

Департамент образования администрации г. Перми
Муниципальное автономное общеобразовательное учреждение
«Лицей № 4»

Методы шифрования в олимпиадных заданиях начальной школы

Выполнил:

Шарипов Айбулат
ученик 2 Б класса

Руководитель:

Хабибуллина Людмила Федаловна
учитель начальных классов

г.Пермь, 2022

Оглавление

| | |
|--|----|
| Введение | 3 |
| 1. История развития криптографии | 4 |
| 2. Методы шифрования в олимпиадных заданиях начальной школы..... | 6 |
| 3. Практическая часть исследования..... | 10 |
| Заключение | 11 |
| Список литературы..... | 12 |
| Приложение 1 | 13 |
| Приложение 2 | 17 |
| Приложение 3 | 18 |
| Приложение 4 | 19 |
| Приложение 5 | 20 |

Введение

Со своей младшей сестрой я часто играю в шпионские игры. Для передачи информации друг другу мы используем записки. Но чтобы информацию никто не рассекретил, мы зашифровываем ее, используя различные методы шифрования.

Недавно я узнал, что умение шифровать информацию развивает логическое мышление. Действительно, знание некоторых методов шифрования мне пригодилось для решения заданий на метапредметных олимпиадах и олимпиадах по математике. Это значит, что кодирование и декодирование, и правда, учит нас логически мыслить: сравнивать, рассуждать, обобщать, делать выводы. Все эти умения пригодятся мне в дальнейшей учебе.

Именно поэтому я заинтересовался криптографией - наукой о математических методах обеспечения конфиденциальности информации и решил изучить данный вопрос в рамках исследовательской работы.

Цель исследования: изучение методов шифрования и применение полученных знаний при решении метапредметных олимпиадных задач и олимпиадных задач по математике в рамках начальной школы.

Задачи исследования:

1. Изучить историю развития криптографии.
2. Провести анализ олимпиадных заданий для учеников начальных классов, позволяющий выявить методы шифрования, наиболее часто применяемые, в данных заданиях.
3. Придумать и описать собственный метод шифрования информации.
4. Разработать сборник заданий и упражнений на освоение основных методов шифрования для учеников 1-2 классов.

1. История развития криптографии

Человек с древних времен стал использовать методы шифрования информации, предназначенной для узкого круга лиц. Чаще всего шифрование информации использовалась в военных целях. Так, например, в древнем Китае часто использовали изощренные способы письма, которые были понятны лишь «избранным». Существует наука о невозможности прочтения информации посторонними – **криптография**, в переводе с греческого «скрытый» + «пишу».¹

XVI-XVIII века вошел в историю криптографии как эра «черных кабинетов». «Черные кабинеты» - это специальные службы, которые занимались перехватом, шифрованием, дешифровкой информации. В них входили агенты по перехвату писем, специалисты по имитированию почерка, по подделке печатей, переводчики и многие другие. Эти люди очень высоко ценились (рис.1).



Рис. 1 «Черные кабинеты», XVI-XVIII века²

Во время Первой мировой войны криптография была признана полноценным боевым инструментом. Стоило только разгадать сообщения противника – и можно было получить ошеломляющий результат. Чуть позже стали развиваться компьютерные системы, так, для засекречивания важной информации во время второй мировой, использовались шифровальные машины (немецкая «Энигма», английская «Бомба Тьюринга»)³.

¹ Википедия <https://ru.wikipedia.org/wiki/>

² Мир цифровых и информационных технологий <https://www.it-world.ru/tech/technology/>

³ <https://www.iphones.ru/> Как взломали немецкий код Enigma во время Второй Мировой войны

Значительное влияние на развитие криптографии оказало появление телеграфа, ведь сам факт передачи данных перестал быть секретным, что заставило отправителей сосредоточиться на шифровании данных.

Сегодня криптография развивается на стыке математики и информатики. В современной жизни каждый из нас сталкивается с цифровизацией (кодированием) информации. В качестве простых примеров можно привести: переписку в различных интернет-мессенджерах; эл. дневник ученика и т.д. Даже обычное управление электронными приборами «умного дома» осуществляется по шифрованным каналам данных во избежание вмешательства в их работу злоумышленников.⁴

Итак, обмен данными должен быть защищен от вмешательства извне, и шифрование - как раз метод, позволяющий этого достичь. Сейчас любая передача данных должна быть шифрованной, если она не предназначена широкому кругу лиц.

⁴ <https://lifehacker.ru/special/umnyj-dom/> Что такое умный дом и как он работает

2. Методы шифрования в олимпиадных заданиях начальной школы

Методы шифрования имеют не только бытовое и военное назначение, но и активно используются в развитии логического мышления ребенка. С первого класса я принимал участие в нескольких метапредметных, тест-рейтинговых олимпиадах и олимпиадах по математике. Мной было замечено, что все олимпиады включали задание на шифрование. Мои наблюдения подтвердились результатом проведенного анализа заданий онлайн-олимпиад интернет платформы «Систематика»⁵ для учащихся 1-4 классов за последние 3 года (табл. 1).

Таблица 1. Наличие заданий на кодирование в онлайн-олимпиадах

| | 2020 год | 2021 год | 2022 год |
|---------|----------|----------|----------|
| 1 класс | + | + | + |
| 2 класс | + | + | + |
| 3 класс | + | - | + |
| 4 класс | + | - | + |

Доля онлайн-олимпиад содержащих задания на кодирование представлена в диаграмме 1.

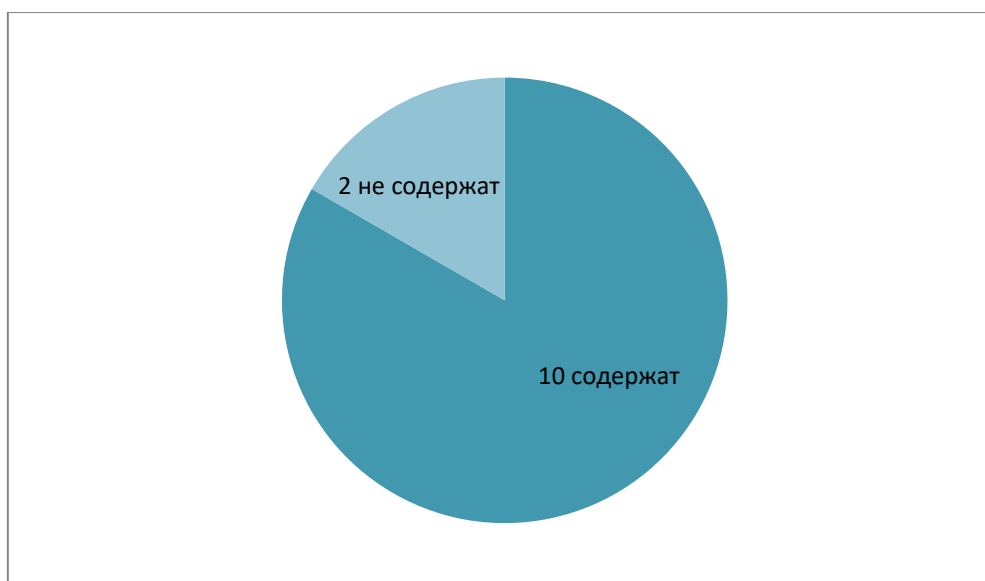


Диаграмма 1. Доля онлайн-олимпиад содержащих задания на кодирование

В результате проведенного анализа, мы видим, что 10 из 12 олимпиад содержат задания на кодирование информации. Примеры олимпиадных заданий (см. приложение 1). Так же проведенный анализ позволил выявить методы шифрования,

⁵ <https://systematika.org/> Онлайн школа Систематика

наиболее часто применяемые, в олимпиадных заданиях для учеников 1-4 классов. Опишем основные из них.

Книжный шифр

В таком шифре ключом является некая книга, имеющаяся и у отправителя, и у получателя. В шифре обозначается страница книги и строка, первое слово которой и является разгадкой. Дешифровка невозможна, если книги у отправителя и корреспондента разных годов издания и выпуска. Книги обязательно должны быть идентичными.

Так, например, возьмем стихотворение А.С.Пушкина «К Чаадаеву»⁶

Любви, надежды, тихой славы

Недолго нежил нас обман,

Исчезли юные забавы,

Как сон, как утренний туман;

В данном виде шифрования указатели выделяют на букву, в некоторых случаях выделяются целые слова. Зашифруем слово «книга».

Зашифрованный текст: 4/1,1/6, 1/5, 2/6, 1/7. Где, первое число – номер строки (начиная отсчет сверху), второе – номер буквы в строке (слева направо).

Шифр Цезаря

Шифр Цезаря заключается в том, что буквы алфавита заменяются буквами того же алфавита, но со сдвигом вправо на 3 позиции. Пример ключа применительно к русскому языку будет выглядеть так:

Таблица 2. Шифр Цезаря

| Открытый текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 | а | б | в |
| Зашифрованный текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

При зашифровывании буква А заменялась буквой Г, Б заменялась на Д, В – Е и так далее. Так, например, «Россия» превращалось в слово «Усххлв».

⁶ <https://www.culture.ru/poems/4453/k-chaadaevu>

Гай Юлий Цезарь использовал этот способ шифрования при переписке со своими генералами для защиты военных сообщений. Этот шифр довольно легко взламывается, поэтому используется редко.

Шифр пар

Алфавит **случайным** образом записывают в 2 строки, и шифрования текста происходит заменой буквы на соседнюю по вертикали.

Таблица 3. Шифр пар

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| в | ы | э | ё | у | ж | и | ф | м | н | о | ъ | к | п | а | р | я |
| е | т | х | й | ш | ю | д | ь | б | щ | з | с | ц | г | ч | л | - |

К примеру, зашифруем слово «Родина», используя шифр пар, получится «Лзидщч».

Шифр с кодовым словом

Еще один простой способ как в шифровании, так и в расшифровке. Используется кодовое слово (любое слово без повторяющихся букв). Данное слово вставляется впереди алфавита и остальные буквы по порядку дописываются, исключая те, которые уже есть в кодовом слове.

Сначала выбирается кодовое слово, которое пишется впереди, а затем пишут все остальные буквы алфавита (за исключением тех, что использовались в кодовом слове).

Таблица 4. Шифр с кодовым словом

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|----------|----------|----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Открытый текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 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 |
| ш | и | ф | р | а | б | в | г | д | е | ё | ж | з | й | к | л | м | н | о | п | с | т | у | х | ц | ч | щ | ъ | ы | ь | э | ю | я |
| Зашифрованный текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

К примеру, зашифруем слово «Родина», используя шифр с кодовым словом «шифр» получится «Нлаекш».

Цифровое (числовое) кодирование

Кодирование с помощью чисел. Появилось, наверное, вместе с первым алфавитом. Например, поскольку каждая буква знает свое место, то у нее есть номер, а

значит, букву можно заменить цифрами: а - 1, к - 12, о - 16 и т.д. Для того чтобы пользоваться цифровым кодом, нужно выучить алфавит.

Ребусы

Ребус - это задача, в которой картинками зашифровано слово. Данное определение ребуса уже всем давно известно. Теперь же ребус можно не редко увидеть и в другом контексте, когда говорят о чем-нибудь загадочном и неизведанном. Ребус играл очень важную роль в образовании письменности всех веков и народов, ведь даже пещерные люди писали на древних скалах рисунками, которые понимали только они, позже эти рисунки переходили впервые буквы названий этих рисунков. Правила расшифровки ребусов (см. приложение 2)

3. Практическая часть исследования

Изучив существующие методы шифрования, я решил разработать свой собственный метод, который назвал – табличный метод. Задание на применение моего метода я включил в сборник метапредметных и математических заданий и упражнений на освоение основных методов шифрования.

Алфавит записан в таблицу. Строчки таблицы пронумерованы, а столбцам присвоен символ. Зашифровать букву значит присвоить ей код, где на первом месте указываем номер строки, на втором месте указываем символ.

«радость» = «3⊗ 1○ 1! 3⋈ 4○ 4□ 5⊗»

Таблица 5. Табличный метод

| | ○ | □ | △ | ⋈ | ! | ⊗ |
|---|---|---|---|---|---|---|
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ё | Ж | З | И | Й | К |
| 3 | Л | М | Н | О | П | Р |
| 4 | С | Т | У | Ф | Х | Ц |
| 5 | Ч | Ш | Щ | Ъ | Ы | Ь |
| 6 | Э | Ю | Я | . | ! | ? |

В рамках исследовательской работы нами был разработан сборник заданий и упражнений на освоение основных методов шифрования для учеников 1-2 классов. Сборник включает задания, в основе которых лежат методы наиболее часто применяемые в олимпиадных заданиях.

Мы предполагаем, что сборник может иметь практическую значимость как для учеников 1-2 классов так и для их учителей.

Заключение

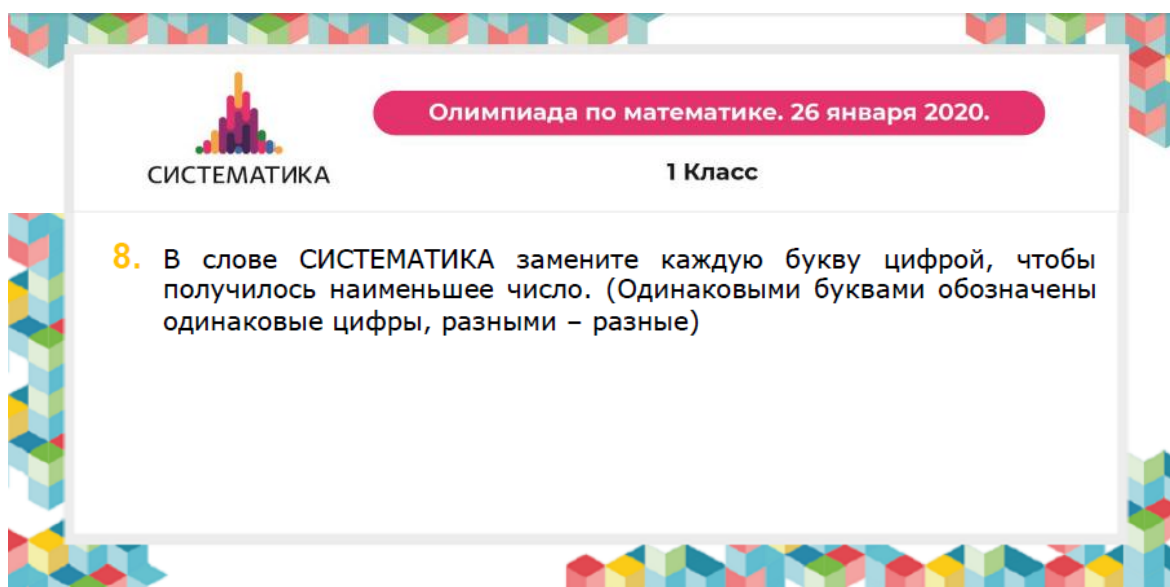
Изучив материалы по теме исследовательской работы, я пришел к выводу, что развитие навыков шифрования и дешифрования информации очень важны при подготовке к олимпиадам по математике и метапредметным олимпиадам. Проведенный мной анализ олимпиадных заданий еще раз подчеркивает актуальность темы исследования.


Разработанный мной метод шифрования информации может быть использован ребятами в играх, тем самым способствуя развитию логического мышления, которое, как говорилось ранее, является основой успешного обучения любого ученика.

В освоении навыка кодирования и декодирования данных главную роль играет тренировка. Именно поэтому считаю, что разработанный мной сборник заданий и упражнений на освоение основных методов шифрования, станет отличным помощником для ребят, готовящихся к олимпиадам. А учителя смогут использовать пособие на факультативных занятиях по математике.

Список литературы

1. Введение в криптографию. Под редакцией В. В. Яценко. Издание четвертое, дополненное. М: Издательство МЦНМО, 2007г.
2. Википедия <https://ru.wikipedia.org/wiki/>
3. Виленкин Н.Я. Математика и шифры, статья // «Квант» для младших школьников.-1996
4. Как взломали немецкий код Enigma во время Второй Мировой войны <https://www.iphones.ru/>
5. Криптография в литературе <http://project.1september.ru/works/600033>
6. Кузьмин Т. В. Криптографические методы защиты информации: моногр. / Т.В. Кузьмин. - Москва: Огни, 2013. - 192 с.
7. Культура РФ <https://www.culture.ru/poems/4453/k-chaadaevu>
8. Мир цифровых и информационных технологий <https://www.it-world.ru/tech/technology/>
9. Онлайн школа Систематика <https://systematika.org/>
10. Что такое умный дом и как он работает <https://lifehacker.ru/special/umnyj-dom/>

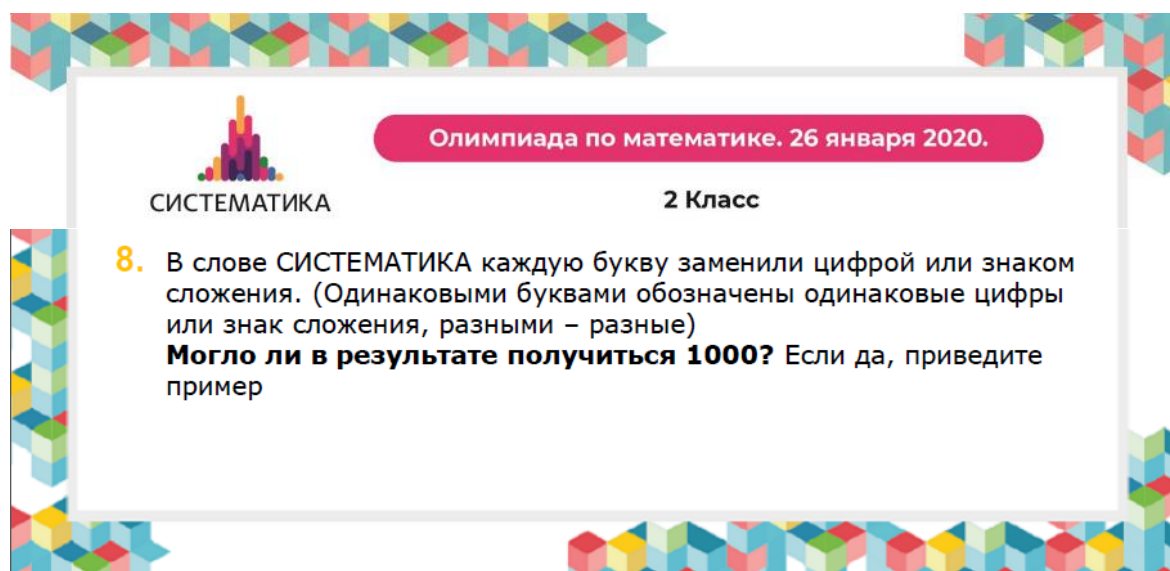





Олимпиада по математике. 26 января 2020.

СИСТЕМАТИКА 1 Класс

8. В слове СИСТЕМАТИКА замените каждую букву цифрой, чтобы получилось наименьшее число. (Одинаковыми буквами обозначены одинаковые цифры, разными – разные)

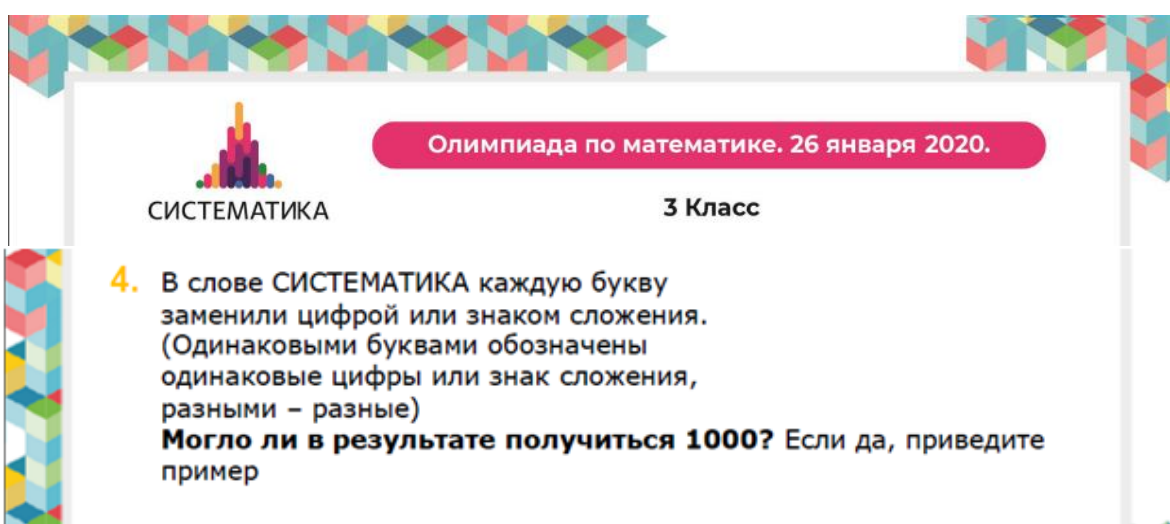





Олимпиада по математике. 26 января 2020.

СИСТЕМАТИКА 2 Класс

8. В слове СИСТЕМАТИКА каждую букву заменили цифрой или знаком сложения. (Одинаковыми буквами обозначены одинаковые цифры или знак сложения, разными – разные)
Могло ли в результате получиться 1000? Если да, приведите пример





Олимпиада по математике. 26 января 2020.

СИСТЕМАТИКА 3 Класс

4. В слове СИСТЕМАТИКА каждую букву заменили цифрой или знаком сложения. (Одинаковыми буквами обозначены одинаковые цифры или знак сложения, разными – разные)
Могло ли в результате получиться 1000? Если да, приведите пример



СИСТЕМАТИКА

Олимпиада по математике. 26 января 2020.

4 Класс

7. Известно что:

$$\otimes = 0$$

$$\nabla = 1$$

$$\blacklozenge = 2$$

$$\nabla \otimes = 3$$

$$\nabla \nabla = 4$$

$$\nabla \blacklozenge = 5$$

$$\nabla \otimes \otimes = 9$$

$$\nabla \otimes \nabla = 10$$

Чему равно?

А) $\nabla \nabla \nabla$

Б) $\blacklozenge \blacklozenge \blacklozenge$

В) $\nabla \otimes \otimes \otimes$



СИСТЕМАТИКА

Олимпиада по математике. 31 января 2021

1 класс


8. Перед вами результаты странного сложения:

$$\text{circle with cross} + \text{circle} = \text{plus sign}$$

$$\text{square with triangle} + \text{triangle} = \text{inverted triangle}$$







Чему тогда равно?

$$\text{square} + \text{crossed square} = ?$$

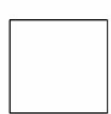
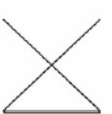
 Олимпиада по математике. 31 января 2021

СИСТЕМАТИКА 2 класс

7. Перед вами результаты странного сложения:

 +  = 
 +  = 


Чему равно?

 + 

Нет

 Олимпиада по математике. 31 января 2021

СИСТЕМАТИКА 3 класс

 Олимпиада по математике. 31 января 2021

СИСТЕМАТИКА 4 класс



Нет

 Олимпиада по математике. 30 января 2022

СИСТЕМАТИКА 1 класс

8. Гермиона зашифровала 3 звука животных: МУ, МЯУ и КРЯ. Разным буквам соответствуют разные цифры, а одинаковым — одинаковые. А потом она перепутала шифровки местами: 325, 982, 35. **Помогите Гермионе восстановить соответствия и понять, какое животное говорит то, что было зашифровано как 358.**

10. Мальвина написала пример, а Буратино, чтобы его не решать, положил на одну цифру яблоко, а на две другие одинаковые цифры по груше. **Какой пример написала Мальвина?**

 + 5 =  



СИСТЕМАТИКА

Олимпиада по математике. 30 января 2022

2 класс

7. Гермiona зашифровала 3 слова, TOP, SOP и SIP, так, что разным буквам соответствовали разные цифры, а одинаковым – одинаковые. А потом перепутала шифровки местами: 423, 123, 463. Помогите Гермione восстановить соответствия и понять, **какое слово было зашифровано как 461.**



СИСТЕМАТИКА

Олимпиада по математике. 30 января 2022

3 класс

9. На нескольких карточках Вася написал цифру, а с оборота букву (если цифры равны, то буквы одинаковы, если цифры различны – буквы разные). Вася считает сумму цифр на карточках. Если выложить слово ВОЛ получится сумма 10, а если МОЛВА, то 20. **А что получится в сумме, если выложить слово МАМА?**






СИСТЕМАТИКА

Олимпиада по математике. 30 января 2022

4 класс

3. На нескольких карточках Вася написал цифру, а с оборота букву (если цифры равны, то буквы одинаковы, если цифры различны – буквы разные). Вася считает сумму цифр на карточках. Если выложить слово ЛОМ, получится сумма 4, МОЛВА – 20, ВОЛ – 10. А что получится в сумме, если выложить слово ВАМ?

| | |
|--|---|
|  | <p>Запятая слева от рисунка означает, что нужно убрать первую букву. Если стоят две запяты - убирают две первые буквы. ГРОЗА - убрали Г, получилось РОЗА</p> |
|  | <p>Запятая справа от рисунка означает, что нужно убрать последнюю букву. Если стоят две запяты - убирают две последние буквы. ВОЛК - убрали К, получилось ВОЛ</p> |
| <p>ПО  КА</p> | <p>Если справа или слева от рисунка стоит одна или несколько букв - это значит, что эти буквы следует добавить. ПО + ДУШ + КА = ПОДУШКА</p> |
|  | <p>Зачёркнутая буква слева от рисунка означает, что нужно убрать первую букву. ГРОЗА - убрали Г, получилось РОЗА</p> |
|  | <p>Зачёркнутая буква справа от рисунка означает, что нужно убрать последнюю букву. ВОЛК - убрали К, получилось ВОЛ</p> |

| | |
|--|--|
|  | <p>Для удаления букв внутри слова их записывают над изображением и перечёркивают. МОНИТОР - убрали НИ, получилось МОТОР</p> |
| <p>3 2 1 </p> | <p>Для изменения порядка букв в слове над ним ставят цифры, которые определяют новый порядок следования букв. КОТ - получилось ТОК</p> |
|  | <p>Если картинка перевернута вверх ногами, это значит, что слово читается справа налево. КОТ - получилось ТОК</p> |
|  | <p>Постановка знака «=» между двумя буквами служит для указания замены одной из этих букв на другую.</p> |
|  | <p>На это же указывает зачёркивание одной буквы и помещение рядом с нею другой буквы. КОРОВА = КОРОНА</p> |

| | |
|---|--|
|  | <p>Если предметы или буквы изображены один в другом, то их названия читаются с прибавлением предлога «в»: ВОЛК</p> |
|  | <p>Если отдельно стоящие буквы зачёркнуты, то их необходимо читать с прибавлением частицы «не»: НЕУЧ</p> |
| <p>7Я</p> | <p>Вместо картинки могут использоваться числа. СЕМЬ + Я = СЕМЬЯ</p> |
|  | <p>Если поверх одной (большой) буквы несколько раз написана другая (маленькая), то при чтении используется предлог «по» (впереди или между названий). ПОЯС</p> |

| | |
|---|---|
|  | <p>Если большая буква составлена из маленьких, повторяющихся несколько раз букв, то при чтении используется предлог «из» (перед или между названий). ИЗБА</p> |
| <p>ФО РИ</p> | <p>Буквы, разделённые чертой, читаются так: ФОНАРИ</p> |
| <p>КА У</p> | <p>Или так: НАУКА</p> |
| <p>Ц Я</p> | <p>Одна буква за другой читаются так: ЗЯЦ</p> |

Глоссарий

Закрытый текст - данные, полученные после применения метода шифрования

Ключ - секретная информация, используемая при зашифровании/расшифровании данных

Код – представление какого либо слова (информации) в более короткой последовательности символов

Криптография - тайнопись

Метод – путь достижения цели

Открытый текст – текст, получившийся в результате расшифровки

Шифр – порядок (алгоритм) преобразования информации

Сборник заданий и упражнений на освоение основных методов шифрования для учеников 1-2 классов



**Сборник заданий и упражнений
на освоение основных методов шифрования
1-2 класс**

*Разработал:
Шарипов Айбулат
ученик 2 Б класса*

*Руководитель:
Хабибуллина Людмила Федаловна
учитель начальных классов*

г.Пермь, 2022



**Сборник заданий и упражнений
на освоение основных методов шифрования
1-2 класс**



A rounded rectangular box with a green border, containing four horizontal lines for writing.

Художественное оформление и макет А.Шарипова

Шарипов А.

Сборник заданий и упражнений на освоение основных методов шифрования, 1-2 класс/ А.Шарипов; МАОУ Лицей №4.-Пермь, 2022. -26

Сборник может быть использован в качестве дополнительного инструмента в процессе формирования у учеников 1-2 классов умений в области выполнения заданий на освоение основных методов шифрования. Он содержит разнообразные задания на шифрование и дешифрование данных.

Книжный шифр

В таком шифре ключом является некая книга, имеющаяся и у отправителя и у получателя. В шифре обозначается страница книги и строка, первое слово которой и является разгадкой. Дешифровка невозможна, если книги у отправителя и корреспондента разных годов издания и выпуска. Книги обязательно должны быть идентичными.

Так, например, возьмем стихотворение А.С.Пушкина «К Чаадаеву»

Любви, Надежды, тихой славы

Недолго нежил нас обман,

Исчезли юные забавы,

Как сон, как утренний туман;

Но в нас горит еще желанье;

Под гнетом власти роковой

Нетерпеливою душой

Отчизны внемлем призыванье.

В данном виде шифрования указатели выделяют на букву, в некоторых случаях выделяются целые слова. Зашифруем слово «КНИГА».

Зашифрованный текст: 4/1, 1/6, 1/5, 2/6, 1/7. Где, первое число – номер строки (начиная отсчет сверху), второе – номер буквы в строке (слева направо).

Задания для закрепления метода

| Закрытый текст | Открытый текст |
|--------------------------------|----------------|
| 6/1, 4/10, 7/15, 4/1, 1/5, 3/9 | |
| 1/18, 2/4, 3/9 | |
| 2/1, 4/2, 4/12, 5/2, 2/3 | |

| Открытый текст | Закрытый текст |
|----------------|----------------|
| надежда | |
| слава | |
| душа | |

Задания на тренировку

1. Расшифруй пословицу, подбери подходящую картинку



В одной маленькой деревушке жила злая и скупая женщина с дочкой и падчерицей. Дочку она любила, а падчерица ничем ей не могла угодить. Что ни сделает падчерица — все не так, как ни повернется — все не в ту сторону. Дочка по целым дням на перине валялась, да пряники ела, а падчерице с утра до ночи и присест некогда было: то воды натаскай, то хворосту из лесу привези, то белье на речке выполощи, то грядки в огороде выполи. Знала она и зимний холод, и летний зной, и весенний ветер, и осенний дождь. Потому-то, может, и довелось ей однажды увидеть все двенадцать месяцев разом.

Была зима. Шел январь месяц. Снегу намело столько, что от дверей его приходилось отгребать лопатами, а в лесу на горе деревья стояли по пояс в сугробах и даже качаться не могли, когда на них налетал ветер. Люди сидели в домах и топили печки.

| | | | | | | | | | | | | | | | | | | | |
|-----|-----|-----|-----|--|-----|-----|-----|-----|-----|-----|--|-----|-----|-----|----|-----|-------|-----|-----|
| 1/2 | 3/7 | 10/ | 7/3 | | 1/1 | 12/ | 12/ | 3/1 | 10/ | 9/8 | | 9/7 | 1/2 | 1/3 | 2/ | 12/ | 11/13 | 6/5 | 6/5 |
| 1 | | 2 | | | 2 | 3 | 9 | 2 | | | | 1 | 6 | 2 | | | | | |
| | | | | | | | | | | | | | | | | | | | |

2. Разгадай загадку и выбери правильный ответ

Загадка — метафорическое выражение, в котором один предмет изображается посредством другого, имеющего с ним какое-нибудь, хотя бы отдалённое сходство; на основании этого выражения человек и должен отгадать задуманный предмет. Загадки встречаются у всех народов, на какой бы ступени развития они ни стояли. Пословица и загадка отличаются тем, что загадку нужно отгадать, а пословица — это поучение.

Утром рано по утрам, всех разбудит ...

| | | | | | | |
|-----|-----|-----|-----|------|-----|------|
| 1/6 | 2/5 | 3/3 | 5/4 | 4/12 | 2/4 | 4/12 |
| | | | | | | |

ИЛИ

| | | | | | | | | |
|------|------|-----|------|------|------|-----|-----|-----|
| 4/31 | 2/14 | 1/5 | 2/19 | 5/11 | 2/42 | 3/3 | 5/1 | 1/6 |
| | | | | | | | | |



3. Расшифруй слова в рамочках и вставь в текст

Стихи Маяковского это всегда что-то неожиданное, непредсказуемое и в то же время мощное как удар молотом. Невероятное сочетание слов и ритма бьет пронзительно, и попадает точно в цель. Маяковский писал о многом, но главной темой, вокруг которого строилось все его творчество, было государство и все, что с ним связано. Именно поэтому, у него так много стихов о политике, разных странах, городах, войне, революции и людях, которые во всем это принимали участие.

Разрезая носом воды,

в море пароходы.

Дуют ветры яростные,

Гонят парусные,

Вечером,

а также к ночи,

плавать в море трудно очень.

Все покрыто скалами,

скалами немалыми.

Ближе к суше

еле-еле

днем обходят мели.

6/5 6/6 1/35 4/2

3/9 3/12 6/5 1/9 5/2

6/7 3/3 6/5 2/5 1/2

Шифр Цезаря

Шифр Цезаря заключается в том, что буквы алфавита заменяются буквами того же алфавита, но со сдвигом вправо на 3 позиции. Пример ключа применительно к русскому языку будет выглядеть так:

| Открытый текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |
| 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 | а | б | в |
| Зашифрованный текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

При зашифровывании буква А заменялась буквой Г, Б заменялась на Д, В – Е и так далее. Так, например, «Россия» превращалось в слово «Усххлв».

Задания для закрепления метода

| Закрытый текст | Открытый текст |
|----------------|----------------|
| озхс | |
| сфзря | |
| клпг | |
| езфрг | |

| Открытый текст | Закрытый текст |
|----------------|----------------|
| дерево | |
| куст | |
| трава | |

Задания на тренировку

1. Выбери правильный вариант

Для шифровки сообщения «олцзм» использован шифр Цезаря, какой из приведенных вариантов соответствует зашифрованному сообщению:

- линия
- ласка
- лицей
- лента

2. Зашифруй код

Используя шифр Цезаря, зашифруй пословицу «Не имей сто рублей, а имей сто друзей»

Ответ: _____

3. «Круг Цезаря»

Расшифруйте слово «нултхсеугчлв» используя «Круг Цезаря»



| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Н | У | Л | Т | Х | С | Е | У | Г | Ч | Л | В |
| | | | | | | | | | | | |

Шифр пар

Алфавит **случайным** образом записывают в 2 строки, и шифрования текста происходит заменой буквы на соседнюю по вертикали.

Пример таблицы:

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| в | ы | э | ё | у | ж | и | ф | м | н | о | ъ | к | п | а | р | я |
| е | т | х | й | ш | ю | д | ь | б | щ | з | с | ц | г | ч | л | - |

К примеру, зашифруем слово «Родина», используя шифр пар, получится «Лзидщч».

Задания для закрепления метода

| Закрытый текст | Открытый текст |
|----------------|----------------|
| уцзрч | |
| рдквё | |
| црчъь | |

| Открытый текст | Закрытый текст |
|----------------|----------------|
| ученик | |
| доска | |
| мел | |

Задания на тренировку

1. Расшифруй зашифрованные слова и запиши их в скобках

Так и стали жить вместе дед Цзцзечщ- (_____), сиротка Ичлйщч (_____) да кошка Бшлйщчч (_____). Жили-поживали, добра много не наживали, а на житьё не плакались, и у всякого дело было. Цзцзечщ- (_____) с утра на работу уходил, Ичлйщч (_____) в избе прибирала, похлёбку да кашу варила, а кошка Бшлйщчч (_____) на охоту ходила — мышей ловила. К вечеру соберутся, и весело им.

2. Используя метод «Шифр пар» зашифруй фамилию и имя автора произведения, отрывок которого приведен в задании 1

| | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | | | | | | | | |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

3. Определи, о каком выражении идет речь

Первоначальный смысл выражения «Гвлб-цъзрйщчтвшуд» отходит к соляным промыслам в Верхнекамье. Люди, работающие на переносе соли имели больные уши. Соль носилась с помощью специальных деревянных приспособлений, которое крепилось к спине. Частички соли, выбиваясь из мешка, попадали на уши и разъедали их. Постепенно уши носильщиков соли становились красными и увеличивались в размерах (конечно, не как у скульптуры), поэтому пермяка можно было отличить по большим «соленым» ушам. С тех пор эта поговорка, относящаяся к XIX веку, стала крылатой и подчеркивала самобытность пермяков.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|--|---|---|---|---|---|---|---|--|---|---|---|
| Г | в | л | б | - | ц | | ъ | з | р | й | щ | т | в | | ш | у | д |
| | | | | | | | | | | | | | | | | | |

4. Отгадай загадку и зашифруй ответ используя метод «Шифр пар»

В воде она родится,
Но странная судьба —
Воды она боится
И гибнет в ней всегда.

Ответ: _____ Шифр: _____

Шифр с кодовым словом

Еще один простой способ как в шифровании, так и в расшифровке. Используется кодовое слово (любое слово без повторяющихся букв). Данное слово вставляется впереди алфавита и остальные буквы по порядку дописываются, исключая те, которые уже есть в кодовом слове.

Сначала выбирается кодовое слово, которое пишется впереди, а затем пишут все остальные буквы алфавита (за исключением тех, что использовались в кодовом слове).

Пример с использованием слова шифр:

| Открытый текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | |
| ш | и | ф | р | а | б | в | г | д | е | ё | ж | з | й | к | л | м | н | о | п | с | т | у | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| Зашифрованный текст | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

К примеру, зашифруем слово «Родина», используя шифр с кодовым словом «шифр» получится «Нлаекш».

Задания для закрепления метода

| Закрытый текст | Открытый текст |
|----------------|----------------|
| ыбпбн | |
| алгаь | |
| окбр | |

| Открытый текст | Закрытый текст |
|----------------|----------------|
| осадки | |
| погода | |
| солнце | |

Задания на тренировку

1. Расшифруй зашифрованные слова используя шифр с кодовым словом «шифр»

Россия всегда была не только густонаселенным, но и многонациональным государством. В стране постоянно проживает более 145 млн. граждан.

Они представляют более 160 национальностей, говорящих на собственных языках.

Большинство народностей малочисленны и живут на ограниченной территории.

Только семь народов имеют численность более одного миллиона.

Расшифруй некоторые из них:

| | | | | | | |
|---|---|---|---|---|---|---|
| н | с | о | о | ж | е | б |
| | | | | | | |



| | | | | | |
|---|---|---|---|---|---|
| ц | с | ф | ш | ч | е |
| | | | | | |



| | | | | | | |
|---|---|---|---|---|---|---|
| и | ш | ч | ж | е | н | ы |
| | | | | | | |






| | | | | | |
|---|---|---|---|---|---|
| п | ш | п | ш | н | ы |
| | | | | | |






2. Используя кодовое слово «Пермь» зашифруй пословицу

Открытый текст

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | |
| П | е | р | м | ь | а | б | в | г | д | ё | ж | з | и | й | к | л | н | о | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |

Зашифрованный текст

- Земля народом сильна _____
- Если народ сплочён — все ему нипочём _____
- Где народ, там и правда _____

3. Реши логические задачи. Использую кодовое слово «Пермь» зашифруй ответы

Как написать слово "мышеловка" пятью буквами?

Ответ: _____ Шифр: _____

Какое колесо автомобиля не вращается во время движения?

Ответ: _____ Шифр: _____

Что принадлежит вам, однако другие им пользуются чаще, чем вы?

Ответ: _____ Шифр: _____

Какой город назван в честь большой птицы?

Ответ: _____ Шифр: _____

Каких камней в море нет?

Ответ: _____ Шифр: _____

Что можно приготовить, но нельзя съесть?

Ответ: _____ Шифр: _____

Как написать «сухая трава» четырьмя буквами?

Ответ: _____ Шифр: _____

Цифровое (числовое) кодирование

Кодирование с помощью чисел. Появилось, наверное, вместе с первым алфавитом. Например, поскольку каждая буква знает свое место, то у нее есть номер, а значит, букву можно заменить цифрами: а - 1, к - 12, о - 16 и т.д. Для того чтобы пользоваться цифровым кодом, нужно выучить алфавит либо пользоваться таблицей:

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

Задания для закрепления метода

| Закрытый текст | Открытый текст |
|---------------------|----------------|
| 19, 20, 16, 13 | |
| 14, 6, 2, 6, 13, 30 | |
| 17, 1, 18, 20, 1 | |

| Открытый текст | Закрытый текст |
|----------------|----------------|
| какаду | |
| грация | |
| академия | |

Задания на тренировку

1. Разгадай и зашифруй фамилию автора сказки, которая начинается со слов «Жил старик со своею старухой, У самого синего моря...»

| | | | | | |
|----------------------------|--|--|--|--|--|
| Открытый текст | | | | | |
| | | | | | |
| Зашифрованный текст | | | | | |
| | | | | | |

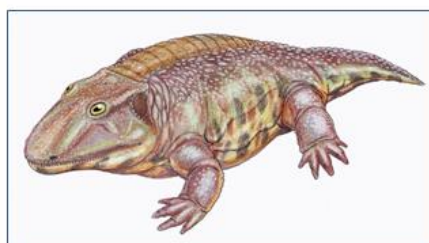
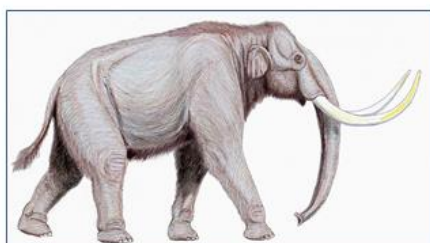
2. Город Пермского края, которому с 2009 г. принадлежит данный герб



| | | | | | | | | |
|----------------------------|----|----|----|----|---|----|----|----|
| Зашифрованный текст | | | | | | | | |
| 19 | 16 | 13 | 10 | 12 | 1 | 14 | 19 | 12 |
| Открытый текст | | | | | | | | |
| | | | | | | | | |

3. Сопоставь зашифрованное название и изображение древнего животного Пермского края

14 1 14 16 15 20








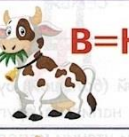




12 1 14 1 12 16 17 19

10 3 1 15 20 16 9 1 3 18

Ребусы

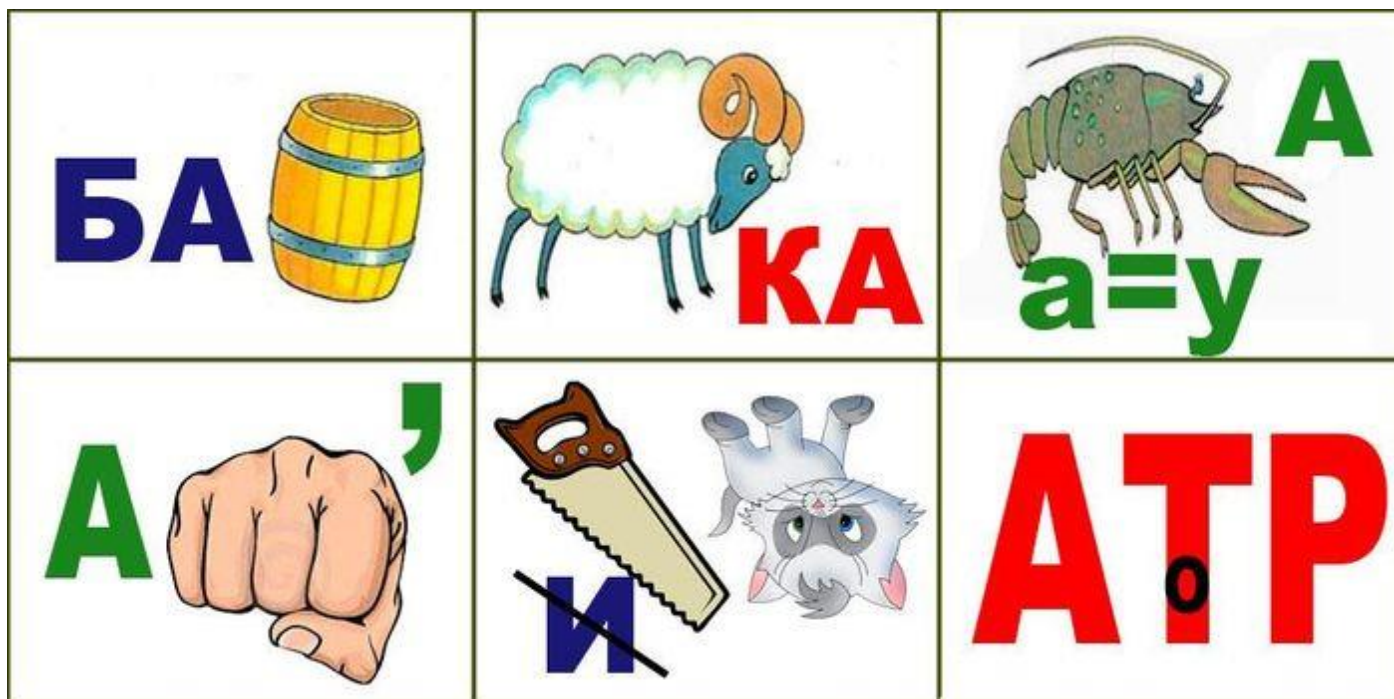
Ребус - это задача, в которой картинками зашифровано слово. Данное определение ребуса уже всем давно известно. Теперь же ребус можно не редко увидеть и в другом контексте, когда говорят о чем-нибудь загадочном и неизведанном. Ребус играл очень важную роль в образовании письменности всех веков и народов, ведь даже пещерные люди писали на древних скалах рисунками, которые понимали только они, позже эти рисунки переходили впервые буквы названий этих рисунков.

| | | | |
|---|---|---|--|
|  | Запятая слева от рисунка означает, что нужно убрать первую букву. Если стоят две запятые - убирают две первые буквы. ГРОЗА - убрали Г, получилось РОЗА |  | Для удаления букв внутри слова их записывают над изображением и перечёркивают. МОНИТОР - убрали НИ, получилось МОТОР |
|  | Запятая справа от рисунка означает, что нужно убрать последнюю букву. Если стоят две запятые - убирают две последние буквы. ВОЛК - убрали К, получилось ВОЛ |  | Для изменения порядка букв в слове над ним ставят цифры, которые определяют новый порядок следования букв. КОТ - получилось ТОК |
|  | Если справа или слева от рисунка стоит одна или несколько букв - это значит, что эти буквы следует добавить. ПО + ДУШ + КА = ПЛОДУШКА |  | Если картинка перевернута вверх ногами, это значит, что слово читается справа налево. КОТ - получилось ТОК |
|  | Зачёркнутая буква слева от рисунка означает, что нужно убрать первую букву. ГРОЗА - убрали Г, получилось РОЗА |  | Постановка знака «=» между двумя буквами служит для указания замены одной из этих букв на другую. |
|  | Зачёркнутая буква справа от рисунка означает, что нужно убрать последнюю букву. ВОЛК - убрали К, получилось ВОЛ |  | На это же указывает зачёркивание одной буквы и помещение рядом с ней другой буквы. КОРОВА = КОРОНА |

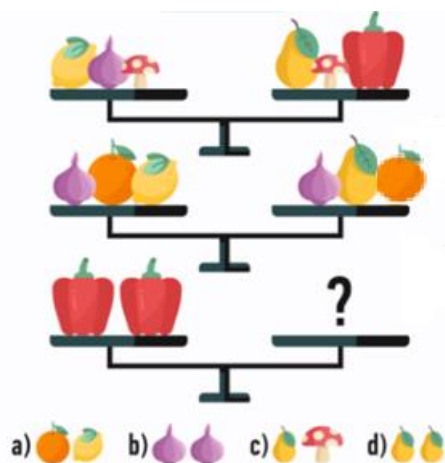
| | | | |
|---|--|---|---|
|  | Если предметы или буквы изображены один в другом, то их названия читаются с прибавлением предлога «в»: ВОЛК |  | Если большая буква составлена из маленьких, повторяющихся несколько раз букв, то при чтении используется предлог «из» (перед или между названий). ИЗБА |
|  | Если отдельно стоящие буквы зачёркнуты, то их необходимо читать с прибавлением частицы «не»: НЕУЧ |  | Буквы, разделённые чертой, читаются так: ФОНАРИ |
|  | Вместо картинки могут использоваться числа. СЕМЬ + Я = СЕМЬЯ |  | Или так: НАУКА |
|  | Если поверх одной (большой) буквы несколько раз написана другая (маленькая), то при чтении используется предлог «по» (впереди или между названий). ПОЯС |  | Одна буква за другой читаются так: ЗАЯЦ |

Задания на тренировку

1. Разгадай ребусы



Ребусы бывают не только на разгадывание слов, но и математические. Разберем пример ребуса, для решения которого необязательно заменять рисунки цифрами, но важно уметь строить уравнения.

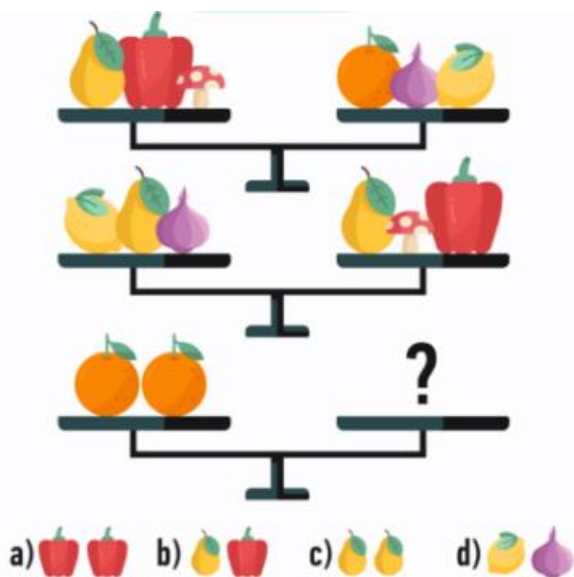


От решающего требуется определить, какие фрукты и в каком количестве должны быть на последней чаше.

Принцип решения: если с правой и левой чаши на вторых весах мы уберем повторяющиеся овощи, фрукты это лук и апельсин, то слева останется лимон, а справа-груша. Получается лимон = груша. Аналогично на первых весах убираем повторы, т.е гриб. Нам уже известно, что лимон = груша, поэтому их также

зачеркиваем. В итоге получим, лук = перец. Так как на последних весах слева два перца, соответственно, справа должно быть два лука.

2. Определи что должно лежать на последней чаше весов и в каком количестве



Ответ: _____

Рассмотрим ребус в котором работаем с конкретными числами.

$$\text{Blue butterfly} + \text{Red butterfly} + \text{Blue butterfly} + \text{Red butterfly} = 58$$

$$\text{Red butterfly} + \text{Green butterfly} + \text{Red butterfly} + \text{Green butterfly} = 56$$

$$\text{Blue butterfly} + \text{Blue butterfly} + \text{Blue butterfly} = 39$$

$$\text{Red butterfly} + \text{Blue butterfly} + \text{Green butterfly} + \text{Blue butterfly} = ?$$

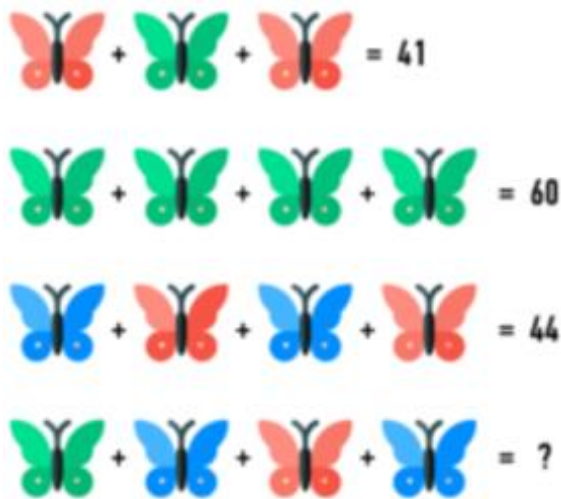
Каждой бабочке соответствует определенное число. Задача определить эти числа и решить последний пример.

Принцип решения: проще начать с третьего равенства $39:3=13$. Синяя бабочка соответствует числу 13. $13*2 + \text{две красные бабочки} = 58$. Две красные бабочки = $58 - 26 = 32$. Одна красная = $32:2 = 16$

Вычислим чему равна зеленая бабочка. Во второе равенство подставим уже известные нам значения: $32 + 2x = 56$, $2x = 56 - 32 = 24$. Значит $x = 12$

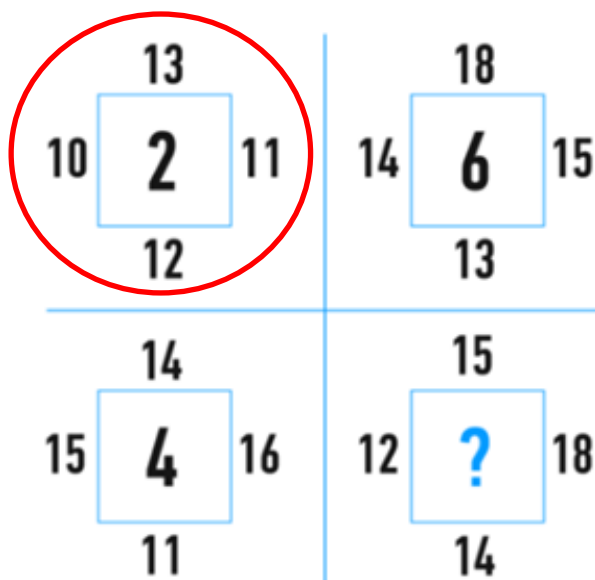
Подставляем полученные числа в последний пример: $16 + 13 - 12 + 13 = 30$

3. Реши последнее равенство



Ответ: _____

Ребус который решается способом подбора.

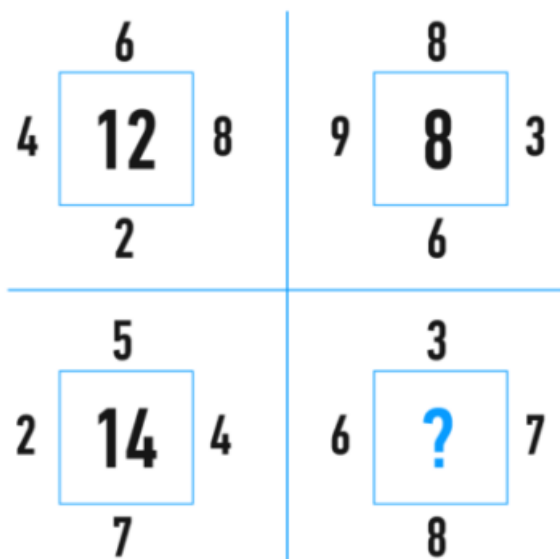


Нужно определить число спрятанное за вопросительным знаком.

Принцип решения: необходимо определить последовательность математических действий с предоставленными числами, которые в результате дают число написанное в центре. Порядок сложения, вычитания во всех примерах одинаков, применив

который можно решить последний пример. Из числа находящегося над квадратом вычитаем число, находящееся под ним. Из числа находящегося справа от квадрата вычитаем число, находящееся слева от него. Сумма полученных чисел будет равна числу в центре квадрата: т.е. $(13-12)+(11-10)=2$.

4. Найди число



Ответ: _____

Табличный метод

Алфавит записан в таблицу. Строчки таблицы пронумерованы, а столбцам присвоен символ. Зашифровать букву значит присвоить ей код, где на первом месте указываем номер строки, на втором месте указываем символ.

«радость» = «3⊗ 1○ 1□ 3⋈ 4○ 4□ 5⊗»

| | | | | | | |
|---|---|---|---|---|---|---|
| | ○ | □ | △ | ⋈ | | ⊗ |
| 1 | А | Б | В | Г | Д | Е |
| 2 | Ё | Ж | З | И | Й | К |
| 3 | Л | М | Н | О | П | Р |
| 4 | С | Т | У | Ф | Х | Ц |
| 5 | Ч | Ш | Щ | Ъ | Ы | Ь |
| 6 | Э | Ю | Я | . | ! | ? |

Задания для закрепления метода

| Открытый текст | Закрытый текст |
|----------------|----------------|
| победа | |
| Обнинск | |
| лицей | |

Задания на тренировку

1. Используя табличный метод шифрования напиши письмо Дедушке морозу



Глоссарий

Закрытый текст – данные, полученные после применения метода шифрования

Ключ – секретная информация, используемая при шифровании/расшифровании данных

Код – представление какого либо слова (информации) в более короткой последовательности символов

Криптография – тайнопись

Метод – путь достижения цели

Открытый текст – текст, получившийся в результате расшифровки

Шифр – порядок (алгоритм) преобразования информации

Ответы

Книжный шифр

1. Утро вечера мудренее, картинка 1
2. Будильник
3. Разрезая носом воды,

Ходят в море пароходы.

Дуют ветры яростные,
гонят **лодки** парусные,

Вечером,

а также к ночи,

плавать в море трудно очень.

Все покрыто скалами,
скалами немалыми.

Ближе к суше

еле-еле

даже

днем обходят мели.

Шифр Цезаря

1. лицей
2. Рз лпзм фхс уцдозм, г лпзм фхс жуцкзм
3. Криптография

Шифр пар

1. Кокованя, Дарёна, Мурёнка

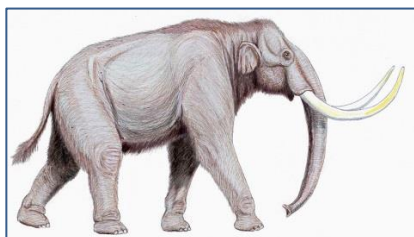
2. Бажов Павел
3. пермяк соленые уши
4. соль, ъзрф

Шифр с кодовым словом

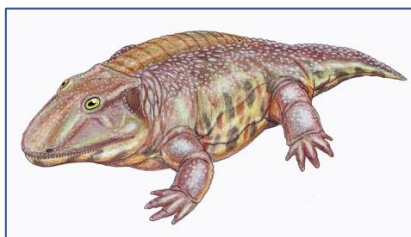
1. русские, татары, башкиры, чувашаи
2. Гаизя йпнкьки одзыйп. Аозд йпнкь олзкцбй - роа аит йдлкцби. Мъа йпнкь, спи д лнпрьп.
3. кошка – жкчжп, запасное – гплпойка, имя – дия, Орёл – Кнбз, сухих – отфдф, уроки – тнкжд, сено – оайк.

Цифровое кодирование

1. Пушкин-17,21,26,12,10,15
2. Соликамск
- 3.



Мамонт



Камакопс



Ивантозавр

Ребусы

1. бабочка, баранка, рука, акула, платок, автор
2. с
3. 46
4. 12