Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

7-8 классы **Заключительный этап** **2023-2024**

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: "НАСЖДЁТГОДДРАКОНА". Текст разбивается на части по 5 букв. В каждой части буквы нумеруются слева направо от 1 до 5 и затем переставляются по правилу: 1 → 4, 2 → 3, 3 → 5, 4 → 1, 5 → 2. Затем текст зашифровывается 9 раз. Какой текст получит адресат?

Ответ: с добавлением символов 'Х' для поддержания групп по 5 букв, полученный текст: "ЖАСНДОТГЁДКРАДОХАХНХ"

Решение: Для решения этой задачи нужно выполнить несколько последовательных шагов:

1. Разбить исходный текст на части по 5 букв: "НАСЖД", "ЁТГОД", и так далее.
2. Переставить буквы в каждой группе согласно правилу:
1 → 4, 2 → 3, 3 → 5, 4 → 1, 5 → 2.
3. Зашифровать полученный текст 9 раз, повторяя шаг 2 каждый раз.

Мы можем выполнить шифрование для одного цикла и затем просто повторить процедуру 9 раз.

Начнем с первой группы букв "НАСЖД":

- "Н" на позиции 1 перейдет на позицию 4,
- "А" на позиции 2 перейдет на позицию 3,
- "С" на позиции 3 перейдет на позицию 5,
- "Ж" на позиции 4 перейдет на позицию 1,
- "Д" на позиции 5 перейдет на позицию 2.

Таким образом, новая последовательность будет "ЖДАНС".

Применяем ту же логику к другим группам букв "ЁТГОД" и "ДРАКОН", и после одного шифрования мы получим "ГДЁОТ" и "КОНДР" соответственно.

После того как мы получим результат первого шифрования, нам нужно повторить процесс еще 8 раз. Однако, поскольку шифрование циклично с периодом 5 (количество перестановок до того, как текст вернется в исходное положение), то после 5-ти шифрований текст снова будет "НАСЖДЁТГОДДРАКОНА". Таким образом, если мы шифруем текст 9 раз (что равно 5 + 4), это будет эквивалентно 4 шифрованиям. То есть, чтобы узнать конечный результат, достаточно зашифровать текст 4 раза.

После выполнения всех шагов, мы получим текст, который адресат увидит после дешифровки.

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 $C_1=2$ и $C_2=3$, найдите все возможные значения числа C_3

Ответ: 1,5

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 $C_1=2$ и $C_2=3$. Необходимо найти все возможные значения C_3.

1. **Рассмотрим $C_1=2$**:
   Поскольку C_1 — это остаток от деления C на 8, C может быть любым числом вида 8k+2, где k — целое число.
2. **Рассмотрим $C_2=3$**:
   Аналогично, C_2 — это остаток от деления C/3 на 8. Следовательно, целая часть числа C/3 может быть любым числом вида 8k+3, где k — целое число. Переписывая, получаем C=3×(8k+3).
3. **Найдем общие значения для C**, удовлетворяющие обоим условиям:
   - C=8k+2
   - C=24k+9

   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)*

Нам предоставлена математическая модель используемого метода шифрования, воспользуйтесь данным знанием, и расшифруйте сообщение:
Формула шифрования для нечетных позиций: $C_i=(25-P_i+1) \bmod 26$

- Формула шифрования для четных позиций: $C_i = P_i$ (без изменений)
- Инверсия порядка результата после применения шифра.
- P_i и C_i определены так же, как и ранее.

Шифротекст: crwvmciix
Ответ: discovery

Решение:

1. Преобразование каждой буквы в её позицию в алфавите: a=0, b=1, ..., z=25.
2. Применение обратной операции шифрования для нечётных и чётных позиций.
   - Для нечётных позиций: $P_i=(25-C_i+1) \bmod 26$
   - Для чётных позиций: $P_i=C_i$
3. Инверсия порядка символов в полученном результате.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	10	Верно описано правило сокрытия.
3	14	В ответе одна неправильная буква. Правило описано.
4	20	Задание решено полностью без ошибок

Практическое задание. *(Максимум 50 баллов)*

Ваш друг, увлекающийся историей, отправил вам зашифрованное сообщение, используя Шифр Цезаря, один из самых старых известных методов шифрования. В этом шифре каждая буква в тексте заменяется другой буквой, которая находится на фиксированное число позиций левее или правее в алфавите. Например, сдвиг на 3 позиции вправо превращает букву A в D, B в E и так далее.
Вот зашифрованное сообщение: "YRIRY GJB CNFFJBEQ EBGGRA"
Ваша задача:

1. Расшифровать сообщение, зная, что использовался сдвиг вправо.
2. Определить, на сколько позиций производился сдвиг.
3. Написать оригинальное сообщение.

(Алфавит латинский, и он циклический, то есть после Z снова идет A.)
Ответ:

1. Расшифрованное сообщение: "LEVEL TWO PASSWORD ROTTEN".
2. Сдвиг, использованный для шифрования: 13 позиций вправо.
3. Оригинальное сообщение: "LEVEL TWO PASSWORD ROTTEN"

Решение: Для решения этой задачи нам нужно расшифровать сообщение, используя Шифр Цезаря. Начнем с попытки сдвига на разные количества позиций в алфавите, пока не найдем правильный сдвиг, который делает текст понятным.

Зашифрованное сообщение: "YRIRY GJB CNFFJBEQ EBGGRA"

Попробуем различные сдвиги. После попыток с различными сдвигами, мы видим, что при сдвиге на 13 позиций влево зашифрованное сообщение "YRIRY GJB CNFFJBEQ EBGGRA" превращается в читаемый текст: "LEVEL TWO PASSWORD ROTTEN".

Ответы на задачу:

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	25	Верно описано правило сокрытия.
3	35	В ответе одна неправильная буква. Правило описано.
4	50	Ответ полностью совпадает. Правило описано.

Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

9-10 классы **Заключительный этап** **2023-2024**

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 → 4, 2 → 3, 3 → 5, 4 → 1, 5 → 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 → 4, 2 → 3, 3 → 5, 4 → 1, 5 → 2):
     - "ШИФРУ" → " РУИШФ"
     - "ЙПОКА" → "КАПЙОР"
     - "ШИФРУ" → " РУИШФ"
     - "ЕТСЯХ" (неполная часть) → " 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 шифровании текст вернется в исходное положение. Таким образом, 9 шифровании эквивалентны 4 шифрованиям (9 mod 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×(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 шифрованного 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.

Многопрофильная инженерная олимпиада «Звезда»
«Информационная безопасность»

11 класс **Заключительный этап** **2023-2024**

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)*

Найдите все тройки натуральных чисел *(x, y, z)*, такие что $5^x + 5^y = z^2$ *и* $x, y < 10, z <= 50$

Ответ: Решений в натуральных числах нет.

Решение: Для решения этой задачи нам нужно найти все тройки натуральных чисел (x,y,z), удовлетворяющие условию $5^x+5^y=z^2$, при этом x, y<10 и z≤50.
Мы можем решить эту задачу, перебрав все возможные значения x и y в диапазоне от 1 до 9 (поскольку они меньше 10) и проверив, удовлетворяет ли соответствующее значение z условию $z^2=5^x+5^y$ и z≤50.

1. Для каждой пары x и y, вычислить $z^2=5^x+5^y$.
2. Проверить, является ли z целым числом, и удовлетворяет ли оно условию $z \leq 50$.

Таких троек не окажется.
Объяснение следующее:
При x>1 и/или y>1 сумма двух чисел оканчивается на 30 или 50. Натуральный квадрат с нулем на конце может быть только квадратом круглого числа, но в таком случае он будет заканчиваться на 00, из чего следует отсутствие натуральных решений в указанном диапазоне.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	3	Ученик понимает задачу и определяет ограничения для x, y и z, правильно формулирует уравнение $5^x+5^y=z^2$ и понимает его математический смысл.
3	7	Ученик показывает отсутствие решений путем полного перебора всех вариантов без указания свойств суммы и квадрата числа.
4	10	Ученик указывает свойства совпадения суммы и квадрата числа, получив вывод с отсутствием ответа в натуральных числах.

Задание 2 *(Максимум 20 баллов)*

Решите в натуральных числах уравнение $17m - 5n = 1$, где m и n лежат в пределах от 1 до 100

Ответ:

1. (3,10)
2. (8,27)
3. (13,44)
4. (18,61)
5. (23,78)
6. (28,95)

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 $17m-5n=1$, 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.

Задание 3 *(Максимум 20 баллов)*

Дана последовательность s_n, где s_n - последняя цифра суммы квадратов первых n натуральных чисел, т.е. s_n - последняя цифра числа $1^2+2^2+3^2+...+n^2$. Определите периодичность этой последовательности. Создайте первую перестановку из последовательных уникальных цифр s_n и определите, образуют ли последующие перестановки периодическую последовательность.

Ответ: НЕ ОБРАЗУЕТ ПЕРЕОДИЧЕСКУЮ ПОСЛЕДОВАТЕЛЬНОСТЬ

Решение:

Для определения периодичности последовательности s_n, которая является последней цифрой суммы квадратов первых n натуральных чисел, нам нужно

вычислить эти суммы для различных значений n и наблюдать за поведением последних цифр этих сумм.

Последовательность задается как $1^2+2^2+3^2+\cdots+n^2$ (мы рассматриваем только последнюю цифру этой суммы).

решить эту задачу вручную, следуя следующим шагам:

1. Вычислить последние цифры сумм квадратов для первых нескольких n, например, от 1 до 50.
2. Наблюдать за последовательностью этих цифр и искать периодичность.
3. Определить уникальные цифры в начале этой последовательности (первая перестановка).
4. Следить за повторением этой перестановки в дальнейшем.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	5	Ученик понимает задачу и может правильно описать последовательность s_n. Ученик корректно вычисляет последние цифры сумм квадратов для первых нескольких n и начинает анализировать последовательность.
3	10	Ученик выявляет уникальные цифры в начале последовательности и формирует первую перестановку.
4	15	Ученик анализирует последовательность на предмет периодичности и частично определяет её, но делает некоторые ошибки или не полностью исследует периодичность.
5	20	Ученик полностью и правильно решает задачу, определяя периодичность последовательности и полностью исследуя её свойства.

Практическое задание. *(Максимум 50 баллов)*

Необходимо разработать и описать алгоритм с выбранными входными параметрами шифра RSA, один из основных методов асимметричного шифрования. Задача включает в себя три основных этапа: генерацию ключей, шифрование и дешифрование сообщений. Вы должны продемонстрировать понимание математических принципов, лежащих в основе RSA, а также умение применять эти принципы на практике.

RSA (названный в честь его создателей Рональда Ривеста, Ади Шамира и Леонарда Адлемана) является одним из первых и наиболее широко используемых алгоритмов асимметричного шифрования. Асимметричное шифрование означает использование

различных ключей для шифрования и расшифровки данных. В RSA используются два ключа: открытый ключ для шифрования и закрытый ключ для расшифровки.

Процесс работы RSA включает в себя следующие шаги:

Генерация ключей

1. Выбор двух больших простых чисел (*p* и *q*): Эти числа генерируются и хранятся в секрете.

2. Вычисление произведения (*n = p * q*): Число n используется как часть обоих ключей и определяет длину ключа RSA.

3. Вычисление функции Эйлера (*φ(n) = (p-1) * (q-1)*): Эта функция используется для генерации ключей.

4. Выбор открытого ключа (e): Число e должно быть взаимно простым с φ(n) и обычно выбирается из набора стандартных значений (например, 65537).

5. Вычисление закрытого ключа (d): Число d вычисляется как мультипликативно обратное к e по модулю *φ(n)*, т.е. такое, что *d * e ≡ 1 (mod φ(n))*.

После этого открытый ключ *(e, n)* может быть распространен, а закрытый ключ *(d, n)* должен быть сохранен в секрете.

Шифрование и расшифровка

1. Шифрование: Чтобы зашифровать сообщение M, отправитель использует открытый ключ получателя. Сообщение преобразуется в число m, меньшее n (например, с использованием кодировки ASCII). Затем зашифрованное сообщение C вычисляется по формуле: *C = m^e mod n*.

2. Расшифровка: Чтобы расшифровать сообщение C, получатель использует свой секретный ключ (d). Оригинальное сообщение m восстанавливается путем вычисления: *m = C^d mod n*. После этого m преобразуется обратно в текст сообщения.

Решение:

1. **Разработка Алгоритма Генерации Ключей:**
   - Выбор двух больших простых чисел p и q.
   - Вычисление модуля $n=p\times q$, который будет частью обоих ключей.
   - Вычисление функции Эйлера: $\phi(n)=(p-1)\times(q-1)$.
   - Выбор открытой экспоненты e, которая взаимно проста с $\phi(n)$.
   - Вычисление закрытой экспоненты d, такой что $d\times e$ дает остаток 1 при делении на $\phi(n)$.
2. **Реализация Алгоритмов Шифрования и Дешифрования:**
   - Шифрование: Преобразование сообщения в число и возведение его в степень e по модулю n.
   - Дешифрование: Возведение зашифрованного числа в степень d по модулю n.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	10	Правильный выбор простых чисел. Корректность вычисления открытого и закрытого ключей.
3	15	Ученик выявляет уникальные цифры в начале последовательности и формирует первую перестановку.
4	25	Правильность алгоритма шифрования, включая применение открытого ключа.
5	50	Ученик полностью и правильно решает задачу.