Урок 2. Шифр Виженера

Криптография · ~35 минут

Слабость Цезаря в том, что все буквы сдвигаются одинаково. А что если сдвигать каждую букву по-своему? Именно это придумали в XVI веке. Три столетия шифр Виженера считали невзламываемым и звали его «le chiffre indéchiffrable» — «нерасшифровываемый шифр».

🎯 Что ты узнаешь

- Что такое ключевое слово и как оно задаёт разные сдвиги.
- Как шифровать и дешифровать по Виженеру.
- Почему частотный анализ здесь спотыкается.
- С чего начинается взлом: как ищут длину ключа.

📖 Разбираемся в теме

Снова **русский алфавит, 33 буквы**, нумерация как в уроке 1 (А=0, …, Я=32).

Идея: ключ-слово

Вместо одного числа-сдвига берём **ключевое слово**, например **КОД**. Его буквы задают сдвиги:

- К = 11
- О = 15
- Д = 4

Первую букву текста сдвигаем на 11, вторую на 15, третью на 4, четвёртую снова на 11, пятую на 15 — и так по кругу. Получается, что мы применяем сразу **несколько шифров Цезаря**, чередуя их. Поэтому Виженер — это **многоалфавитный** шифр.

📌 **Запомни:** формула та же, что у Цезаря, только сдвиг у каждой буквы свой: $$C_i = (T_i + K_i) \bmod 33,$$ где T_i — номер i-й буквы текста, K_i — номер соответствующей буквы ключа.

Шифрование пошагово

Зашифруем **ШИФР** ключом **КОД**. Ключ короче текста, поэтому повторяем его: К-О-Д-К.

i	Буква текста	T_i	Буква ключа	K_i	T_i+K_i	mod 33	Шифробуква
1	Ш	25	К	11	36	3	Г
2	И	9	О	15	24	24	Ч
3	Ф	21	Д	4	25	25	Ш
4	Р	17	К	11	28	28	Ы

Получаем: **ШИФР** → **ГЧШЫ**.

Дешифрование

Вычитаем сдвиги ключа: $T_i = (C_i - K_i) \bmod 33$.

Проверим ГЧШЫ ключом КОД: Г(3)−11=−8, −8+33=25=Ш; Ч(24)−15=9=И; Ш(25)−4=21=Ф; Ы(28)−11=17=Р. Снова **ШИФР**. ✅

Почему частотный анализ не проходит

Посмотри внимательно на слово **ШИФР** → **ГЧШЫ**. Взгляни ещё раз: в исходном слове все буквы разные, но важнее другое. Возьмём слово, где буква повторяется. Одна и та же буква текста, стоящая на разных позициях, шифруется **по-разному**, потому что попадает под разные буквы ключа. И наоборот, одинаковые буквы в шифровке могут происходить из совсем разных букв текста.

Из-за этого частота букв в шифровке **выравнивается** — «горб» на букве О размазывается. Простой частотный анализ, который ломал Цезаря, здесь

бессилен.

> 🤔 **А знаешь ли ты?** Шифр назвали в честь француза Блеза де Виженера, хотя похожую идею раньше описал Джованни Баттиста Белласо. В истории криптографии так бывает часто — имя достаётся не тому, кто придумал первым.

Как всё-таки его ломают: длина ключа

Ключ длины **L** превращает Виженер в **L независимых шифров Цезаря**: буквы на позициях 1, L+1, 2L+1, … шифруются одним и тем же сдвигом; буквы на позициях 2, L+2, … — другим, и так далее.

Значит, если бы мы знали L, то могли бы разбить шифровку на L «стопок» и взломать каждую стопку обычным частотным анализом Цезаря!

Как узнать L? Ищут **повторяющиеся куски** в шифровке. Если одинаковый фрагмент текста зашифровался одинаково, значит между этими местами уложилось целое число длин ключа. Расстояния между повторами кратны L — из их общего делителя угадывают длину ключа (это метод Касиски).

> 💡 Вывод: чем **длиннее** ключевое слово по сравнению с текстом, тем труднее взлом. А если ключ такой же длины, как текст, и случайный — шифр становится абсолютно невзламываемым (это «одноразовый блокнот», о нём ты ещё услышишь).

✍️ Разбор примера

Задача: расшифруй ГЧШЫ, ключ КОД. (Разберём чуть подробнее, чем выше.)

Повторяем ключ под шифровкой: К(11) О(15) Д(4) К(11). Вычитаем:

- Г = 3, 3 – 11 = –8 → +33 = 25 → **Ш**
- Ч = 24, 24 – 15 = 9 → **И**

- Ш = 25, 25 − 4 = 21 → **Ф**
- Ы = 28, 28 − 11 = 17 → **Р**

Получилось **ШИФР**. Обратная проверка совпала выше — значит, всё верно. ✅

📝 Задачи

1. Зашифруй слово **ГОРА** ключом **РЕКА**.
2. Зашифруй слово **ТАЙНА** ключом **ШИФР**.
3. Расшифруй **ЧОЦПЫДЭЧОК**, ключ **КОД**.
4. Зашифруй слово **МАМА** ключом **ВОД**. Убедись, что две одинаковые буквы М превратились в разные шифробуквы, и объясни, почему так вышло.
5. Шифровку длиной 40 букв зашифровали ключом из 5 букв. На сколько шифров Цезаря она распадается и сколько букв попадёт в каждую «стопку»?
6. В перехваченном тексте одинаковый трёхбуквенный фрагмент встретился дважды, а расстояние между началами повторов равно 12 букв. Каким может быть длина ключа? Перечисли варианты (делители 12, кроме 1).
7. Объясни своими словами, почему у Цезаря частотный анализ работает сразу, а у Виженера — только после того, как найдена длина ключа.
8. *Со звёздочкой.* Если взять ключ длины 1, в какой знакомый шифр превратится Виженер?