Государственное учреждение образования «Гимназия №1 г. Бреста»

**Взлом шифра Цезаря**

**Выполнил:**

Соболь Владислав Владимирович, ученик 8 класса

**Руководитель:**

Терещук Виктор Александрович, учитель информатики

Брест, 2011 г.

Люди всегда нуждались в способе шифрования информации для безопасной ее передачи. Согласно легенде, самый древний способ тайнописи был такой: обривали голову раба, писали на коже головы нужное послание, ждали пока вырастут волосы и слали к адресату. Расшифровка походила на зашифровку: обривали раба и читали послание.

Также известно, что Юлий Цезарь был, якобы, первым, кто придумал настоящий шифр. Алфавит размещали на круге так, что после Я идет А, далее Б, В, Г и т.д. Для зашифровки буквы текста заменяются на буквы, стоящие дальше по кругу на заданное число. Оно и являлось ключом. То есть при ключе 3 в зашифрованном сообщении вместо n-ой буквы алфавита использовали (n+3)-юю, вместо А в таком шифре будет Г, вместо И будет стоять Л.

Помимо потребности в шифровании люди нуждались и во взломе шифрованных сообщений. Например, это очень важно во время военных действий, чтобы узнать о действиях противника. Также взлом может потребоваться, если был забыт пароль, например от архива.

Взлом – это расшифровка сообщения без знания ключа.

Шифр Цезаря не настолько надежен, как кажется. Способ взлома основывается на знании частоты вхождения букв алфавита в текст. Каждая буква языка входит в текст с разной частотой. Например, буква О входит в текст на русском языке часто, по сравнению с буквой Ъ.

Чтобы узнать текст сообщения, зашифрованного способом Цезаря нужно сначала расшифровать текст со всеми возможными ключами, затем из полученных вариантов выбрать оптимальный. Лучшим вариантом будет тот, в котором разница оригинальной встречаемости букв и частотой вхождения букв в полученном тексте минимальна. Эта разность рассчитывается по следующей формуле:

Где n – количество букв в тексте, – оригинальная частота вхождения буквы в текст на русском языке, – полученная частота вхождения буквы в текст.

Данный метод можно применять не только для взлома шифра Цезаря, но и для взлома других шифров, основанных на подстановке (в которых одна буква заменяет другую по какому-то правилу).