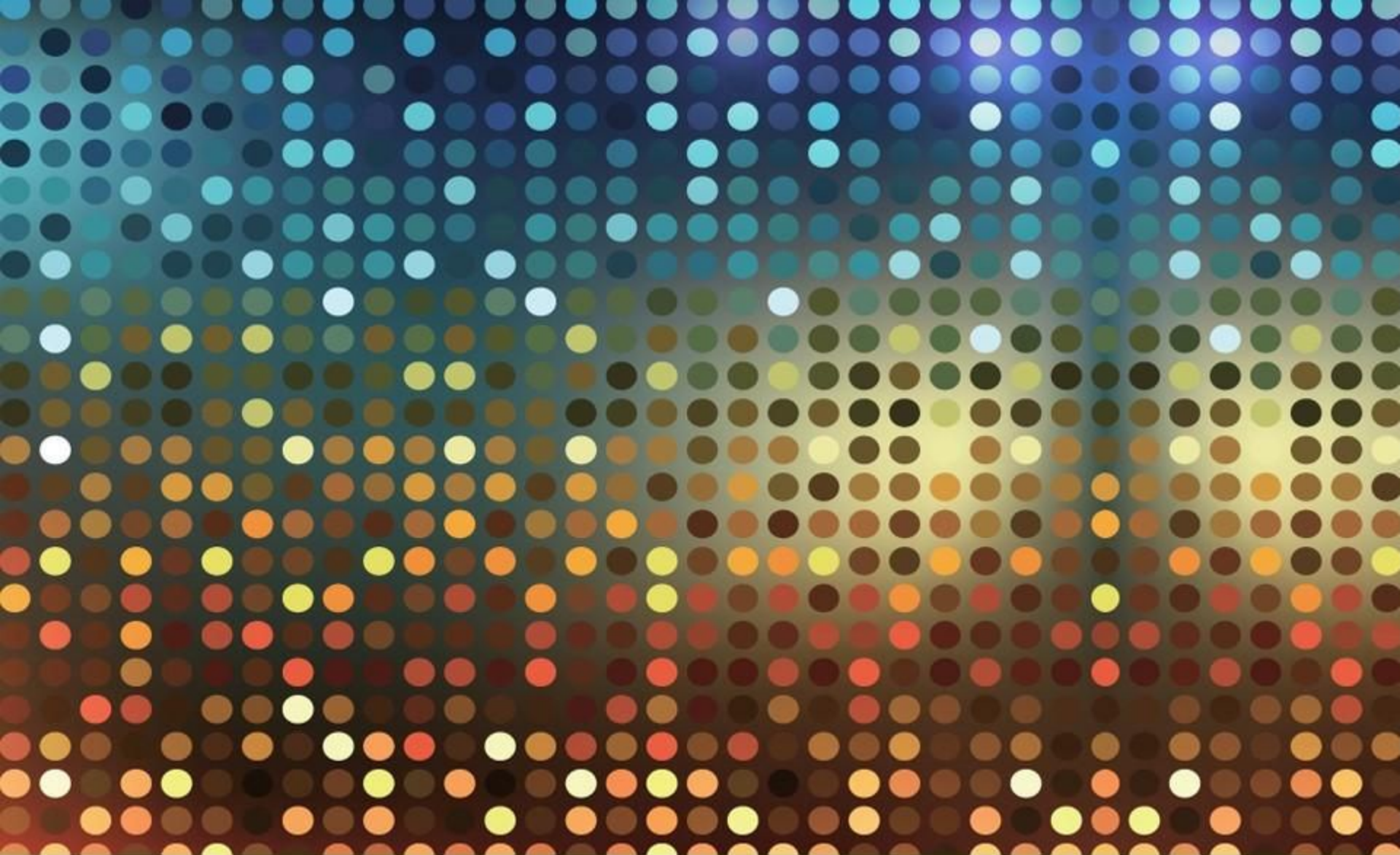




# РАЗЛИЧНЫЕ СПОСОБЫ ШИФРОВАНИЯ

# Примеры шифров:

1. [«Тарабарская грамота»](#)
2. [Код Цезаря](#)
3. [Шифрование с помощью кодового слова](#)
4. [Книжный шифр](#)
5. [Маршрутная перестановка](#)

# «Тарабарская грамота»

Фразеологизм тарабарская грамота «что-либо бессмысленное, непонятное (печатные сочинения, чье-либо выступление, речи)».



*Пример.* В книге В. Тредиаковский «Разговор об ортографии»:

«Что за тарабарская подлинно грамота? Как можно удержаться от смеха?»



Все гласные буквы оставались неизменными, а согласные заменялись друг на друга по следующей схеме: (в первой строке согласные идут в обычном порядке, а во второй строке — в обратном).

|   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|
| б | в | г | д | ж | з | к | л | м | н |
| щ | ш | ч | ц | х | ф | т | с | р | п |

□ Криптография — т м и н к о ч м а з и я

□ Параллелограмм — н а м а с с е с о ч м а р р

# Код 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.

|           |   |   |   |   |   |   |   |   |   |     |   |     |
|-----------|---|---|---|---|---|---|---|---|---|-----|---|-----|
| На 3<br>→ |   |   | А | Б | В | Г | Д | Е | Ё | Ж   | З | ... |
| А         | Б | В | Г | Д | Е | Ё | Ж | З | И | ... |   |     |



# Сдвиг на 2

А Б В Г Д Е Ё 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

- Треугольник – Ф т ж х е р н ю п к м;
- График – Е т в ц к м

# С помощью кодового слова

Рассмотрим способ шифрования с помощью кодового слова. Выбирается слово, все буквы которого различны. Его буквы нумеруются по порядку появления их в алфавите. Затем в таблицу помещается кодовое слово, под ним - номера букв, а текст вписывается по горизонтали. Для зашифровки текст из столбцов по порядку номеров записывается в строку.



| Ц | Е | З | А | Р | Ь |
|---|---|---|---|---|---|
| 5 | 2 | 3 | 1 | 4 | 6 |
| м | а | т | е | м | а |
| т | и | к | а | - | ц |
| а | р | и | ц | а | в |
| с | е | х | н | а | у |
| к | , | а | р | и | ф |
| м | е | т | и | к | а |
| - | ц | а | р | и | ц |
| а | м | а | т | е | м |
| а | т | и | к | и | а |

□ Кодовое слово *ЦЕЗАРЬ*

□ Пронумеруем столбцы

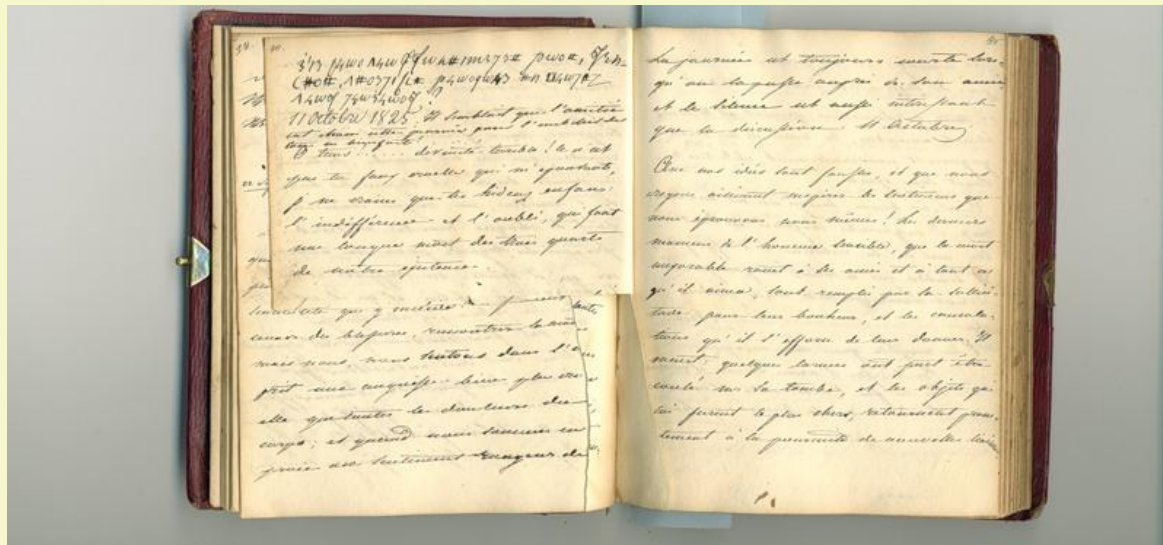
□ Текст «*Математика - царица всех наук, арифметика – царица математики*». В последней строчке остались свободные места, заполним их буквами.

□ Выпишем текст по столбцам в строку.

□ Получим шифровку:  
*ЕАЦНРИРТКАИРЕ,  
 ЕЦМТТКИХАТААИМ-  
 ААИКИЕИМТАСК-  
 АААЦВУФАЦМ*

# Книжный шифр

Суть этого шифра состоит в замене букв на номер строки и номер этой буквы в строке в заранее оговоренной странице некоторой книги. Ключом такого шифра является книга и используемая страница в ней.



*Птичка Божия не знает  
Ни заботы, ни труда,  
Хлопотливо не свивает  
Долговечного гнезда.  
В долгу ночь на ветке дремлет;  
Солнце красное взойдет,  
Птичка гласу бога внимлет,  
Встрепенется и поет.  
А. С. Пушкин «Цыганы»*

- Положим ключом к шифру будет отрывок из стихотворения *А.С.Пушкина*: «Цыганы».
- Предстоит зашифровать слово: «Книга».

- Первая буква слова – «К», мы её обозначаем  $1/5$ , где числителем будет строка, знаменателем – порядок букв в этой строке.

- Книга –  $1/5, 3/10, 7/3, 7/7, 4/18$

# Маршрутная перестановка

Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

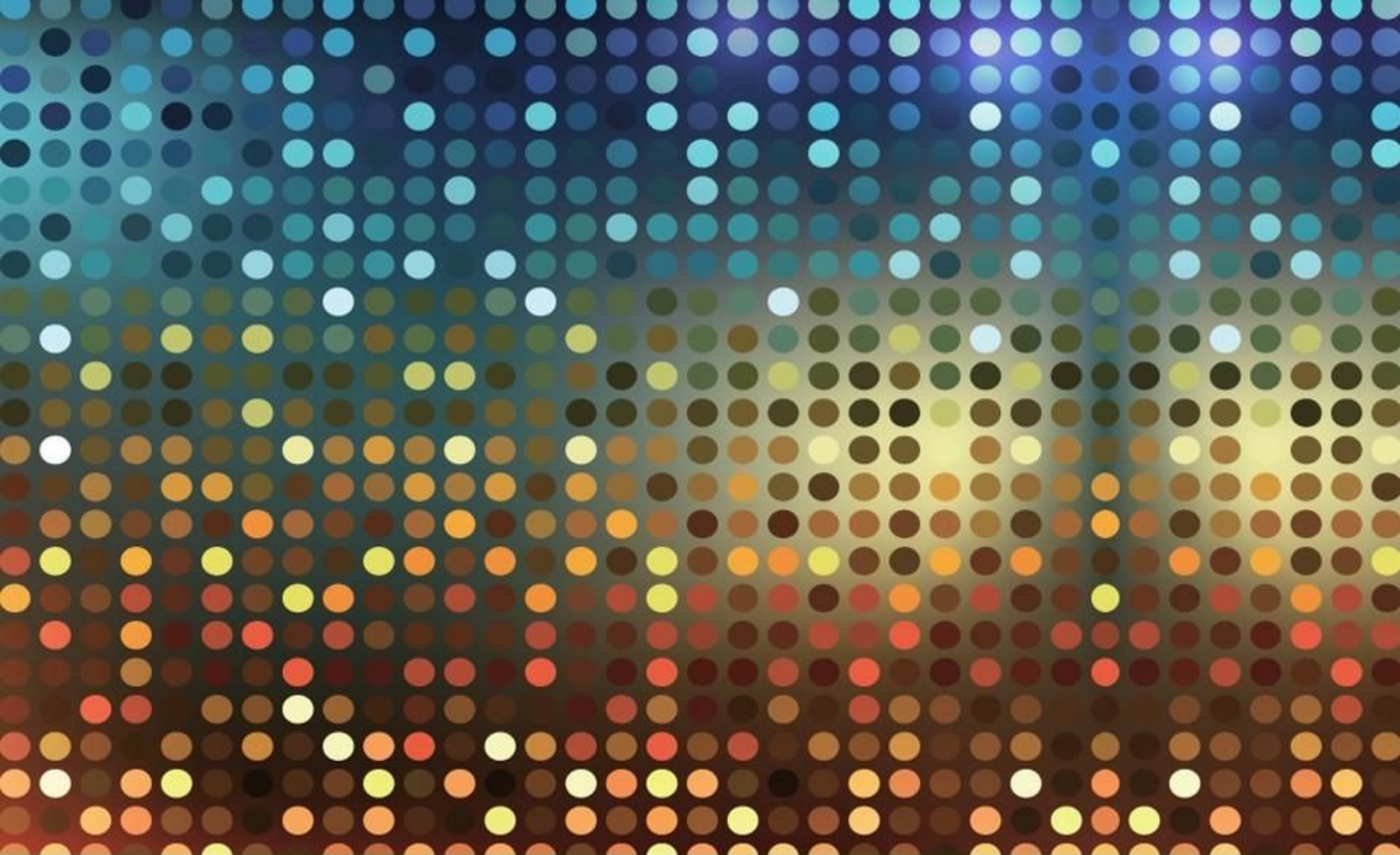


|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | к | р | а | с | н |
| 2 | а | п | т | и | ц |
| 3 | а | п | е | р | ь |
| 4 | е | м | , | а | ч |
| 5 | е | л | о | в | е |
| 6 | к | у | ч | е | н |
| 7 | ь | е | м | а | б |

- Зашифруем фразу: « *Красна птица перьем, а человек учением* » размера пять на семь :
- Зашифрованная фраза выглядит так: *НЦЬЧЕНБСИРАВЕААТЕ, ОЧМРППМЛУЕКААЕЕЕКЪ*
- Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.

- Зашифрованная фраза выглядит так: *НЦЬЧЕНБСИРАВЕААТЕ, ОЧМРППМЛУЕКААЕЕЕКЪ*

- Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.



*Выполнила ученица 10 «А» класса :  
Петрова П.*