Урок 1. Шифр Цезаря

Криптография · ~35 минут

Больше двух тысяч лет назад Юлий Цезарь не хотел, чтобы враги читали его письма. Он придумал простую хитрость: сдвигать каждую букву на несколько позиций вперёд по алфавиту. Сегодня этот шифр взламывается за секунды, но именно с него удобнее всего начать путь криптографа.

🎯 Что ты узнаешь

- Как зашифровать и расшифровать текст сдвигом по алфавиту.
- Что такое ключ шифра и сколько ключей у Цезаря.
- Как взломать шифр полным перебором.
- Как взломать его умнее — частотным анализом.

📖 Разбираемся в теме

Алфавит и номера букв

Работаем с **русским алфавитом из 33 букв** (Е и Ё считаем разными). Пронумеруем буквы с нуля:

```
А=0  Б=1  В=2  Г=3  Д=4  Е=5  Ё=6  Ж=7  З=8  И=9  Й=10 К=11
Л=12 М=13 Н=14 О=15 П=16 Р=17 С=18 Т=19 У=20 Ф=21 Х=22 Ц=23
Ч=24 Ш=25 Щ=26 Ъ=27 Ы=28 Ь=29 Э=30 Ю=31 Я=32
```

Шифрование

Ключ — это число сдвига **k**. Чтобы зашифровать букву, берём её номер, прибавляем **k**, и если вышли за 32 — «заворачиваемся» обратно в начало алфавита. Математически это остаток от деления на 33:

$$\text{номер шифробуквы} = (\text{номер буквы} + k) \bmod 33$$

📌 **Запомни:** запись $a \bmod 33$ означает остаток от деления a на 33. Например, $35 \bmod 33 = 2$, потому что $35 = 33 + 2$.

Зашифруем слово **ЗАЯЦ** с ключом **k = 3**:

Буква	Номер	+3	mod 33	Шифробуква
З	8	11	11	К
А	0	3	3	Г
Я	32	35	2	В
Ц	23	26	26	Щ

Получилось: **ЗАЯЦ** → **КГВЩ**.

Дешифрование

Чтобы расшифровать, делаем обратное — **вычитаем** k (и если ушли ниже нуля, прибавляем 33):

$$\text{номер буквы} = (\text{номер шифробуквы} - k) \bmod 33$$

Проверим КГВЩ с k = 3: К(11)−3=8=З, Г(3)−3=0=А, В(2)−3=−1, а −1+33=32=Я, Щ(26)−3=23=Ц. Снова **ЗАЯЦ**. Отлично, шифрование и дешифрование согласованы. ✅

💡 Сдвиг «назад на k» — это то же самое, что «вперёд на 33−k». Расшифровать ключом 3 = зашифровать ключом 30.

Сколько всего ключей?

Сдвиг может быть от 1 до 32 (сдвиг 0 и 33 ничего не меняют). Значит, осмысленных ключей всего **32**.

⚠️ Это катастрофически мало! Компьютер (да и человек с бумажкой) переберёт все 32 варианта за минуту. Поэтому шифр Цезаря нельзя

использовать всерьёз.

Взлом №1: полный перебор

Если ты не знаешь ключ, просто попробуй все 32 сдвига и посмотри, при каком получается осмысленный текст. Этот метод называется **атака полным перебором** (или «грубой силой», brute force).

Взлом №2: частотный анализ

А что если текст длинный, и перебирать лень? Тут помогает статистика языка. В русском тексте буквы встречаются неравномерно: чаще всего **О**, затем **Е, А, И, Н, Т**. Самая частая буква в шифровке почти наверняка соответствует **О**.

🤔 **А знаешь ли ты?** В русском языке буква **О** занимает около 11% всех букв, а вот **Ф** — меньше 0,1%. Именно на таких перекосах держится частотный анализ, который сломал не один исторический шифр.

Идея взлома: находим самую частую букву шифровки, считаем, на сколько её надо сдвинуть назад, чтобы получить О — это и есть ключ.

✍️ Разбор примера

Задача: расшифруй ПХНФЧУ, зная, что использовался шифр Цезаря с ключом k = 5.

Вычитаем 5 из каждого номера (и при необходимости +33):

Шифробуква	Номер	–5	mod 33	Буква
П	16	11	11	К
Х	22	17	17	Р
Н	14	9	9	И
Ф	21	16	16	П

Шифробуква	Номер	−5	mod 33	Буква
Ч	24	19	19	Т
У	20	15	15	О

Ответ: **КРИПТО**. Проверим обратно: К(11)+5=16=П, Р(17)+5=22=Х, И(9)+5=14=Н… всё сходится. ✅

📝 Задачи

1. Зашифруй слово **МИР** ключом **k = 7**.
2. Зашифруй слово **ПОБЕДА** ключом **k = 10**.
3. Расшифруй **УПЧ** (шифр Цезаря, ключ 7).
4. Расшифруй **ЫМХПТ** (шифр Цезаря, ключ 4).
5. Тебе попалась шифровка **РУЗНПЕ**. Ты знаешь только, что ключ где-то от 3 до 7. Найди осмысленное слово (подсказка: перебери эти 5 ключей).
6. В длинной перехваченной шифровке самая частая буква — **Ц**. Каким, скорее всего, был ключ? (Считай, что ей соответствует буква О.)
7. Сколько существует различных осмысленных ключей у шифра Цезаря для русского алфавита? А для английского (26 букв)?
8. *Со звёздочкой.* Костя зашифровал слово ключом k, а его сестра случайно зашифровала уже готовую шифровку ещё раз ключом m. Каким одним ключом можно расшифровать результат сразу?