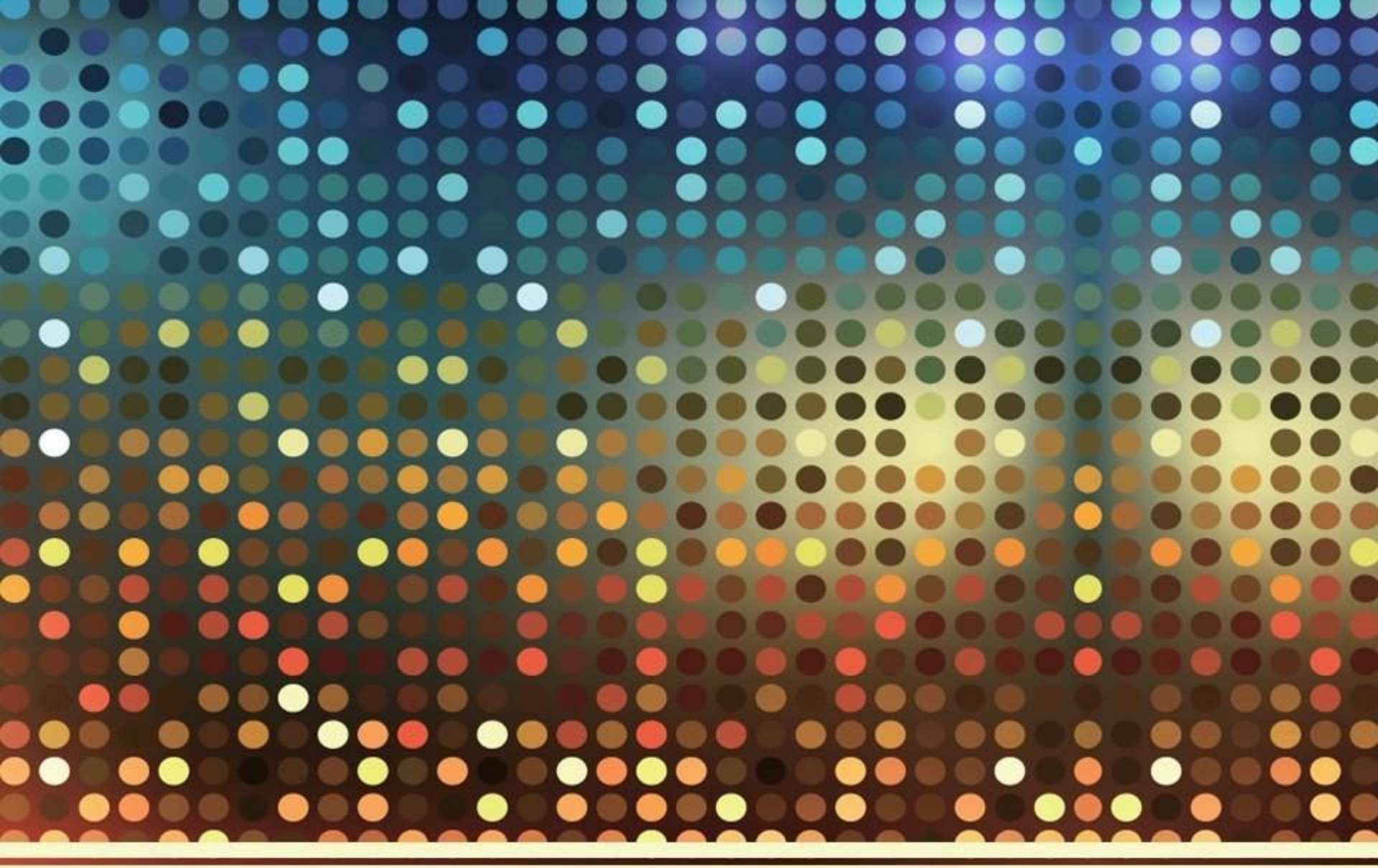


СВЯЗЬ МАТЕМАТИКИ И КРИПТОГРАФИИ

Книжный шифр

Ключ шифра – книга и страница в ней.

Из криптографии:

Зашифрованный текст состоит из дробей, где числителем будет строка, знаменателем – порядок букв в этой строке.

Из математики:

Дробь – координата буквы на странице.

Код Цезаря

Ключ шифра – алфавит, произвольное постоянное число.

Из криптографии:

Зашифрованный текст состоит из замен буквы на букву, полученную сдвигом на постоянное число в алфавите.

Из математики:

Функция – однозначное соответствие элементов одного множества с элементами другого.

Например: $f(x) = x + 3$

Свойства:

D(f) = все буквы алфавита

E(f) = все буквы алфавита

T = 33

Скитала

Ключ шифра – две палки одинаковой длины и толщины.

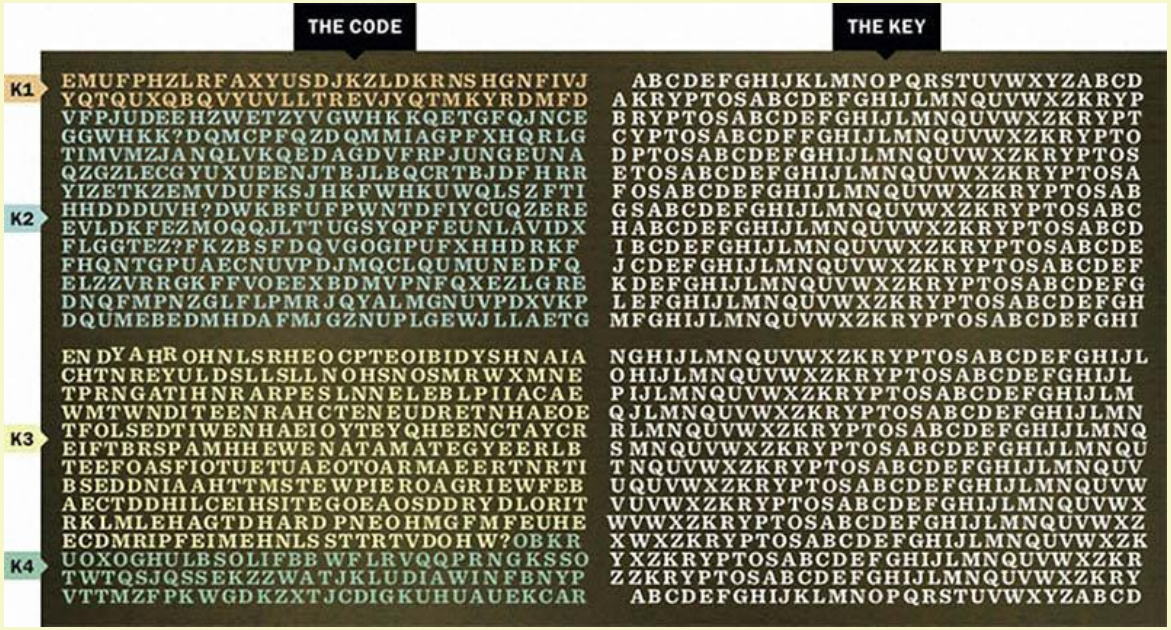
Из криптографии:

Длинную узкую полосу папируса наматывали на скиталу (без промежутков), записывали текст вдоль оси цилиндра, отправляли собеседнику только папирус.

Расшифруйте послание:

«Меж смутною тенью и отсутствием света лежит иллюзии нюанс» - Джим Сэнборн

Расшифрованный фрагмент К1 на скульптуре созданной Джимом Сэнборном «Криптос» .



Из математики:

1. Чтобы расшифровать текст, необходимо знать диаметр скитала (предположим, что высота букв 1 см – легко проверить, а D=2). Т. о, $l_{\text{окр.}} = \pi D = 2\pi \approx 6{,}28 \approx 6$. Тогда можно прочитать текст, состоящий из n букв, пронумеровав каждую от 1 до 6, от 1 до 6 и т.д.
2. Если диаметр скиталы не дан, то надо изготовить длинный конус и, начиная с основания, обертывать его лентой с шифрованным сообщением, сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения. Так вычисляется диаметр скиталы (метод Аристотеля).

1 с	1
2 т	2 ф
3 м	3 а
4 й	4 р
5 и	5 п
6 ь	6 и
1 в	1 к
2 о	2 и
3 а	3 т
4	4 о
5 е	5 о
6 ю	6 т
1 я	1 р
2 г	2 и
3 т	3 и
4 ш	4 в
5	5 м
6	6 а
1 з	1 и
2 р	2
3 е	3 к
4 и	4 а
5 с	5 о
6 с	6 л
1 ь	1 п
2 а	2 с
3 м	3 о
4 ф	4 н
5	5 щ
6 к	6 ы

Тарабарская грамота

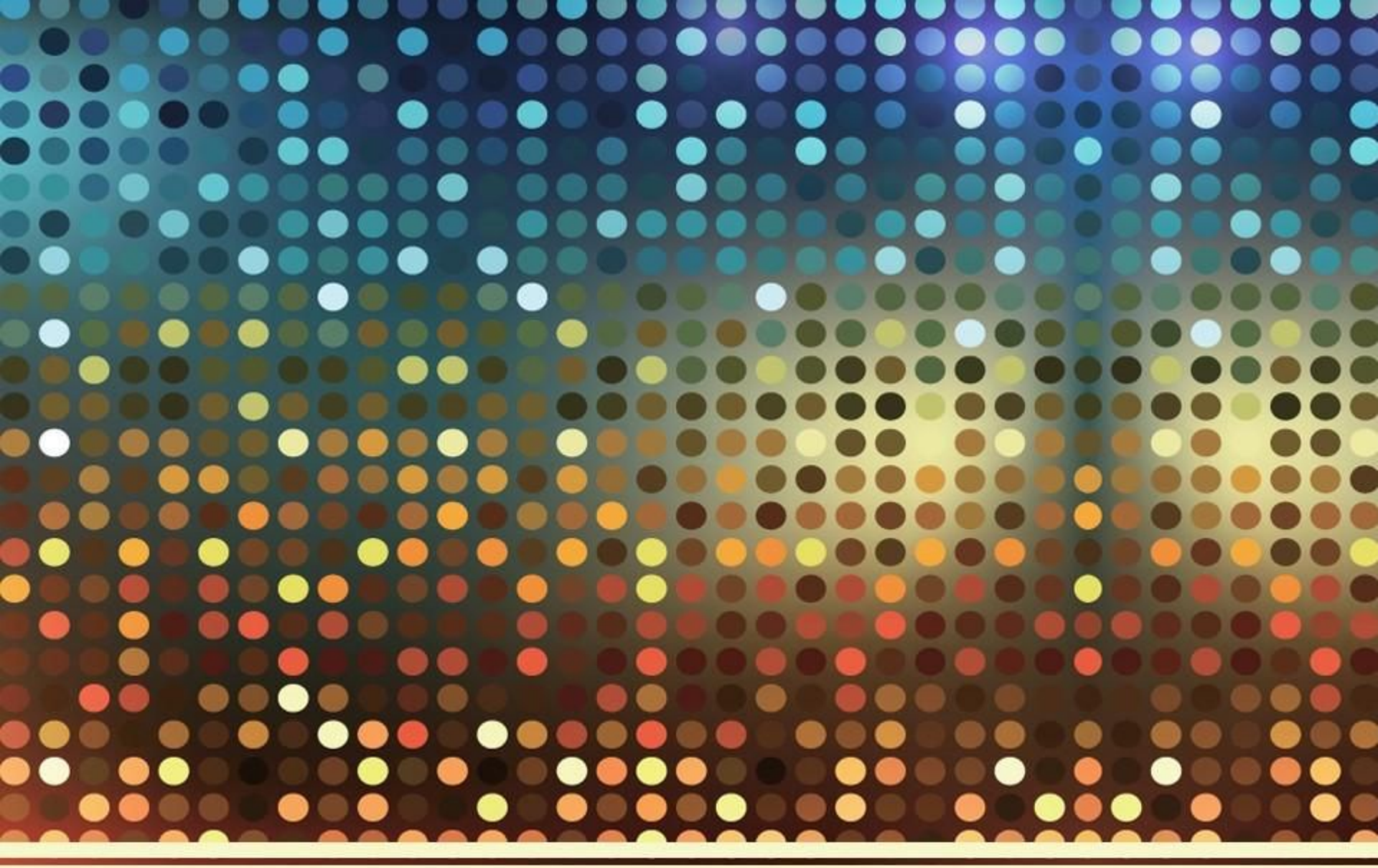
Ключ шифра – две строчки с буквами русского алфавита

Из криптографии:

Каждая согласная буква слов сообщения переходит в другую согласную по правилу.

Из математики:

Принцип шифрования и дешифрования сообщений подразумевает взаимно однозначное соответствие элементов двух множеств $A = \{б, в, г, д, ж, з, к, л, м, н\}$ и $B = \{щ, ш, ч, ц, х, ф, т, с, р, п\}$



Выполнил ученик 10 «А» класса :
Смирнов С.