12	3	М	6			6	А	5	11	4	Р	МЛР
13	4	А	9			5	У	7	12	5	А	МЛРА
14	5	_	10			3	Р	4	7	7	У	МЛРАУ
15	6	М	13			6	А	5	11	4	Р	МЛРАУР
16	7	Ы	#ЗНАЧ!	Ы		1	У	7	8	1	Ы	МЛРАУРЫ
17	8	Л	#ЗНАЧ!	ЫЛ		2	Р	4	6	6	М	МЛРАУРЫМ
18	9	А	12	ЫЛ		5	А	5	10	3	_	МЛРАУРЫМ_
19	10	_	#ЗНАЧ!	ЫЛ_		3	У	7	10	3	_	МЛРАУРЫМ__
20	11	Р	#ЗНАЧ!	ЫЛ_Р		4	Р	4	8	1	Ы	МЛРАУРЫМ__Ы
21	12	А	#ЗНАЧ!	ЫЛ_РА		5	А	5	10	3	_	МЛРАУРЫМ__Ы_
22	13	М	#ЗНАЧ!	ЫЛ_РАМ		6	У	7	13	6	М	МЛРАУРЫМ__Ы_М
23	14	У	#ЗНАЧ!	ЫЛ_РАМУ		7	Р	4	11	4	Р	МЛРАУРЫМ__Ы_МР

Результат заносим в ячейку шифртекста при помощи специальной вставки.

2. Статистический анализ открытого текста и шифртекста

2.1. Для статистического анализа открытого текста и шифртекста воспользуемся созданной ранее расчетной электронной таблицей, скопировав из нее рабочий лист с расчетом частот появления символов в текущую рабочую книгу.

Повторим поиск алфавитов и расчет частот появления символов дважды:

1) для открытого текста;

2) для шифртекста.

При помощи специальной вставки скопируем (только значения) алфавиты и 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
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**	**МЛРАУРЫМ__Ы_МР**						
6	**Символ**	Л	А	У	Ы	_	М	Р
7	**Количество**	1	1	1	2	3	3	3

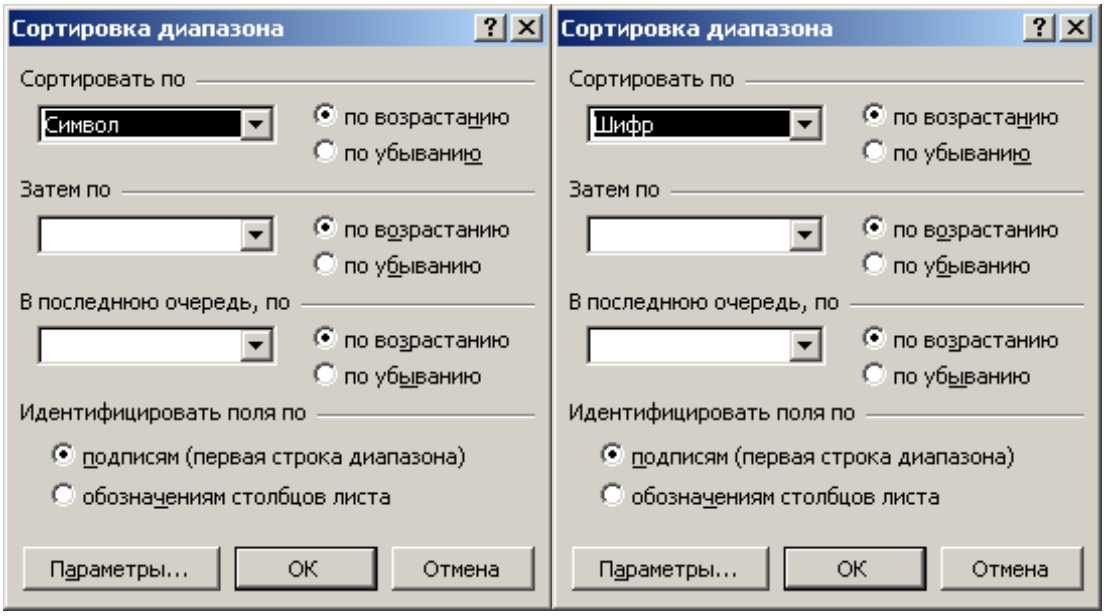
2.2. Для проверки наличия свойства перемешивания у шифра со сдвигом по кодовому слову скопируем трижды при помощи специальной вставки (только значения …) на новый рабочий лист столбцы с символами открытого текста (столбец B) и шифртекста (столбец K).

	A	B	C	D	E	F	G	H
1	**Символ**	**Шифр**		**Символ**	**Шифр**		**Символ**	**Шифр**
2	М	М		М	М		М	М
3	А	Л		А	Л		А	Л
4	М	Р		М	Р		М	Р
5	А	А		А	А		А	А
6	_	У		_	У		_	У
7	М	Р		М	Р		М	Р
8	Ы	Ы		Ы	Ы		Ы	Ы
9	Л	М		Л	М		Л	М
10	А	_		А	_		А	_
11	_	_		_	_		_	_
12	Р	Ы		Р	Ы		Р	Ы
13	А	_		А	_		А	_
14	М	М		М	М		М	М
15	У	Р		У	Р		У	Р

Первую пару столбцов оставим без изменений (для самопроверки), а две другие пары упорядочим их для упрощения поиска повторяющихся символов.

Используем диалоговое окно меню Данные → Сортировка …

Столбцы D и E отсортируем по символам открытого текста, а столбцы G и H – по шифртексту.



Наиболее часто встречающиеся символы открытого текста и шифртекста уже найдены – на рабочем листе статистического анализа – в нашем примере это символы _, А, М для открытого текста и _, М. Р для шифртекста.

Обведем рамками эти символы в соответствующих отсортированных столбцах вместе с соседними символами.

	A	B	C	D	E	F	G	H
1	**Символ**	**Шифр**		**Символ**	**Шифр**		**Символ**	**Шифр**
2	М	М		_	У		А	_
3	А	Л		_	_		_	_
4	М	Р		А	Л		А	_
5	А	А		А	А		А	А
6	_	У		А	_		А	Л
7	М	Р		А	_		М	М
8	Ы	Ы		Л	М		Л	М
9	Л	М		М	М		М	М
10	А	_		М	Р		М	Р
11	_	_		М	Р		М	Р
12	Р	Ы		М	М		У	Р
13	А	_		Р	Ы		_	У
14	М	М		У	Р		Ы	Ы
15	У	Р		Ы	Ы		Р	Ы

Итак, все готово для того, чтобы выписать полученный результат в отчет и сделать вывод о наличии у шифра сдвига по кодовому слову свойства перемешивания.

Один символ открытого текста превращается в разные символы шифртекста:

_ → У, _

А → Л, А, _

М → М, Р

Один символ шифртекста образуется из разных символов открытого текста:

А, _ → _

М, Л → М

М, У → Р

Содержание отчета о лабораторной работе:

- номер группы, ФИО, дата выполнения работы;
- открытый текст сообщения и его длина;
- ключ (кодовое слово);
- шифртекст;
- алфавит открытого текста и частоты появления символов;
- алфавит шифртекста и частоты появления символов;
- наиболее часто встречающиеся буквы открытого текста и соответствующие им символы шифртекста;
- наиболее часто встречающиеся буквы шифртекста и соответствующие им символы открытого текста;
- выводы о наличии перемешивания символов и отсутствия статистической связи между символами открытого текста и шифртекста.

Контрольные вопросы

- 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?
- В чем заключается идея шифра переменного сдвига?
- В чем заключается преимущество переменного сдвига по сравнению с простым?
- Алфавиты открытого текста и шифртекста совпадают или отличаются?
- Частоты появления символов открытого текста и шифртекста совпадают или отличаются?
- Как изменяются частоты появления символов шифртекста по сравнению с открытым текстом в шифре переменного сдвига?
- Есть ли статистическая связь между частотами символов открытого текста и шифртекста (для шифра переменного сдвига)?

Кодовые слова

Вариант	Кодовое слово переменного сдвига	Вариант	Кодовое слово переменного сдвига

Вариант	Кодовое слово переменного сдвига	Вариант	Кодовое слово переменного сдвига
1	ОСЕЛ	16	САЛО
2	КИНО	17	СЛОН
3	СТУЛ	18	СТОП
4	КРОТ	19	ГРОМ
5	КРАН	20	ВИНА
6	РУКА	21	ЛЕТО
7	ХРАМ	22	ЛОСК
8	РУКА	23	РУКА
9	РЕКА	24	ПОЗА
10	ВЕНА	25	УЛОВ
11	РУКА	26	БАРС
12	САЛО	27	САЛО
13	ЛУНА	28	МИЛО
14	ГОРН	29	КОСА
15	РЕКА	30	САЛО