

Шифр Цезаря — это вид шифра замены, в котором каждая буква заменяется буквой, находящейся на некотором числе позиций правее неё в алфавите. Например, в шифре со сдвигом на 3, А была бы заменена на Г, Б станет Д, и так далее. Алфавит считается записанным по кругу: так, в приведённом примере буква Ю переходит в Б. Число, на которое мы сдвигаем, называется **ключом шифра**.

Шифр Виженера — усовершенствованный вариант шифра Цезаря. У нас есть ключевое слово, например, БАНК (**ключ шифра**). Мы заменяем каждую его букву на её номер в алфавите: 2 1 15 12. Затем к буквам слова, которое хотим зашифровать, прибавляем по очереди числа ключевой последовательности (если числа закончились, начинаем заново). Например, если мы хотим зашифровать слово ГВАРДИЯ, то получим: $Г + 2 = Е$, $В + 1 = Г$, $А + 15 = О$, $Р + 12 = Ъ$, $Д + 2 = Ё$, $И + 1 = Й$, $Я + 15 = Н$. Получили ЕГОБЁЙН.

- Используя шифр Цезаря с ключом 1, расшифруйте:
ДБК ЯМЙК ЧЁИВСЭ — ЮУП ОЁ ТБМБУ!
- Как начинаются «Записки о Галльской войне» Гая Юлия Цезаря?
ЯОБ АЭИИЁБ НЭЕВВИВКЭ КЭ ПНЁ ФЭОПЁ.
- Зашифруйте шифром Виженера с ключом «ШИФР» слово «АНАНАС».
- Слово ЗЁВЭОЖЭ получено с помощью шифра Виженера с ключевым словом ЧАЙ. Восстановите исходное слово.
- Расшифруйте следующее сообщение, зашифрованное шифром Виженера.
Фбхй д пудянэрб ёачэ труй ряннйшщн! (ключ: панда)
- Внимание! В этой задаче в алфавите нет букв ё, й, ъ! Сообщение (из нескольких слов) зашифровано шифром Виженера. Известно, что ключевая последовательность букв не содержала никаких букв, кроме А, Б и В. Прочтите шифрованное сообщение: РБЪНПТСИТСРРЕЗОХ.

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