



Многопрофильная инженерная олимпиада «Звезда» «Информационная безопасность»

11 классы

Заключительный этап

2024-2025

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.

Задание 1 (максимум 10 баллов)

Определите какое равенство точнее $49/13 = 3,77$ или $\sqrt{14} = 3,74$.

Ответ: $49/13 = 3,77$ более точное

Решение:

- 1) Найдём значение выражений с большим числом знаков после запятой

$$49/13 = 3,76923$$

$$\sqrt{14} = 3,74166$$

- 2) Вычисли предельные абсолютные погрешности, округляя с избытком

$$\Delta_1 = |3,76923 - 3,77| = 7,7 \cdot 10^{-4} \leq 0,0008$$

$$\Delta_2 = |3,74166 - 3,74| = 1,66 \cdot 10^{-3} \leq 0,002$$

- 3) Вычислим предельные относительные погрешности

$$\delta_1 = \frac{0,0008}{3,77} \approx 2 \cdot 10^{-4} = 0,02\%$$

$$\delta_2 = \frac{0,002}{3,74} \approx 5 \cdot 10^{-4} = 0,05\%$$

Т.к. δ_1 меньше δ_2 , значит равенство $49/13 = 3,77$ более точное.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	5	Верно описан метод расчета
3	7	В ответе допущена ошибка. Метод расчета описан верно.
4	10	Ответ полностью совпадает. Метод расчета описан верно.

Задание 2 (максимум 20 баллов) Сколько существует способов размещения на полке девяти книг, если среди них имеется трёхтомник (трёхтомником считается набор из трёх книг, расположенных в порядке возрастания нумерации)?

Ответ: 5040

Решение: Для подсчета числа комбинаций используем формулу перестановки $P=n!$, где n – общее число книг. Но имеется трёхтомник, значит будем считать его за одну книгу, т.к. предполагается, что три книги из одного трёхтомника должны располагаться рядом и в порядке возрастания. Тогда $n = 7$, а $7! = 5040$

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	13	Метод решения не учёл однозначное расположение томов в трёхтомнике
3	17	Метод решения учёл однозначное расположение томов в трёхтомнике. Допущена ошибка в расчётах
4	20	Ответ дан верно. Метод решения учёл однозначное расположение томов в трёхтомнике

Задание 3 (максимум 20 баллов)

Шифр Цезаря, также известный как шифр сдвига, код Цезаря — один из самых простых и наиболее широко известных методов шифрования. 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.

Необходимо зашифровать текст «Квадратное уравнение», если сдвиг совершается вправо на 83. Алфавит используется русский без потерь букв (т.е. е и ё разные символы).

Ответ: Ытрфбргюях дбртюющих

Решение: Перебирать все 83 комбинации или отсчитывать 83 шага нет необходимости. При таком методе алфавит будет начинаться с начала несколько раз, т.к. $83 > 33$. Для нахождения последнего цикла прохода, найдем остаток от деления $83/33$, это будет равняться 17. Таким образом необходимо делать 17 шагов от расположения буквы.

Критерии оценивания

Номер критерия	Количество баллов	Описание
1	1	Написан верный ответ без решения.
2	12	Решено методом перебора. Ответ верный.
3	17	Правильно описано правило упрощенного решения, в ответе допущена одна ошибка .
4	20	Ответ полностью совпадает. Правильно описано правило упрощенного решения.

Практическое задание. (Максимум 50 баллов)

Шифрование текста основано на следующем алгоритме:

- 1) Текст разбивается на 2 блока одинаковой длины и переводится в их численное значение
- 2) Правый блок становится новым левым блоком, а новый правый блок рассчитывается как $L0 + f1(R0)$,
где $L0$ - старое значение левого блока
 $R0$ – старое значение правого блока

$f_1(R_0)$ – некоторая заранее определённая функция с данными из R_0 , содержащее некоторые ключи k

3) Этап 2 повторяется несколько повторов (раундов)

4) Полученный набор чисел переводят обратно в текст

Пример:

Используются буквы русского алфавита, представленные своими индексами (А- 0, Б-1 и т.д.), необходимо зашифровать текст «Буря» 2-мя раундами. $f(x_1, x_2) = (\max\{k_i, x_1\}, x_1 * x_2 + k_i)$, $k_1=19$, $k_2=10$

Буря = (1,20,17,32)

$L_0=1,20$ $R_0=17,32$

$L_1 = R_0$ (17,32) $R_1 = L_0 + f_1(R_0) = (1,20) + (\max\{19,17\}, 17*32+19) = (20,22)$

$L_2 = R_1$ (20,22) $R_2 = L_1 + f_2(R_1) = (17,32) + (\max\{10,20\}, 20*22+10) = (4,20)$

Зашифрованный текст $Y = (20,22,4,20) = \text{УХДУ}$

Задание: необходимо зашифровать текст «Укор» 3-мя раундами, если $f(x_1, x_2) = (\min\{k_i, x_1\}, x_1 + x_2 * k_i)$, $k_1=8$, $k_2=11$, $k_3=14$. Таблица перевода букв в цифры представлена ниже.

А	0	К	11	Х	22
Б	1	Л	12	Ц	23
В	2	М	13	Ч	24
Г	3	Н	14	Ш	25
Д	4	О	15	Щ	26
Е	5	П	16	Ъ	27
Ё	6	Р	17	Ы	28
Ж	7	С	18	Ь	29
З	8	Т	19	Э	30
И	9	У	20	Ю	31
Й	10	Ф	21	Я	32

Ответ: ЩЛИЩ

Решение:

Укор = (20,11,15,17)

$L_0=20,11$ $R_0=15,17$

$L_1 = R_0$ (15,17) $R_1 = L_0 + f_1(R_0) = (20,11) + (\min\{8,15\}, 15+17*8) = (28,30)$

$L_2 = R_1$ (28,30) $R_2 = L_1 + f_2(R_1) = (15,17) + (\min\{11,28\}, 28+30*11) = (26,12)$

$L_3 = R_2$ (26,12) $R_3 = L_2 + f_3(R_2) = (28,30) + (\min\{14,26\}, 26+12*14) = (9,26)$

Зашифрованный текст $Y = (26,12,9,26) = \text{ЩЛИЩ}$

Номер критерия	Количество баллов	Описание
1	1	Ответ без решения
2	15	Задача решена без использования метода шифрования
3	25	Используется метод шифрования, но в ответе допущена ошибка
4	50	Задание решено правильно, используя метод шифрования