Лабораторная работа 2. **Шифр Цезаря и метод прогрессивного ключа Тритемиуса.**

Цель работы: Освоить технологию шифрования и дешифрования информации в среде MS Excel, с использованием шифра Цезаря. Разработать программный код на языке программирования C#, для

Методические указания

Теоретическая часть

Шифр Цезаря является частным случаем шифра простой замены (*одно*алфавитной 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={a1, a2,…,am,...,a$_N$},

где a1, a2,…,am,...,aN – символы алфавита; **N** ширина алфавита.

Пусть ***k*** – число позиций сдвига символов алфавита при шифровании, 0<***k***<**N**. При шифровании каждый символ алфавита с номером ***m*** из кодируемого текста заменяется на символ этого же алфавита с номером ***m***+***k***. Если ***m***+***k*** >**N**, номер символа в алфавите **A** определяется как ***m***+***k***-**N**.

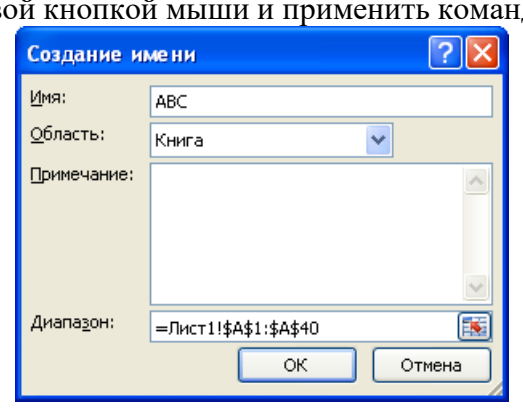
Для дешифрования текстовой информации номер позиции символа восстанавливаемого текста определяется как ***m***-***k***. Если ***m***-***k***<0, то вычисление этого номера производится как ***m***-***k***+**N**. Достоинством этой системы является простота шифрования и дешифрования. К недостаткам системы 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.

Порядок выполнения лабораторной работы

Пример. Выполнить шифрование и дешифрование текста применив метод Цезаря.

1. Войти в среду Excel. Создать новый документ. На первом листе начиная с ячейки **A**1 до **A**40 набрать алфавит, в точности так, как показано на рис. 1а. Выделить весь диапазон алфавита и назначить ему имя "**ABC**". Для этого щелкнуть по выделенному диапазону правой кнопкой мыши и применить команду "Имя диапазона…".

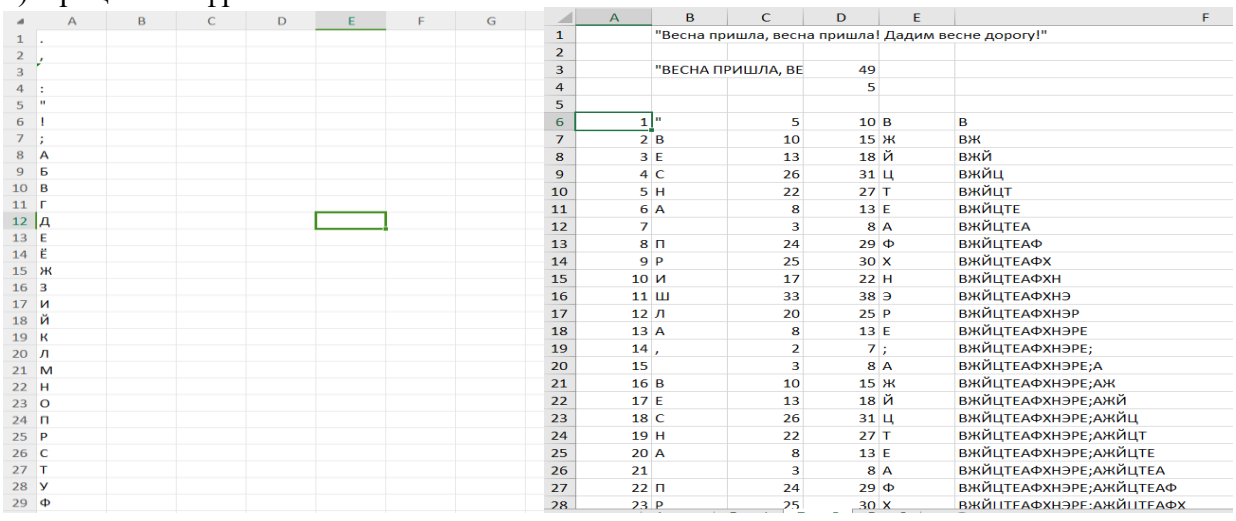


2. На втором листе документа в ячейке **B**1 набрать текст, который необходимо зашифровать, например: **"Весна пришла, весна пришла! Дадим весне дорогу!"**

При наборе текста необходимо использовать только те символы, которые входят в набранный алфавит!

3. В ячейке **B**3 записать формулу "=ПРОПИСН(**B**1)", функция ПРОПИСН переводит символы в строке в прописные буквы.
4. В ячейке **D**3 записать формулу "=ДЛСТР(**B**3)", функция ДЛСТР позволяет определить длину строки, что необходимо пользователю, для кодировки исходной строки. Должно получиться 49.
5. В ячейку **D**4 записать значение **k**, например, 5.
6. В столбце **A**, начиная с ячейки **A**6, пронумеровать ячейки числами последовательного ряда от 1 до **N**, где **N** – число символов в тексте, включая пробелы. **N** рассчитано в ячейке **D**3 (**N** = 49).
7. В ячейку **B**6, записать формулу "=ПСТР(**B**$3;**A**6;1)", которая разделяет кодируемый текст на отдельные символы. Скопировать эту формулу в ячейки **B**7-**B**54.
8. В ячейку **C**6 записать формулу "=ПОИСКПОЗ(**B**6;**ABC**;0)". Функция ПОИСКПОЗ производит поиск индекса (номера позиции) символа в массиве **ABC**, который был определен на листе 2. Скопировать содержимое ячейки **C**6 в ячейки **C**7-**C**54.
9. Получив номер символа в алфавите **ABC**, произвести сдвиг нумерации алфавита для кодируемой последовательности символов. Для этого в ячейку **D**6 записать формулу:
"=ЕСЛИ(ПОИСКПОЗ(**B**6;**ABC**;0)+$**D**$4>40;ПОИСКПОЗ(**B**6;**ABC**;0)+$**D**$4-40;ПОИСКПОЗ(**B**6;**ABC**;0)+$**D**$4)"
(1)
Эта формула производит сдвиг номеров символов алфавита на величину ***k*** и определяет номер заменяющего символа из алфавита **ABC**. Содержимое **D**6 скопировать в область **D**7-**D**54.
10. Выбрать символы из алфавита **ABC** в соответствии с новыми номерами. В ячейку **E**6 записать формулу "=ИНДЕКС(**ABC**;**D**6)". Скопировать содержимое ячейки **E**6 в область **E**7-**E**54.
11. Для получения строки закодированного текста необходимо в ячейку **F**6 записать "=**E**6", в ячейку **F**7 соответственно – "=**F**6&**E**7". Далее скопировать содержимое ячейки **F**7, в область **F**8-**F**54. В ячейке **F**54 прочитать зашифрованный текст.
12. Для проверки произвести дешифрование полученного текста и сравнить его с исходным. На третьем листе выполнить дешифрование аналогично пунктам 2-11 лабораторной работы. При этом необходимо учесть следующие особенности:
- в п. 2 набрать зашифрованный текст;
- в п. 9 в ячейку **D**6 записать формулу:
=ЕСЛИ(ПОИСКПОЗ(**B**6;**ABC**;0)-$**D**$4<0;ПОИСКПОЗ(**B**6;**ABC**;0)-$**D**$4+40;ПОИСКПОЗ(**B**6;**ABC**;0)-$**D**$4). (2)
Получение исходного текста в ячейке **F**54 третьей страницы свидетельствует о корректном выполнении лабораторной работы.

а) Процесс шифрования



б) процесс дешифрования

	B	C	D	E	F	G	H	I	J	K
31	Р	25	20	Л	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛ					
32	Е	13	8	А	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА					
33	Г	11	6	!	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА!					
34	А	8	3		"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА!					
35	И	17	12	Д	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! Д					
36	Е	13	8	А	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДА					
37	И	17	12	Д	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАД					
38	Н	22	17	И	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИ					
39	С	26	21	М	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ					
40	А	8	3		"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ					
41	Ж	15	10	В	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ В					
42	Й	18	13	Е	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕ					
43	Ц	31	26	С	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕС					
44	Т	27	22	Н	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСН					
45	Й	18	13	Е	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ					
46	А	8	3		"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ					
47	И	17	12	Д	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ Д					
48	У	28	23	О	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДО					
49	Х	30	25	Р	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДОР					
50	У	28	23	О	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДОРО					
51	З	16	11	Г	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДОРОГ					
52	Ш	33	28	У	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДОРОГУ					
53	Г	11	6	!	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДОРОГУ!					
54	В	10	5	"	"ВЕСНА ПРИШЛА, ВЕСНА ПРИШЛА! ДАДИМ ВЕСНЕ ДОРОГУ!"					

Рис. 1. Фрагменты документов MS Excel по лабораторной работе.

Задание 1.

1)Зашифровать и дешифровать предложение согласно своему варианту, с числом позиций сдвига – k, применив программное приложение MS Excel.

2) Написать программный код на языке программирования C# для шифрования и дешифрования информации методом Цезаря.

№	Предложение для шифрования	k
1	«Информатика – наука о способах получения, накопления, хранения, преобразования, передачи, защиты и использования информации»	3
2	«Мир информатики» очень хороший журнал.	8
3	«Наибольшего успеха добивается тот, кто располагает лучшей информацией»	5
4	Информация – движущая сила развития общества!	2
5	Не владеть компьютером - быть безграмотным!	1
6	«Человек придает кибернетическим машинам способность творить и создает этим себе могучего помощника»	4
7	«Тайная (важная) информация - это почти всегда источник большого состояния и результат публичного скандала»	7
8	«Информация есть форма отражения материи»	9
9	«Прогресс проистекает из паритета двух начал - хаоса и порядка (энтропии и информации)»	2
10	«Компьютерная программы выполняет ваши приказы, а не ваши желания»	3
11	"Кто владеет информацией, тот владеет миром!"	5
12	Машины должны работать. Люди должны думать.	1
13	Компьютер за две секунды делает столько же ошибок, сколько двадцать человек за двадцать лет непрерывной работы.	8
14	Настоящая опасность не в том, что компьютеры начнут мыслить, как люди, а в том, что люди начнут мыслить, как компьютеры.	5
15	Информатика — это операционная система для всех инноваций.	6

16	В обычной науке вам дан мир, и ваша задача — выяснить правила. В информатике вы даете компьютеру правила, и он создает мир.	3
17	Программная инженерия — это та часть компьютерных наук, которая слишком сложна для компьютерного ученного.	4
18	Термин «информатика» был впервые определён Солом Горном из Пенсильванского университета в тысяча девятьсот восемьдесят третьем году.	9
19	Рекурсия — основа программирования, поскольку она сокращает время написания программы.	1
20	«Математика - гимнастика ума!»	5

Задание 2. Изучить метод шифрования с применением прогрессивного ключа Тритемиуса (*методом ключа Вигнера)* и зашифровать слово согласно своему варианту написав программный код на языке программирования C#.

№	Слово для шифрования	Ключевое слово
1	Информатика	поток
2	Программирование	тип
3	Шифрование	поле
4	Криптография	ключ
5	Криптосистема	шифр
6	Шифр Цезаря	тип
7	Квадрат Полибуса	шифр
8	Методы шифрования	ключ
9	Дешифрование	вид
10	Цифровая подпись	поток
11	Безопасность	пять
12	Конфиденциальность	стик
13	Симметрия	вид
14	Асимметрия	пять
15	Криптология	три
16	Компьютер	два
17	Программы - шифраторы	один
18	Алгоритмы шифрования	ключ
19	Ключ шифрования	шифр
20	Блочное шифрование	блок