**Шифрование и дешифрование сообщений методами Цезаря и Виженера**

Сутью шифра Цезаря является замена одной буквы другой, находящейся на некоторое постоянное число позиций левее или правее от неё в алфавите.

**Шифр Виженера** представляет собой усовершенствованную многоалфавитную систему шифрования (или, как её ещё называют, полиалфавитная). Идея шифра состоит в использовании в качестве ключа (кодовое слово) текст самого сообщения (открытого - не зашифрованного) или же шифрованного текста (закрытого). Кроме того, для усиления стойкости шифра, в качестве первого символа ключа берется случайным образом буква из алфавита.

Процесс шифрования осуществляется следующим образом:

1. Под каждой буквой шифруемого текста записываются буквы ключа.

Ключ при этом повторяется необходимое число раз.

2. Каждая буква шифруемого текста заменяется по подматрице буквами находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящимися под ними букв ключа.

3. Полученный текст может разбиваться на группы по несколько знаков.

Пусть, например, требуется зашифровать сообщение: максимально допустимой ценой является пятьсот руб. за штуку.

В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

максимально допустимой ценой является пятьсот руб. за штуку

книгакнигак нигакнигак нигак нигакниг акнигак ниг ак нигак

Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (К); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (К),-- в нашем примере такой буквой является Ч; выбранную таким образом букву помещаем в зашифрованный текст. Эта процедура циклически повторяется до зашифрования всего текста.

**Задание. Зашифруйте сообщение, используя шифры Цезаря и Вижинера.**

|  |  |
| --- | --- |
| **Вариант** | **Сообщение** |
| **1** | Буря мглою небо кроет,  Вихри снежные крутя;  То, как зверь, она завоет,  То заплачет, как дитя  *Ключ: Радио* |
| **2** | Если жизнь тебя обманет,  Не печалься, не сердись!  В день уныния смирись:  День веселья, верь, настанет.  *Ключ: Солнце* |
| **3** | Приветствую тебя, пустынный уголок,  Приют спокойствия, трудов и вдохновенья,  Где льется дней моих невидимый поток  На лоне счастья и забвенья.  *Ключ: Море* |
| **4** | Во глубине сибирских руд  Храните гордое терпенье,  Не пропадет ваш скорбный труд  И дум высокое стремленье.  *Ключ: Судья* |
| **5** | В поле чистом серебрится  Снег волнистый и рябой,  Светит месяц, тройка мчится  По дороге столбовой.  *Ключ: Книга* |
| **6** | Великий день Бородина  Мы братской тризной поминая,  Твердили: "Шли же племена,  Бедой России угрожая.  *Ключ: Крот* |
| **7** | **Умом Россию не понять,**  **аршином общим не измерить,**  **у ней особенная стать —**  **В Россию можно только верить.**  ***Ключ: Липа*** |
| **8** | **Нам не дано предугадать,**  **как слово наше отзовётся, —**  **и нам сочувствие даётся,**  **как нам даётся благодать…**  ***Ключ: Ружьё*** |
| **9** | **Роняет лес багряный свой убор,**  **Сребрит мороз увянувшее поле,**  **Проглянет день как будто поневоле**  **И скроется за край окружных гор.**  ***Ключ: Весна*** |
| **10** | Роняет лес багряный свой убор,  Сребрит мороз увянувшее поле,  Проглянет день как будто поневоле  И скроется за край окружных гор.  *Ключ: Лист* |

|  |  |  |
| --- | --- | --- |
| \* | АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ | |
| А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Ъ Э Ю Я | абвгдежзийклмнопрстуфхцчшщьыъэюя бвгдежзийклмнопрстуфхцчшщьыъэюяА вгдежзийклмнопрстуфхцчшщьыъэюяАБ гдежзийклмнопрстуфхцчшщьыъэюяАБВ дежзийклмнопрстуфхцчшщьыъэюяАБВГ ежзийклмнопрстуфхцчшщьыъэюяАБВГД жзийклмнопрстуфхцчшщьыъэюяАБВГДЕ зийклмнопрстуфхцчшщьыъэюяАБВГДЕЖ ийклмнопрстуфхцчшщьыъэюяАБВГДЕЖЗ йклмнопрстуфхцчшщьыъэюяАБВГДЕЖЗИ клмнопрстуфхцчшщьыъэюяАБВГДЕЖЗИЙ лмнопрстуфхцчшщьыъэюяАБВГДЕЖЗИЙК мнопрстуфхцчшщьыъэюяАБВГДЕЖЗИЙКЛ нопрстуфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМ опрстуфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМН прстуфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМНО рстуфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМНОП стуфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМНОПР туфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМНОПРС уфхцчшщьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТ фхцчшщьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУ хцчшщьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФ цчшщьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХ чшщьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦ шщьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ щьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШ ьыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ ыъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬ ъэюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫ эюяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪ юяАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭ яАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮ |  |