



Задания, ответы и критерии оценивания

Требования к оформлению заданий. При проверке заданий учитывается не только ответ, но и само решение. Важно оформлять решения во всех заданиях. Ответы без решения оцениваются не более чем в 1 балл.

Задача 1 (Максимум 10 баллов)

Исходный текст: "ШИФРУЙПОКАШИФРУЕТСЯ". Текст разбивается на части по 5 букв. В каждой части буквы нумеруются слева направо от 1 до 5 и затем переставляются по правилу: $1 \rightarrow 4, 2 \rightarrow 3, 3 \rightarrow 5, 4 \rightarrow 1, 5 \rightarrow 2$. Затем текст зашифровывается 9 раз. Опишите закономерности данного шифра. Какой текст получит адресат?

Ответ: «РИФШУКПОЙАРИФШУЯТСЕХ»

Решение: Чтобы решить эту задачу, необходимо выполнить указанные шаги шифрования для исходного текста "ШИФРУЙПОКАШИФРУЕТСЯ". Первым шагом является разбиение текста на части по 5 букв и перестановка букв в каждой части в соответствии с указанным правилом. Затем текст шифруется 9 раз.

Шаги решения:

- 1. Разбиение текста и первичное шифрование:** Исходный текст: "ШИФРУЙПОКАШИФРУЕТСЯ".
 - Разбиваем на части по 5 букв: "ШИФРУ", "ЙПОКА", "ШИФРУ", "ЕТСЯ" (последняя часть неполная).
 - Перестановка по правилу ($1 \rightarrow 4, 2 \rightarrow 3, 3 \rightarrow 5, 4 \rightarrow 1, 5 \rightarrow 2$):
 - "ШИФРУ" \rightarrow "РУИШФ"
 - "ЙПОКА" \rightarrow "КАПЙОР"
 - "ШИФРУ" \rightarrow "РУИШФ"
 - "ЕТСЯХ" (неполная часть) \rightarrow "ЯХТЕС"
- 2. Повторное шифрование 9 раз:** так как процедура шифрования циклична и период составляет 5 (количество перестановок до того, как текст вернется в исходное положение), то после 5 шифрований текст вернется в исходное положение. Таким образом, 9 шифрований эквивалентны 4 шифрованиям ($9 \bmod 5 = 4$). Значит, нам нужно зашифровать текст еще 3 раза после первого шифрования.
- 3. Выполнение оставшихся шифрований:** повторяем процедуру перестановки еще 3 раза.
- 4. Финальный текст:** Текст после 4-го шифрования является результатом, который получит адресат.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	5	Верно описано правило сокрытия.
3	7	В ответе одна неправильная буква. Правило описано.
4	10	Ответ полностью совпадает. Правило описано.

Задание 2 (Максимум 20 баллов)

Выбрано натуральное число C . Найдены числа $C_1=[C]_8$, $C_2=[C/3]_8$ и $C_3=[C/6]_8$, где $[X]_8$ — остаток от деления целой части числа X на 8. Если известно, что $C_1=5$ и $C_2=4$, найдите все возможные значения числа C_3

Ответ: 2,6

Решение:

- C — натуральное число.
- $C_1=[C]_8$ — остаток от деления целой части C на 8.
- $C_2=[C/3]_8$ — остаток от деления целой части $C/3$ на 8.
- $C_3=[C/6]_8$ — остаток от деления целой части $C/6$ на 8.

Известно, что $C_1=5$ и $C_2=4$. Необходимо найти все возможные значения C_3 .

1. Рассмотрим $C_1=5$:

Поскольку C_1 — это остаток от деления C на 8, C может быть любым числом вида $8k+5$, где k — целое число.

2. Рассмотрим $C_2=4$:

Аналогично, C_2 — это остаток от деления $C/3$ на 8. Следовательно, целая часть числа $C/3$ может быть любым числом вида $8k+4$, где k — целое число. Переписывая, получаем $C=3 \times (8k+4)$.

3. Найдем общие значения для C , удовлетворяющие обоим условиям:

- $C=8k+5$
- $C=24k+12$

Необходимо найти такие значения C , которые удовлетворяют обоим уравнениям.

Таких чисел не окажется, потому что вторая формула исходит из **целой части** числа. Поэтому необходимо к ней применить сдвиг $+1$ или -1 . Для этих условий требуемый сдвиг: $+1$.

4. Рассчитаем C_3 :

После нахождения подходящих значений C , используем их для расчета $C_3=[C/6]_8$.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	7	Ученик правильно понимает задачу и уравнения для C_1 и C_2 . Ученик корректно записывает уравнения для C_1 и C_2 и понимает их значение.
3	10	Ученик находит уравнение для C , удовлетворяющее условиям для C_1 и C_2 .
4	15	Ученик правильно находит значения C , которые удовлетворяют обоим условиям. .
5	20	Ученик правильно вычисляет все возможные значения C_3 , основываясь на найденных значениях C .

Задание 3 (Максимум 20 баллов)

Решите в натуральных числах уравнение $15m - 4n = 1$, где m и n лежат в пределах от 1 до 100

Ответ:

1. (3,11)
2. (7,26)
3. (11,41)
4. (15,56)
5. (19,71)
6. (23, 86)

Решение:

Диофантово уравнение вида $ax - by = c$, где a, b, c — известные целые числа, а x, y — неизвестные, которые нужно найти.

Если предположить, что ваше уравнение должно выглядеть как $15m - 4n = 1$, где m и n — натуральные числа, лежащие в пределах от 1 до 100, тогда мы можем решить его, перебирая значения m и n и проверяя, удовлетворяют ли они уравнению.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	10	Ученик понимает задачу и может правильно записать уравнение, понимает концепцию линейного диофантова уравнения и методы его решения.
3	15	Ученик применяет метод перебора или другой подход для нахождения частичного решения задачи.
4	20	Ответ полностью совпадает. Правило описано.

Практическое задание. (Максимум 50 баллов)

Вам предстоит создать шифр, похожий на шифр Виженера, но использующий несколько ключей одновременно. Каждый ключ применяется в соответствии с определенным алгоритмом. Требуется описать алгоритм подбора ключей, зашифровывания и расшифровывания сообщения и показать пример. Описание классического шифра Виженера:

Принцип работы(для латинского алфавита)

Шифр Виженера основан на использовании таблицы алфавитов, называемой таблицей Виженера. В этой таблице каждая строка сдвигается на одну позицию относительно предыдущей, создавая 26 возможных шифров Цезаря (для алфавита из 26 букв).

Ключ

Шифр Виженера использует ключевое слово или фразу, которая повторяется, пока её длина не сравняется с длиной открытого текста. Каждая буква ключа определяет, какой ряд таблицы Виженера использовать для шифрования соответствующего символа открытого текста.

Шифрование

1. **Выберите ключевое слово:** Например, ключ "KEY".
2. **Повторите ключевое слово:** Повторяйте ключ до тех пор, пока его длина не станет равной длине сообщения. Например, если сообщение "HELLO WORLD", ключ станет "KEYKEYKEYK".

Примените таблицу Виженера: Используйте букву ключа, чтобы определить строку, и букву открытого текста, чтобы определить столбец. Точка пересечения в таблице даст вам букву зашифрованного текста.

1. Разработка Множественного Шифра:

- Выбор набора ключей и разработка алгоритма их применения.
- Реализация шифрования, включая переключение между ключами по заданному алгоритму.

2. Анализ и Взлом Шифра:

- Использование методов криптоанализа для выявления паттернов применения ключей.
- Расшифровка текста, используя обнаруженные закономерности.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Ответ без решения.
2	10	Понимание подходов шифрования при использовании шифра Виженера.
3	15	Не полное и точное решение задачи.
4	25	Ученик почти полностью и правильно решает задачу, минимально ошибаясь в вычислениях или записи результата.
5	50	Ученик полностью и правильно решает задачу.