# Шифры, пароли и Имаджинариум

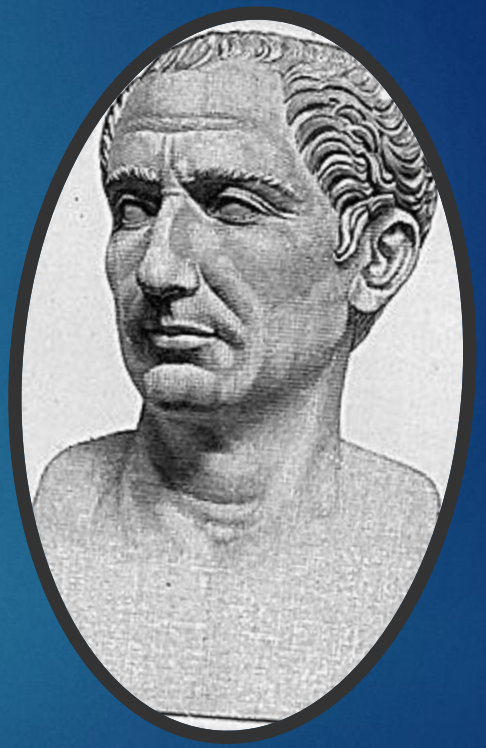
ИЛИ КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ

# Шифр Цезаря

- Шифр Цезаря – это шифр, где каждая буква заменяется следующей или предыдущей по алфавиту. (А⇨Б или наоборот)

Пример:

Шифр Цезаря ⇨ Щйхс Чёибса



# История Шифра Цезаря

Шифр Цезаря называют в честь Юлия Цезаря, который согласно «Жизни двенадцати цезарей» использовал его со сдвигом 3, чтобы защищать военные сообщения.

Хотя Цезарь был первым зафиксированным человеком, использующим эту схему, другие шифры подстановки, как известно, использовались и ранее.

*"Если у него было что-либо конфиденциальное для передачи, то он записывал это шифром, то есть так изменял порядок букв алфавита, что нельзя было разобрать ни одно слово. Если кто-либо хотел дешифровать его и понять его значение, то он должен был подставлять четвертую букву алфавита, а именно, D для A, и так далее, с другими буквами."*

# Шифр Атбаш

В этом шифре каждая буква заменяется противоположной

(А⇨Я, Б⇨Ю…)

Пример: Шифр Атбаш⇨Жцко Ямюяж

# История Шифра Атбаш

- Шифр Атбаш был, скорее всего, изобретен иудейской сектой повстанцев. Они разработали множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования. Шифр был использован на протяжении многих лет, с V до XIII вв. до н.э.

אתבש – Вот как он записывается на еврейском.

1 – ש буква

ב – последняя (22)

2 - ת

א – предпоследняя (21)

# Шифр Виженера

Здесь необходим ключ в виде слова, например “труден”

Если мы хотим зашифровать фразу “Шифр Виженера очень”, то необходимо записать слова таким образом:

ШифрВиженераочень

Т р у денТ руден т руде (Записать буквы одна под другой)

Далее воспользоваться данной таблицей

Получить “кщзф жцщхбихн бзшсб”

Таким образом, “Шифр Виженера Очень”  труден =

Кщзф жцщхбин бзшсб

# История Шифра Виженера

- В 1466 году Леон Альбертии, знаменитый архитектор и философ представил трактат о шифрах в папскую канцелярию. В трактате рассматриваются различные способы шифрования, в том числе маскировка открытого текста в некотором вспомогательном тексте. Работа завершается собственным шифром, который он назвал «шифр, достойный королей». Это был многоалфавитный шифр, реализованный в виде шифровального диска. Суть заключается в том, что в данном шифре используется несколько замен в соответствии с ключом. Позднее Альберти изобрел код с перешифровкой. Данное изобретение значительно опередило свое время, поскольку данный тип шифра стал применяться в странах Европы лишь 400 лет спустя.

# Музыкальная Пауза

# Степени и суммы

- Здесь пусть текст напишет Константин Шмидт (о том, как считать степени).

- P.s. Если не получится, на слайде 8 есть кнопка пропуска в правом нижнем углу.

# А теперь, о паролях

Есть правила составления паролей, чтобы ваши данные были надёжно защищены и не попали в руки плохим людям.

1) Не используйте одинаковые пароли везде
2) Пароль должен быть длиннее 7 символов
3) Используйте заглавные и строчные буквы, цифры, символы.

Совет: Можно использовать зашифрованное название сайта.

# Этим мы сейчас и займёмся!

- Зашифруйте слово из 4-5 букв на английском языке
- Дайте зашифрованное слово соседу по парте
- Расшифруйте слово.

- Используйте ассоциации, воображение!

Пример: APPLE ⇨ A2!pl_3< ⇨ A 2P L E ⇨ APPLE

# Подведём итог:

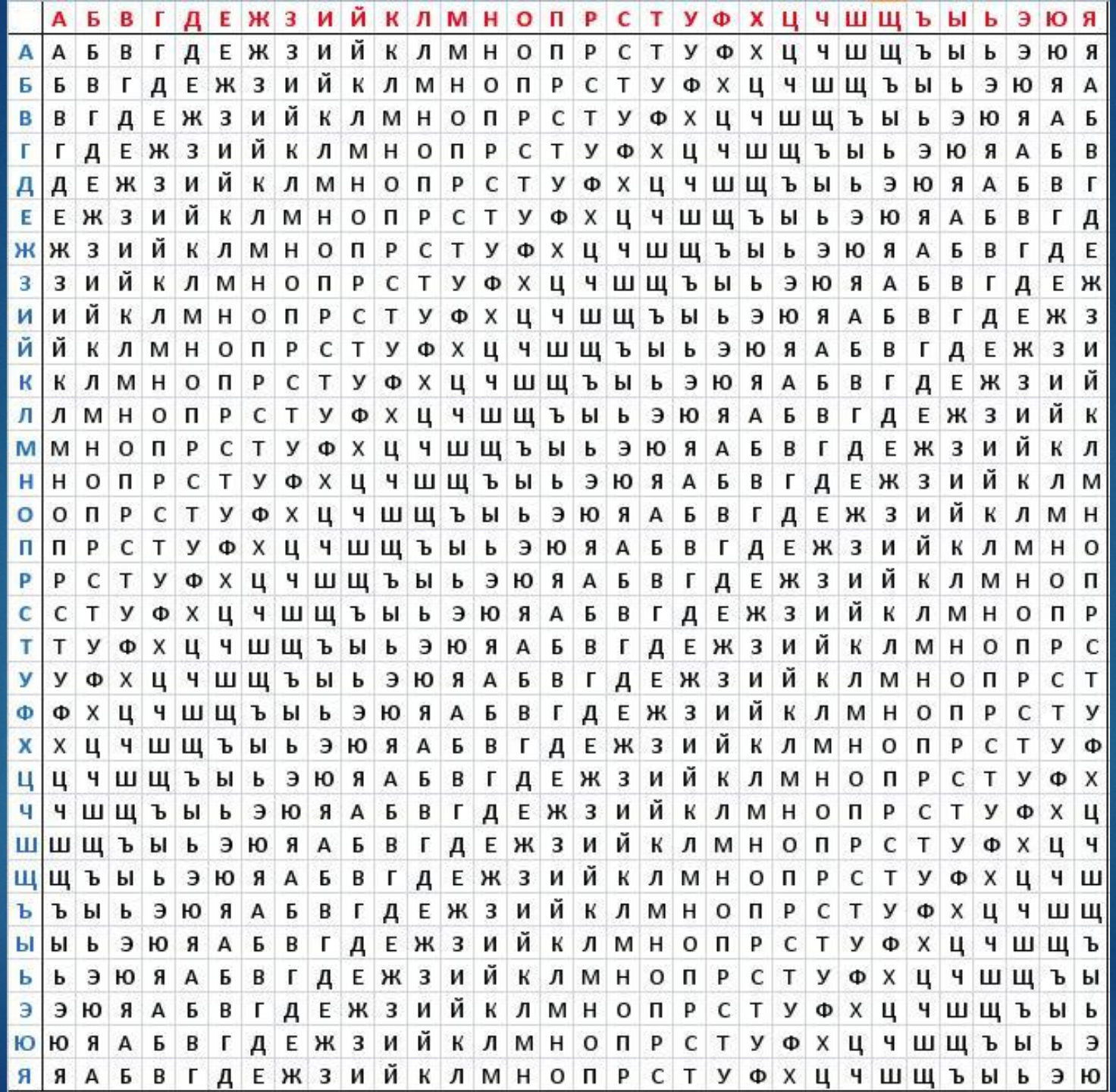
Мы научились:

1) Разгадывать шифры
2) Составлять пароли
3) Серьёзно относиться к информации

Мы узнали:

1) Несколько разных шифров
2) Правила составления паролей
3) Как использовать воображение в математике

# СПАСИБО ЗА ВНИМАНИЕ!



| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | 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 |
| Б | 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 | А |
| В | 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 | А | Б |
| Г | 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 | А | Б | В |
| Д | 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 | А | Б | В | Г |
| Е | 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 | А | Б | В | Г | Д |
| Ж | 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 | А | Б | В | Г | Д | Е |
| З | 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 | А | Б | В | Г | Д | Е | Ж |
| И | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З |
| Й | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И |
| К | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й |
| Л | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К |
| М | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л |
| Н | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М |
| О | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н |
| П | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О |
| Р | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П |
| С | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р |
| Т | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С |
| У | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т |
| Ф | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У |
| Х | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| Ц | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| Ч | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц |
| Ш | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч |
| Щ | Щ | Ъ | Ы | Ь | Э | Ю | Я | 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 |
| Ъ | Ъ | Ы | Ь | Э | Ю | Я | 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 |
| Ы | Ы | Ь | Э | Ю | Я | 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 |
| Ь | Ь | Э | Ю | Я | 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 |
| Э | Э | Ю | Я | 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 |
| Ю | Ю | Я | 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 |
| Я | Я | 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 |