ШИФРОВАНИЕ ТЕКСТОВЫХ СООБЩЕНИЙ. ШИФР ЦЕЗАРЯ

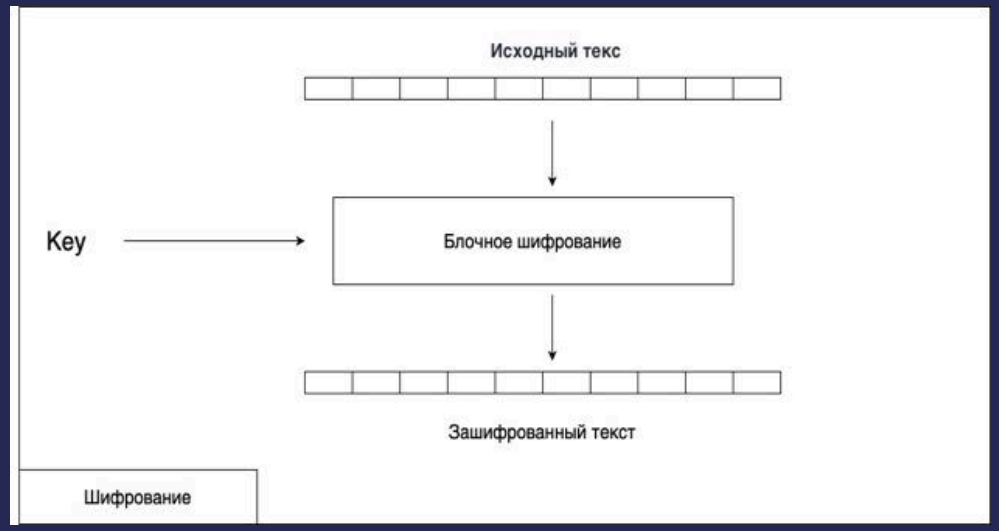
Чинянина Анастасия Сергеевна,

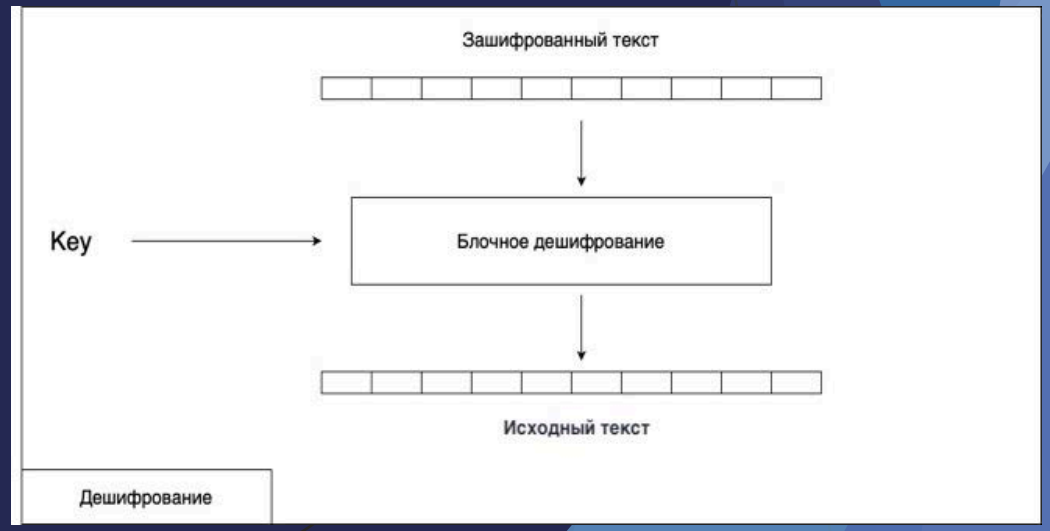
педагог дополнительного образования

БУ ДО «Омская областная станция юных техников»

- **Шифрование** – это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочитать данные, если они это сообщение перехватят. Делается это преобразование по специальным математическим и логическим алгоритмам, некоторые из которых мы рассмотрим ниже.
- **Исходное сообщение** – это, собственно, то, что мы хотим зашифровать. Классический пример — текст.
- **Шифрованное сообщение** – это сообщение, прошедшее процесс шифрования.
- **Шифр** — это сам алгоритм, по которому мы преобразовываем сообщение.
- **Ключ** — это компонент, на основе которого можно произвести шифрование или дешифрование.
- **Алфавит** – это перечень всех возможных символов в исходном и зашифрованном сообщении. Включая цифры, знаки препинания, пробелы, отдельно строчные и заглавные буквы и т.д.

- **Криптография** – это наука защиты информации от нежелательных лиц путем преобразования ее в форму, не распознаваемую злоумышленниками при хранении и передаче.
- Криптология не нова, она существует более 2000 лет. Слово криптология происходит от двух греческих слов: kryptos, что означает «скрытый или секретный» и graphein что означает писать.
- **Криптология** - наука позволяющая делать общение непонятным для всех, кроме предполагаемых получателей.



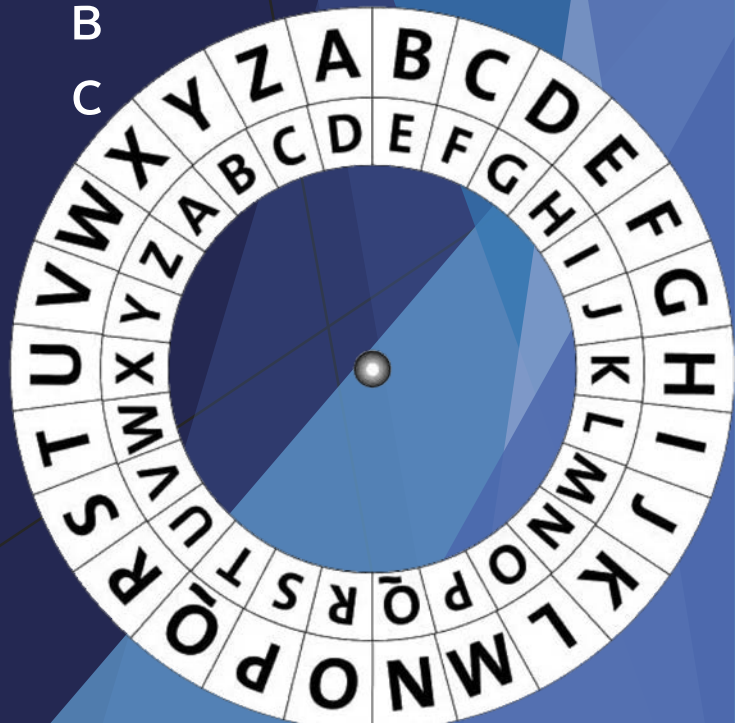


Ылчу Щзкгув

или в переводе с «Шифра Цезаря» на русский — **Шифр Цезаря**.

- **Шифр Цезаря** — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.
- Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.
- Величину сдвига можно рассматривать как ключ шифрования.

- Шифр Цезаря - моноалфавитный шифр. Это тип шифра подстановочного типа, где каждая буква в открытом тексте заменяется на другую букву, смещенную на некоторое фиксированное количество позиций в алфавите. Шифрование представлено с использованием модульной арифметики.



- Сдвиги в шифре обозначаются как ROTN, где N - это количество сдвигов. Например, ROT13 обозначает шифр с использованием сдвига 13.
- Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.
- Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

При сдвиге на 3:

- Буква «А» становится буковой «Г»;
- Буква «О» становится буквой «С».

При сдвиге на -2:

- Буква «Г» становится буковой «Б»;
- Буква «И» становится буквой «Ж».

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
1	2	3	4	5	6	7	8	9	10	11
К	Л	М	Н	О	П	Р	С	Т	У	Ф
12	13	14	15	16	17	18	19	20	21	22
Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
23	24	25	26	27	28	29	30	31	32	33

При сдвиге на 2:

- Учитель
- Информация
- Кабинет
- Компьютер

При сдвиге на -1:

- Фспл
- Ибебойё
- Сфшлб
- Тёнйобс

Применение в педагогической деятельности:

- Шифрование темы или цели занятия с помощью Шифра Цезаря;
- Подвести с помощью шифра к теме «Шифровка информации»;
- Подвести с помощью шифра к теме «Гай Юлий Цезарь»

Задачи по программированию:

- **Задача** 1: Дана строка размерностью n, которую пользователь вводит с клавиатуры. Зашифровать это строку с помощью Шифра Цезаря с шагом 1.

- **Задача** 2: Дана строка размерностью n, которую пользователь вводит с клавиатуры. Дешифровать это строку с помощью Шифра Цезаря с шагом 2.

- **Задача** 3: Дана строка размерностью n, которую пользователь вводит с клавиатуры и число k. Зашифровать это строку с помощью Шифра Цезаря с шагом k.

Трбтйвп иб гойнбойё!

Чинянина Анастасия Сергеевна

Контактная информация

Телефон: 8 999 454 78 41

Email : andreevatma55@gmail.com