ШИФР ЦЕЗАРЯ

Подготовили:
студенты 3 курса
экономического ф-та
группы М112б (ПМ)
Поронник Елена
Жарикова Полина
Петров Николай

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки).

Название шифра

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 $m+k$.

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

Если ***m-k***<0, то вычисление этого номера производится как ***m-k***+**N**.

Достоинством **этой системы является простота шифрования и дешифрования.**

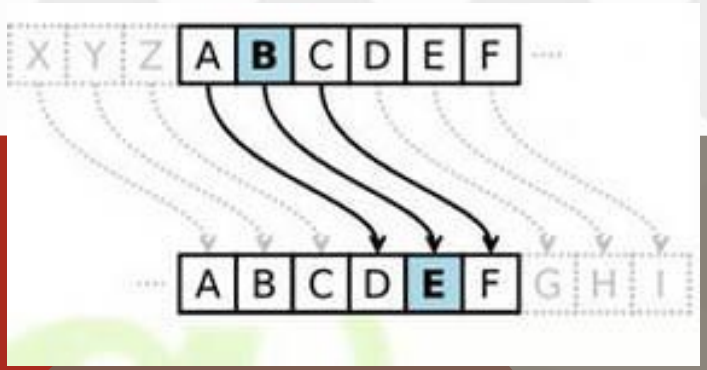
К недостаткам системы Цезаря следует отнести:

- 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

Войти в Excel. Перейти на второй лист. Начиная с ячейки **A**1 до **A**40 набрать алфавит, как показано на рисунке. Выделить весь диапазон алфавита и назначить ему имя “**ABC**”.

На первом листе документа в ячейке **B**1 набрать текст, который необходимо зашифровать, например: **Гай Юлий Цезарь:”Пришел, увидел, победил!”**



. В ячейке **B**3 записать формулу «**=ПРОПИСН(B1)**», функция ПРОПИСН переводит символы в строке в прописные буквы.

В ячейке **D**3 записать формулу «**=ДЛСТР(B3)**», функция ДЛСТР позволяет определить длину строки, что необходимо пользователю, для кодировки исходной строки.

В ячейку **D**4 записать значение **k**, например, 5

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.

В ячейку **B**6, записать формулу “**=ПСТР (B$3;A6;1)**”, которая разделяет кодируемый текст на отдельные символы. Скопировать эту формулу в ячейки **B**7-**B**47.

В ячейку **C**6 записать формулу “**=ПОИСКПОЗ (B6;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

Получив номер символа в алфавите **ABC**, произвести сдвиг нумерации алфавита для кодируемой последовательности символов. В ячейку **D**6 записать формулу: **=ЕСЛИ(ПОИСКПОЗ (B6;ABC;0)+$D$4>40;ПОИСКПОЗ (B6;ABC;0)+$D$4-40;ПОИСКПОЗ (B6;ABC;0)+$D$4)**

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.

Выбрать символы из алфавита **ABC** в соответствии с новыми номерами. В ячейку **E**6 записать формулу “**=ИНДЕКС(ABC;D6)**”. Скопировать содержимое ячейки **E**6 в область **E**7-**E**47

Для получения строки закодированного текста необходимо в ячейку **F**6 записать “=**E**6”, в ячейку **F**7 соответственно – “**=F6&E7**”. Далее скопировать содержимое ячейки **F**7, в область **F**8-**F**47. В ячейке **F**47 прочитать зашифрованный текст.

Для проверки шифрования произвести дешифрование полученного текста и сравнить его с исходным. На третьем листе выполнить дешифрование аналогично пунктам 2-11. При этом необходимо учесть следующие особенности:

- в п. 2 набрать зашифрованный текст;
- в п. 9 в ячейку **D**6 записать формулу:

=ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)-$D$4<0;ПОИСКПОЗ(B6;ABC;0)-$D$4+40;ПОИСКПОЗ(B6;ABC;0)-$D$4).

Получение исходного текста в ячейке **F**47 третьей страницы свидетельствует о корректном выполнении лабораторной работы.

Групп

1 группа	2 группа	3 группа	4 группа	5 группа
Гришина Маргарита	Крылова Анастасия	Коршунова Алена	Тихий Виталий	Сладкова Анна
Прохоренкова Анастасия	Казарян Артур	Маршанкин Георгий	Кузнецова Анна	Григорьева Елена
Музаффарзаде Гюльшан	Федорова Екатерина	Шалаева Елена	Полозков Артем	Музаффарзаде Эльшан
	Фадина Виктория	Фадина Екатерина		