kaspersky.academy

Лекция 1

Шифр Цезаря

Онлайн-курс по математике в информационной безопасности

Лекция 1. Шифр Цезаря

Привет!

В этой лекции мы должны понять на практике, что такое открытый текст и шифртекст, ключ шифрования. Мы рассмотрим реальный исторический шифр – шифр Цезаря, а также научимся его дешифровать.

Наш план на эту лекцию:

Как шифровал Цезарь?

Цезарь использовал свой собственный шифр для военных переписок. Это пример исторического шифра – в наше время он не используется из-за его простоты.

Шифр состоит в том, **чтобы сдвинуть все символы алфавита на несколько позиций вперед,** – это называется **шаг сдвига, или ключ.** Например, если шаг сдвига $k = 1$, каждая буква исходного алфавита сдвигается вперед на один шаг. То есть,

$$А \rightarrow Б, Б \rightarrow В, ..., Я \rightarrow А$$

Шифр Цезаря – это шифр подстановки: вместо символов исходного алфавита подставляются символы алфавита замены.

Давайте расположим все буквы русского алфавита на окружности и зашифруем слово ЦЕЗАРЬ. ЦЕЗАРЬ – это открытый текст. Так как ключ $k = 1$, будем сдвигать буквы на один шаг по часовой стрелке.

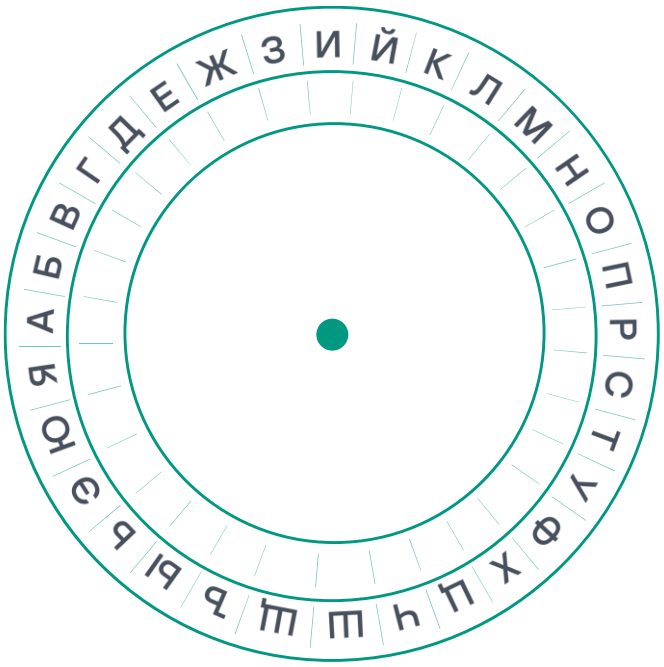

Рисунок 1:
Русский алфавит

Русский алфавит:
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Мы выбросим букву Ё – за "Ё" немного обидно, но мы жертвуем ею ради ясности. Строго необходимо, чтобы у всех участников переписки был одинаковый алфавит, иначе сдвиги букв не будут совпадать.

На 1-м месте открытого текста стоит буква Ц. Идём по окружности на 1 шаг вправо и получаем букву Ч – это будет 1-я буква шифртекста. Еще раз повторяем это действие. Е переходит в Ж, З → И, А → Б, Р → С, Ь → Э.

Получается, что шифртекст – это ЧЖИБСЭ.

Классическим шифром Цезаря считается шифр, в котором **ключ сдвига равен 3 (*k* = 3).**

Попробуем зашифровать теперь открытый текст, используя сдвиг на 3. Возвращаемся к окружности, смотрим на букву А и делаем 3 шага вперед:

Ц → Ч → Ш → Щ

И буква Ц переходит в букву Щ. Так же поступим и с другими буквами:
Е → И, З → К, А → У, Р → У, Ь → Я

ЦЕЗАРЬ→ ЩИКГУЯ

Шифр Цезаря на языке математики

Составляем математическую модель шифра Цезаря. Пронумеруем буквы алфавита начиная с 0.

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Пусть *x* – номер символа открытого текста, *y* – номер символа шифртекста, *k* – ключ, *n* – мощность множества букв алфавита. В русском языке 32 буквы, так что *n* = 32.

Тогда получать символ шифртекста будем с помощью такой формулы:

$$y = (x+k) \bmod n$$

А чтобы расшифровать:

$$x = (y-k) \bmod n$$

Мы используем mod n, чтобы не выйти за пределы алфавита.

Шифрование текста

Еще раз зашифруем слово ЦЕЗАРЬ с ключом = 3. Ц стоит под номером 22. Используем формулу:

22	23	24	25
Ц	Ч	Ш	Щ

$$x = (22+3) \bmod 32 = 25$$

Найдем букву с номером 25 в таблице. Это буква Щ. То есть, Ц →Щ. Пример не новый, поэтому остальную часть текста вы знаете.

Дешифрование текста

Чтобы расшифровать шифртекст, будем шагать по окружности против часовой стрелки. Пусть ключ = 3, а зашифрованное слово – ЩИКГУЯ.

От буквы Щ делаем 3 шага влево и получаем букву Ц.

И → Е, К → З, Г → А, У → Р, Я → Ь

Вот и наше тайное слово – ЦЕЗАРЬ.

А теперь используем формулу для расшифровки. Для буквы Щ:

$$x = (25-3) \bmod 32 = 22$$

Тогда Щ→Ц.

Аналогично расшифровываем остальные буквы.

Если же при расшифровке ключ больше, чем номер буквы, вспомните о том, как переходить от отрицательных чисел по модулю к положительным (или отправляйтесь прямо в модуль «Арифметика»). Например:

$k = 18$,
шифртекст = ВЪЮ

Найдем первую букву.

$$x_1 = (2-18) \bmod 32 = -16 \bmod 32 = 32-16 = 16$$

В → Р

Находим вторую букву: Ъ → И

Последняя буква: Ю → М

И мы понимаем, что открытый текст – это слово РИМ!

Криптоанализ шифра Цезаря

Мы будем анализировать шифр Цезаря и постараемся его дешифровать. Алгоритм работы этого шифра нам известен: алфавит замены мы получаем сдвигом на длину ключа. А что будет, если сдвинуть русский алфавит на 32 позиции вперед? Да ничего не произойдет. Вообще ничего. **Сдвиг на 32 позиции – то же самое, что и нулевой сдвиг:** буква «А» вернется в букву «А», «Б» в «Б» и так далее. Это значит, что, если перебрать все возможные сдвиги алфавита (а разных таких сдвигов всего 31), мы когда-нибудь найдем верный ключ. Мы применим **брутфорс-атаку** – то есть будем перебирать все варианты ключа. **Критерий остановки:** заканчиваем перебирать в тот момент, когда из нечитаемого шифртекста появится осмысленный текст. Давайте уже ~~ломать~~расшифровывать!

Наш зашифрованный текст:

ТЛП
ДЗЩПЭЛ
ЕРТРМ

Мы видим три слова, но чтобы понять, что ключ верный, хватило бы и первого. С него и начнем.

Если тот, кто шифровал сообщение, сдвигал алфавит на k шагов вперед, то мы будем сдвигать его на те же k шагов назад.

Начинаем с $k = 1$.

Для первой буквы Т

$$y_1 = (x_1 - k) \bmod 32 = 25 - 1 = 24$$

Т → С

Для остальных букв: Л → К, П → О

Получившееся слово: СКО

Кажется, оно не слишком осмысленное! Значит, берем следующий ключ $k = 2$.

Т → Р, Л → И, П → М

А тут мы, кажется, угадали. Применяя ключ $k = 2$ к остальному тексту, получаем:

РИМ - ВЕЧНЫЙ ГОРОД

Теперь можно почувствовать себя Цезарем - одновременно шифровать и, расшифровывать ~~и взламывать~~! Успехов с задачами!