**Шифр Цезаря**

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря – один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря – это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3 «А» была бы заменена на «Г», «Б» станет «Д» и так далее.

Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами. Сейчас шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

При этом если результат сложения (сдвига) будет превышать мощность алфавита, то результатом станет остаток от деления суммы на мощность алфавита.

Пример.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |  |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |  |

Необходимо зашифровать символ «Ч». Сдвиг равен 12. Тогда 25 + 12 = 37. И остаток от деления 37 на 33 будет равен 4. Это и есть номер зашифрованного символа.

Эти вычисления можно сделать с помощью арифмометра, воспользовавшись операциями «сложение», «вычитание» или «деление».

**Шифр Виженера**

Простота шифра Цезаря, частотный анализ и другие методы дедукции привели к тому, что сдвиг кода каждого символа не может быть одинаковым. Сдвиг должен задаваться какой-то последовательностью, быть разным. Например, первый символ будет «сдвинут» на 3, второй – на 7, третий – на 13 и так далее. Тогда его будет гораздо труднее взломать. Ключом может быть какая-то последовательность или слово.

Пример.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |  |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |  |

Исходное сообщение: «документ».

Ключ: «печать».

Наложение:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Исх.:** | **Д** | **О** | **К** | **У** | **М** | **Е** | **Н** | **Т** |
| Коды: | 5 | 16 | 12 | 21 | 14 | 6 | 15 | 20 |
| **Ключ:** | **П** | **Е** | **Ч** | **А** | **Т** | **Ь** | **П** | **Е** |
| Коды: | 17 | 6 | 25 | 1 | 20 | 30 | 17 | 6 |
| Сумма: | 22 | 22 | 37 => 4 | 22 | 34 => 1 | 36 => 3 | 32 | 26 |
| **Шифр** | **Ф** | **Ф** | **Г** | **Ф** | **А** | **В** | **Ю** | **Ш** |

**ФФГФАВЮШ**

Обратите внимание, символами «Ф» зашифрованы разные буквы: «Д», «О» и «У».

Если длина ключа превышает длину шифруемого текста, ключ является истинно случайным и не используется для шифрования других сообщений, то такое преобразование является абсолютно стойким. Шифр является совершенным. И его невозможно взломать.

**Шифр Вернама**

Вернам предложил, чтобы символы текста и ключа представлялись в двоичных кодах, а затем каждая пара двоичных разрядов складывалась (для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»).

Пример.

Результатом выражения «1010 ⊕ 1011» будет «0001».

В таблице ниже представим коды символов в кодировке Windows-1251 и их двоичное представление (Dec-код – десятичный код символа, Bin-код – двоичный код символа):

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Буква** | **Dec-код** | **Bin-код** | **Буква** | **Dec-код** | **Bin-код** | **Буква** | **Dec-код** | **Bin-код** |
| **А** | 192 | 1100 0000 | **Л** | 203 | 1100 1011 | **Ц** | 214 | 1101 0110 |
| **Б** | 193 | 1100 0001 | **М** | 204 | 1100 1100 | **Ч** | 215 | 1101 0111 |
| **В** | 194 | 1100 0010 | **Н** | 205 | 1100 1101 | **Ш** | 216 | 1101 1000 |
| **Г** | 195 | 1100 0011 | **О** | 206 | 1100 1110 | **Щ** | 217 | 1101 1001 |
| **Д** | 196 | 1100 0100 | **П** | 207 | 1100 1111 | **Ъ** | 218 | 1101 1010 |
| **Е** | 197 | 1100 0101 | **Р** | 208 | 1101 0000 | **Ы** | 219 | 1101 1011 |
| **Ж** | 198 | 1100 0110 | **С** | 209 | 1101 0001 | **Ь** | 220 | 1101 1100 |
| **З** | 199 | 1100 0111 | **Т** | 210 | 1101 0010 | **Э** | 221 | 1101 1101 |
| **И** | 200 | 1100 1000 | **У** | 211 | 1101 0011 | **Ю** | 222 | 1101 1110 |
| **Й** | 201 | 1100 1001 | **Ф** | 212 | 1101 0100 | **Я** | 223 | 1101 1111 |
| **К** | 202 | 1100 1010 | **Х** | 213 | 1101 0101 |  |  |  |

Пример шифрования сообщения «путь» с помощью ключа «дуб» показан в следующей таблице.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Открытое сообщение | Буква | П | У | Т | Ь |
| Dec-код | 207 | 211 | 210 | 220 |
| Bin-код | 1100 1111 | 1101 0011 | 1101 0010 | 1101 1100 |
| Ключ | Буква | Д | У | Б | Д |
| Dec-код | 196 | 211 | 193 | 196 |
| Bin-код | 1100 0100 | 1101 0011 | 1100 0001 | 1100 0100 |
| Шифрограмма | Dec-код | **11** | **0** | **19** | **24** |
| Bin-код | 0000 1011 | 0000 0000 | 0001 0011 | 00011000 |

Данный шифр обладает прекрасным свойством. В случае наложения «ложного» ключа на зашифрованное сообщение можно получить осмысленное выражение, но не имеющее с исходным ничего общего.

**Телеграф и азбука Морзе**

Один из первых пишущих телеграфов был произведен Борисом Семеновичем Якоби, академиком Петербургской Академии наук. Прибор Якоби был установлен в 1841 году на подземной телеграфной линии в Петербурге и соединял кабинет императора Николая I в Зимнем дворце с Главным штабом. В 1842 году была проложена линия от Зимнего дворца до главного управления путей сообщения, в 1843 – до дворца в Царском Селе.

Свое изобретение Якоби усовершенствовал в 1850 году, создав первый в мире буквопечатающий телеграфный аппарат.

Конструкция другого телеграфа – телеграфа Морзе – была устроена следующим образом. Главные части приемника – это вертикальный электромагнит, рычаг (для замыкания цепи) и бумажная лента, на которой с помощью специального механизма наносятся условные знаки. Электромагнит при пропускании через него тока притягивает к себе железный стерженек, находящийся на конце рычага; другое плечо рычага при этом поднимается и придавливает стальное острие на его конце к бумажной ленте, которая все время продвигается вперед. Когда ток прерывается, рычаг оттягивается пружиной в прежнее положение. В зависимости от продолжительности тока на ленте острие рычага оставляет следы в виде или точек, или чёрточек. Различные комбинации этих знаков и составляют условный алфавит.

Такие знаки (черточки и точки) могут быть произведены посредством нажатия на бумагу рычажного штифта, который будет оставлять на ней следы в виде углублений; так это и было устроено в первоначальных приборах системы Морзе. Но рельефно пишущие приборы неудобны в том отношении, что требуют довольно значительной силы тока. Поэтому вместо штифта стали применять небольшое колесо, которое нижней частью погружается в сосуд с густыми чернилами. При действии прибора оно постепенно поворачивается и оставляет на бумажной ленте след краски.

В дальнейшем были изобретены приборы, которые преобразовывали набор слов на клавиатуре в код Морзе, который передавался по каналам связи. Такой прибор позволял отправителю не знать азбуку Морзе. Или же сохранить «почерк» отправителя в секрете. «Почерк» в данном случае – это уникальная особенность отправителя делать паузы определенной длины.