Станция шифрования

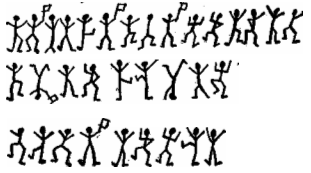
7-8 классов

Коды и шифры — не одно и то же: в коде каждое слово заменяется другим, в то время как в шифре заменяются все символы сообщения.

Простейшие методы шифрования текста

Помните удивительную историю с пляшущими человечками, рассказанную знаменитым сыщиком Шерлоком Холмсом своему другу доктору Ватсону? Мы её пересказывать не будем, а только приведём странные записки, которые преступник посылал своей жертве, а потом напомним конец рассказа.

Вот эти записки:



Пляшущие человечки каждому могут показаться смешными: детские рисунки, глупая забава. А вот Шерлок Холмс, хорошо знакомый с различными видами тайнописи и даже написавший небольшую статью по этому вопросу, сразу определил, что перед ним шифр. Он понял: фигурки означают буквы, и начал искать ключ.

Вскоре ключ был найден, и знаменитый сыщик постепенно вытащил из небытия одну букву за другой.

Это позволило ему не только прочитать записки, но и самому послать преступнику строчку пляшущих человечков, и... преступник попал в руки правосудия. Пляшущие фигурки означали слова: «Приходите сюда сейчас».

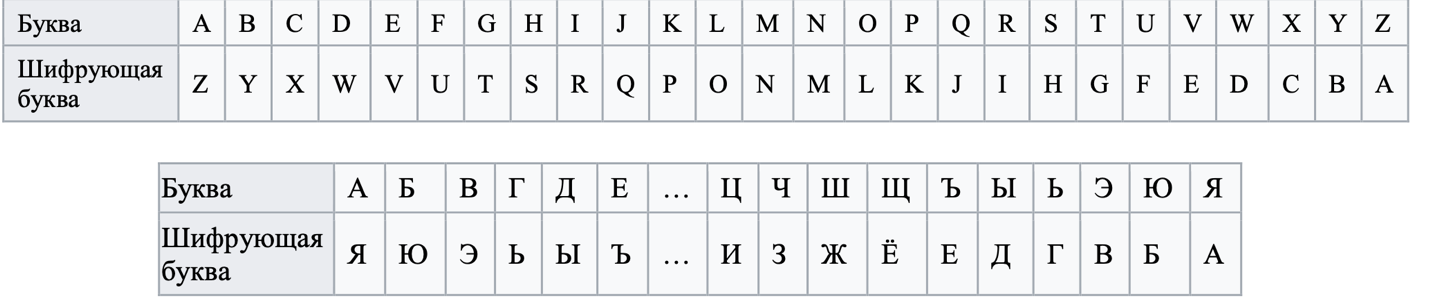
Существует много разных систем шифрования. К ним прибегают в военном деле, на дипломатической службе, вообще в тех случаях, когда нужно сохранить в тайне содержание переписки. Шифрование текста используется человечеством с того самого момента, как появилась первая секретная информация, то есть такая, которая должна быть недоступна тем, кому она не предназначена1.

Опишем несколько простейших методов шифрования текста.

page1image3191289728

Шифр «атбаш»

«Атба́ш» – один из самых древних методов шифрования. Шифрование заключается в замене каждой буквы исходного текста на «симметричную» ей букву алфавита, то есть первая алфавита заменялась на последнюю и наоборот, вторая буква – на предпоследнюю и наоборот и т.д. Ниже даны примеры для латинского и русского алфавитов.



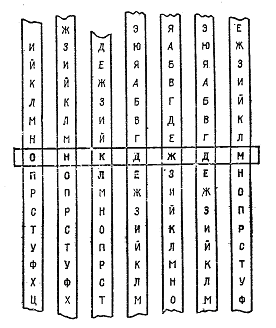
Шифр «атбаш» был, скорее всего, изобретен ессеями, иудейской сектой повстанцев. Они разработали множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования [2].

Происхождение названия шифра объясняется используемым принципом замены букв. Еврейское слово, звучащее как «атбаш», אשבת, составлено из букв (справа налево) «алеф», «тав», «бет» и «шин», то есть первой, последней, второй и предпоследней букв еврейского алфавита.

Шифр Цезаря

Метод шифрования назван носит имя римского императора Юлия Цезаря (I век до н. э.), который если и не сам изобрел его, то активно им пользовался. Этот метод основан на замене каждой буквы шифруемого текста на другую путем смещения в алфавите от исходной буквы на фиксированное количество символов, причем алфавит читается по кругу, то есть после буквы я рассматривается а. Регистр символов не учитывается. Так, например, слово БАЙТ при смещении на два символа вправо кодируется словом ГВЛФ.

Оказывается, что имеется простой способ расшифровки текста, зашифрованного шифром Цезаря, даже если направление и величина сдвига букв в алфавите неизвестны — так называемый «метод полосок». Берутся несколько полосок из бумаги, картона и т.п. и на каждую из них наносятся по порядку все буквы алфавита (см. рисунок на следующей странице).

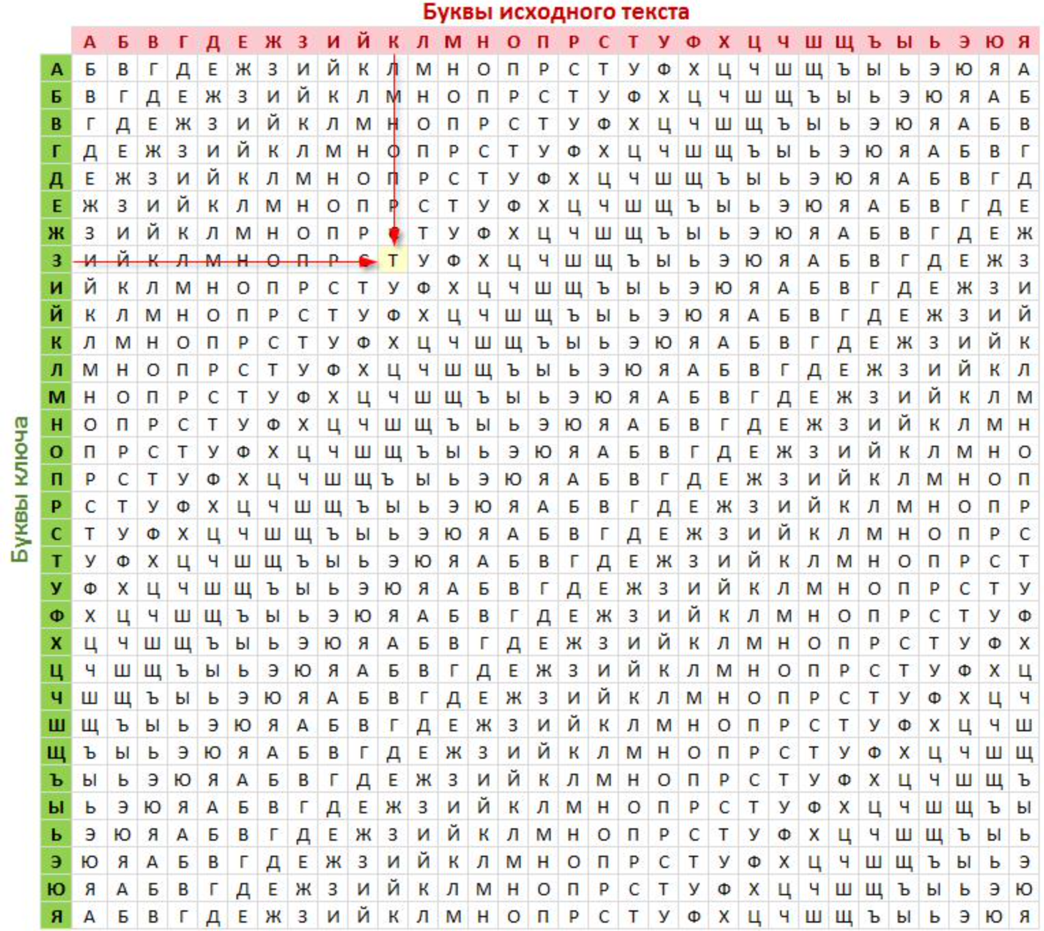


В криптограмме (зашифрованном тексте) берется некоторое слово, например, онкдждм. Полоски прикладываются друг к другу так, чтобы образовать данное слово (см. рисуно). Двигаясь вдоль полосок, находим среди строк единственное осмысленное сочетание полезен, которое и служит расшифровкой данного слова. Одновременно можно найти величину сдвига.

Шифр Виженера

Шифр Виженера использует тот же принцип, что и шифр Цезаря, за тем исключением, что каждая буква меняется в соответствии с кодовым словом.

Данный шифр на порядок более устойчив к взлому, чем моноалфавитные, хотя представляет собой шифр простой замены текста.Пример:

  
Давайте зашифруем слово «Пароль» с помощью данного шифра. Ключевое слово будем использовать «Код». Нарисуем таблицу:



Берем первые буквы ключа и нашего слова и скрещиваем между собой с помощью таблицы Виженера и получается буква «ъ» и идем далее. Остальное попробуйте самостоятельно и напишите ответ в комментариях

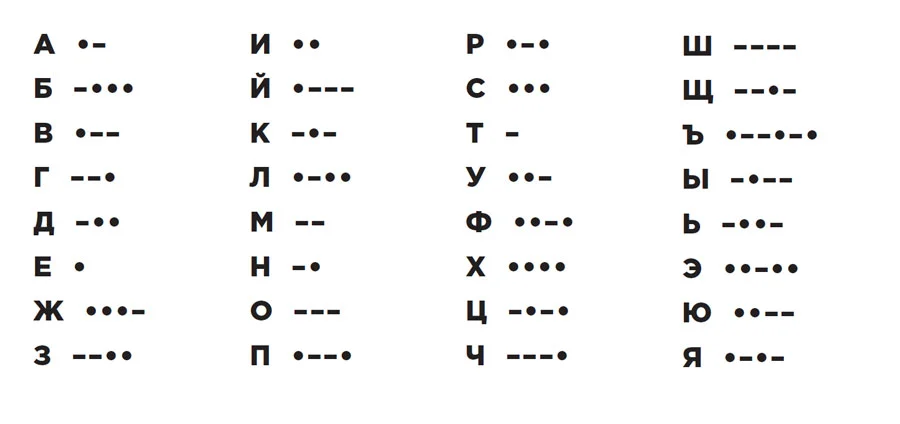
ROT1

Этот шифр известен многим детям. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, А заменяется на Б, Б — на В, и т. д. Фраза «Уйрйшоьк Рспдсбннйту» — это «Типичный Программист».

Попробуйте расшифровать сообщение:

Лбл еёмб, рспдсбннйту?

Азбука Морзе

В азбуке Морзе каждая буква алфавита, цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов:  
Чаще всего это шифрование передаётся световыми или звуковыми сигналами.

Сможете расшифровать сообщение, используя картинку?

•−− −•− −−− −• −•−• • ••• − •− − −••− •• • ••• − −••− −•• • −−−− •• ••−• •−• •− − −−− •−• −•−−

Моноалфавитная замена

Коды и шифры также делятся на подгруппы. Например, ROT1, азбука Морзе, шифр Цезаря относятся к моноалфавитной замене: каждая буква заменяется на одну и только одну букву или символ. Такие шифры очень легко расшифровываются с помощью частотного анализа.

Например, наиболее часто встречающаяся буква в английском алфавите — «E». Таким образом, в тексте, зашифрованном моноалфавитным шрифтом, наиболее часто встречающейся буквой будет буква, соответствующая «E». Вторая наиболее часто встречающаяся буква — это «T», а третья — «А».

Однако этот принцип работает только для длинных сообщений. Короткие просто не содержат в себе достаточно слов.

Шифр Энигмы

Энигма — это машина, которая использовалась нацистами во времена Второй Мировой для шифрования сообщений.

Есть несколько колёс и клавиатура. На экране оператору показывалась буква, которой шифровалась соответствующая буква на клавиатуре. То, какой будет зашифрованная буква, зависело от начальной конфигурации колес.

Существовало более ста триллионов возможных комбинаций колёс, и со временем набора текста колеса сдвигались сами, так что шифр менялся на протяжении всего сообщения.

Шифр A1Z26

Это простая подстановка, где каждая буква заменена её порядковым номером в алфавите. Только нижний регистр.

Попробуйте определить, что здесь написано:

15-6-2-16-13-30-26-16-11 17-18-10-14-6-18