# Лаб. Работа 1. Шифр Цезаря

***Цель работы***: Освоить технологию шифрования и дешифрования информации в среде Excel с использованием шифра Цезаря.

## 1. 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:

$$\mathbf{A}=\{a_1, a_2,\ldots,a_m,\ldots,a_N\},$$

где $a_1, a_2,\ldots,a_m,\ldots,a_N$ **–** символы алфавита; **N** ширина алфавита.

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

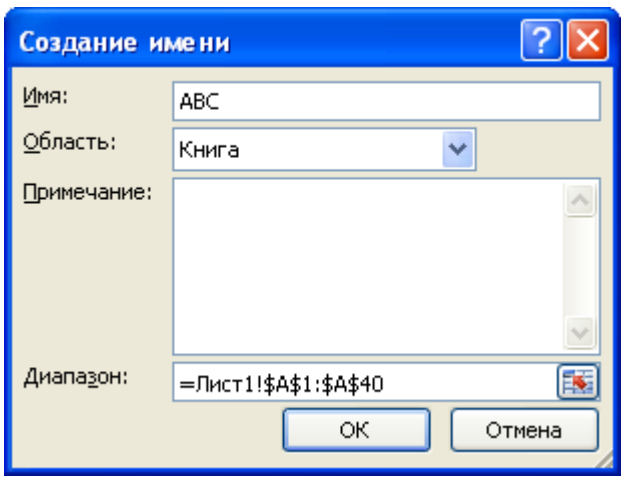
Для дешифрования текстовой информации номер позиции символа восстанавливаемого текста определяется как $\boldsymbol{m}-\boldsymbol{k}$. Если $\boldsymbol{m}-\boldsymbol{k}<0$, то вычисление этого номера производится как $\boldsymbol{m}-\boldsymbol{k}+\mathbf{N}$.

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.

## 2. Порядок выполнения лабораторной работы

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: **Гай Юлий Цезарь:"Пришел, увидел, победил!"**

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 42.

У каждого варианта должно быть свое смещение!

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** = 42).

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**47.

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**47.

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**47.

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**47.

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**47.

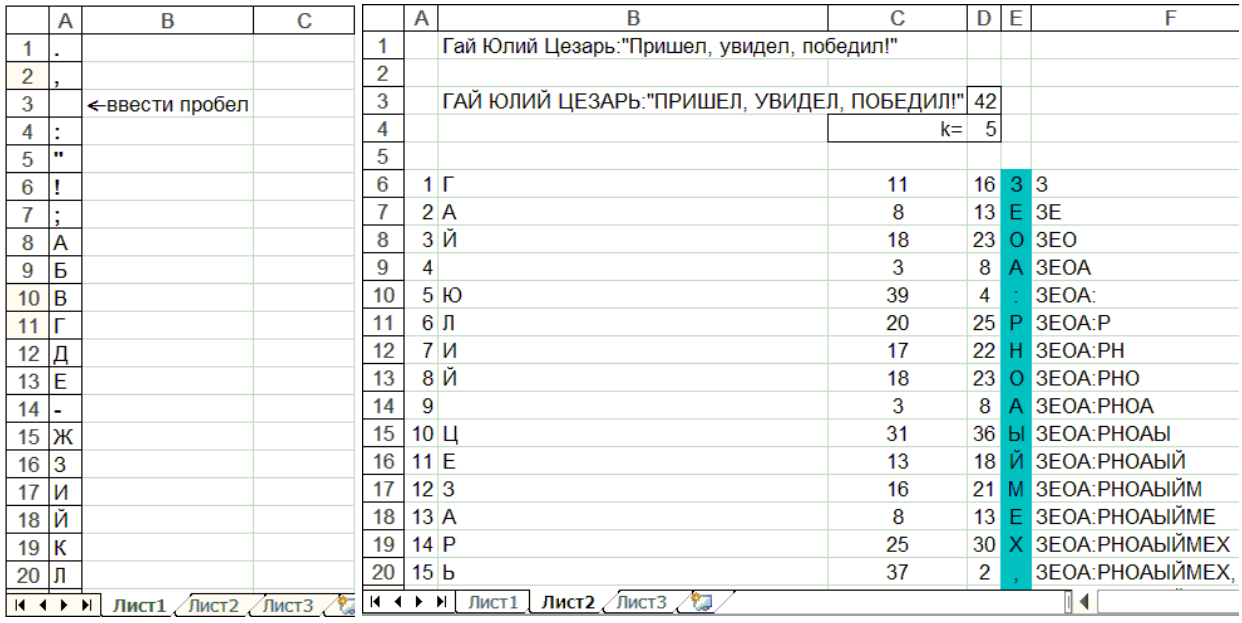
В ячейке **F**47 прочитать зашифрованный текст.

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**47 третьей страницы свидетельствует о корректном выполнении лабораторной работы.



а)

| | A | B | C |
|---|---|---|---|
| 1 | . | | |
| 2 | , | | |
| 3 | | ←ввести пробел | |
| 4 | : | | |
| 5 | " | | |
| 6 | ! | | |
| 7 | ; | | |
| 8 | А | | |
| 9 | Б | | |
| 10 | В | | |
| 11 | Г | | |
| 12 | Д | | |
| 13 | Е | | |
| 14 | - | | |
| 15 | Ж | | |
| 16 | З | | |
| 17 | И | | |
| 18 | Й | | |
| 19 | К | | |
| 20 | Л | | |

Лист1 Лист2 Лист3

б)

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | | Гай Юлий Цезарь:"Пришел, увидел, победил!" | | | | |
| 2 | | | | | | |
| 3 | | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ!" | | 42 | | |
| 4 | | | k= | 5 | | |
| 5 | | | | | | |
| 6 | 1 | Г | 11 | 16 | З | З |
| 7 | 2 | А | 8 | 13 | Е | ЗЕ |
| 8 | 3 | Й | 18 | 23 | О | ЗЕО |
| 9 | 4 | | 3 | 8 | А | ЗЕОА |
| 10 | 5 | Ю | 39 | 4 | : | ЗЕОА: |
| 11 | 6 | Л | 20 | 25 | Р | ЗЕОА:Р |
| 12 | 7 | И | 17 | 22 | Н | ЗЕОА:РН |
| 13 | 8 | Й | 18 | 23 | О | ЗЕОА:РНО |
| 14 | 9 | | 3 | 8 | А | ЗЕОА:РНОА |
| 15 | 10 | Ц | 31 | 36 | Ы | ЗЕОА:РНОАЫ |
| 16 | 11 | Е | 13 | 18 | Й | ЗЕОА:РНОАЫЙ |
| 17 | 12 | З | 16 | 21 | М | ЗЕОА:РНОАЫЙМ |
| 18 | 13 | А | 8 | 13 | Е | ЗЕОА:РНОАЫЙМЕ |
| 19 | 14 | Р | 25 | 30 | Х | ЗЕОА:РНОАЫЙМЕХ |
| 20 | 15 | Ь | 37 | 2 | , | ЗЕОА:РНОАЫЙМЕХ, |

Лист1 Лист2 Лист3

в)

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | | | ЗЕОА:РНОАЫЙМЕХ,БВФХНЭЙР;АШЖНИЙР;АФУ-ЙИНРГВ | | | |
| 2 | | | | | | |
| 3 | | | ЗЕОА:РНО | 42 | | |
| 4 | | | k= | 5 | | |
| 5 | | | | | | |
| 6 | 1 | З | 16 | 11 | Г | Г |
| 7 | 2 | Е | 13 | 8 | А | ГА |
| 8 | 3 | О | 23 | 18 | Й | ГАЙ |
| 9 | 4 | А | 8 | 3 | | ГАЙ |
| 10 | 5 | : | 4 | 39 | Ю | ГАЙ Ю |
| 11 | 6 | Р | 25 | 20 | Л | ГАЙ ЮЛ |
| 12 | 7 | Н | 22 | 17 | И | ГАЙ ЮЛИ |
| 13 | 8 | О | 23 | 18 | Й | ГАЙ ЮЛИЙ |
| 14 | 9 | А | 8 | 3 | | ГАЙ ЮЛИЙ |
| 15 | 10 | Ы | 36 | 31 | Ц | ГАЙ ЮЛИЙ Ц |
| 16 | 11 | Й | 18 | 13 | Е | ГАЙ ЮЛИЙ ЦЕ |
| 17 | 12 | М | 21 | 16 | З | ГАЙ ЮЛИЙ ЦЕЗ |
| 18 | 13 | Е | 13 | 8 | А | ГАЙ ЮЛИЙ ЦЕЗА |
| 19 | 14 | Х | 30 | 25 | Р | ГАЙ ЮЛИЙ ЦЕЗАР |
| 20 | 15 | , | 2 | 37 | Ь | ГАЙ ЮЛИЙ ЦЕЗАРЬ |

Лист1 Лист2 Лист3

г)

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 28 | 23 | Р | 25 | 20 | Л | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ |
| 29 | 24 | ; | 7 | 2 | , | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, |
| 30 | 25 | А | 8 | 3 | | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, |
| 31 | 26 | Ш | 33 | 28 | У | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, У |
| 32 | 27 | Ж | 15 | 10 | В | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВ |
| 33 | 28 | Н | 22 | 17 | И | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИ |
| 34 | 29 | И | 17 | 12 | Д | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИД |
| 35 | 30 | Й | 18 | 13 | Е | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕ |
| 36 | 31 | Р | 25 | 20 | Л | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ |
| 37 | 32 | ; | 7 | 2 | , | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, |
| 38 | 33 | А | 8 | 3 | | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, |
| 39 | 34 | Ф | 29 | 24 | П | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, П |
| 40 | 35 | У | 28 | 23 | О | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПО |
| 41 | 36 | - | 14 | 9 | Б | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБ |
| 42 | 37 | Й | 18 | 13 | Е | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕ |
| 43 | 38 | И | 17 | 12 | Д | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕД |
| 44 | 39 | Н | 22 | 17 | И | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕДИ |
| 45 | 40 | Р | 25 | 20 | Л | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ |
| 46 | 41 | Г | 11 | 6 | ! | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ! |
| 47 | 42 | В | 10 | 5 | " | ГАЙ ЮЛИЙ ЦЕЗАРЬ:"ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ!" |

Лист1 Лист2 Лист3

Рис. 1. Фрагменты документов Excel по лабораторной работе

а) алфавит символов шифра Цезаря; б) начальная часть документа шифрования; в) и г) начальная и конечная часть документа дешифрования

## 3. **Контрольные вопросы**:

1. В чем заключается принцип защиты информации с использованием шифра Цезаря?
2. Объяснить формулы (1) и (2).
3. В чем достоинства и недостатки шифра Цезаря?