ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТРУДУ (ТЕХНОЛОГИИ)

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

ТЕОРЕТИЧЕСКИЙ ТУР

9 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и кейс-задания.

Время выполнения заданий теоретического тура 3 астрономических часа (180 минут).

Часть предложенных Вам заданий может быть представлена в электронном виде. Для удобства работы с такими заданиями часть их условий перенесена на имеющийся у Вас черновик, на котором Вы можете делать любые записи, пометки, прорабатывать версии решения и иным образом активно работать с заданием. После завершения работы над заданиями черновик подлежит сдаче представителю организатора заключительного этапа олимпиады.

Выполнение заданий целесообразно организовать следующим образом:

– не спеша, внимательно прочитайте описательную часть задания;

– прочитайте часть задания, указывающую, что требуется определить и в какой форме ожидается ответ;

– определите наиболее верный и соответствующий требованиям задания ответ;

– отвечая на кейс-задание, обдумайте и сформулируйте конкретные ответы только на поставленные вопросы;

– если Вы выполняете задание, связанное с заполнением таблицы или схемы, не старайтесь детализировать информацию, вписывайте только те сведения или данные, которые указаны в вопросе;

– после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности выбранных Вами ответов и решений.

Предупреждаем Вас, что:

– при оценке тестовых заданий, где необходимо определить один правильный ответ, 0 баллов выставляется за неверный ответ и в случае, если участником отмечены несколько ответов (в том числе правильный), или все ответы;

– при оценке тестовых заданий, где необходимо определить все правильные ответы, 0 баллов выставляется, если участником отмечены неверные ответы, большее количество ответов, чем предусмотрено в задании (в том числе правильные ответы) или все ответы.

Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри.

Содержащий материалы заданий черновик теоретического тура входит в комплект материалов участника и подлежит сдаче по окончании работы.

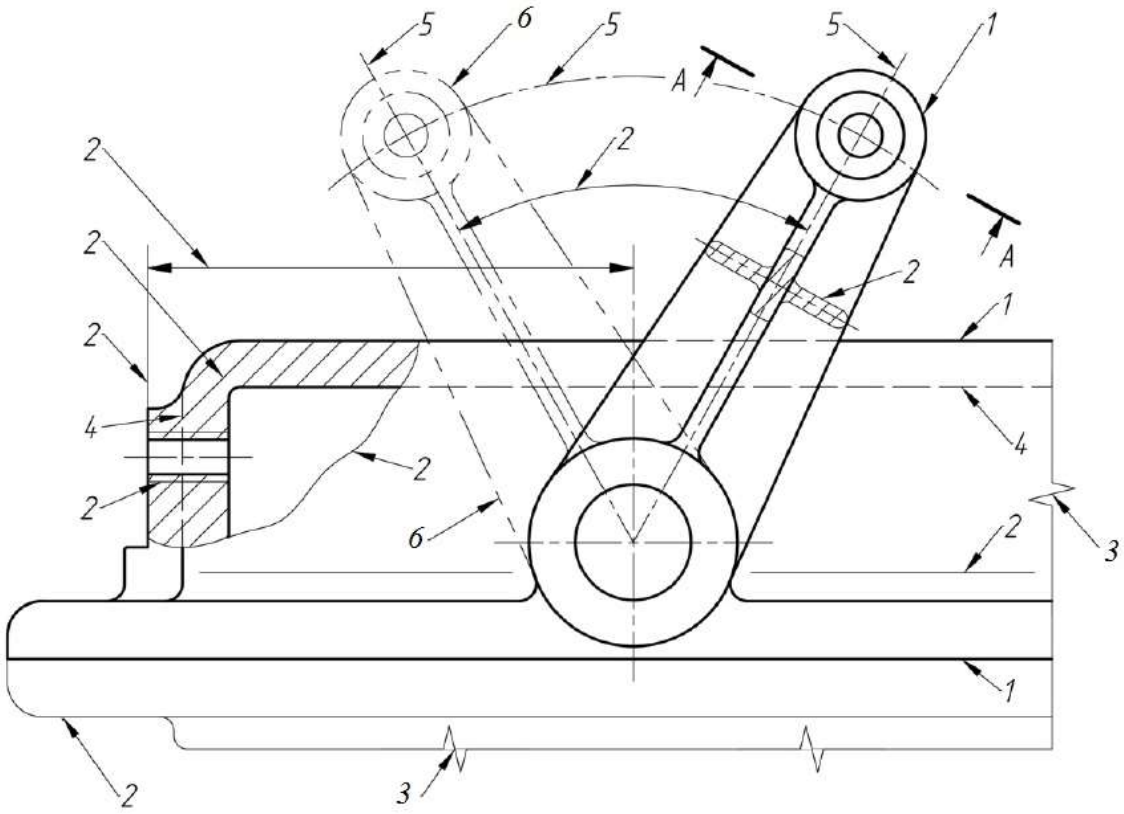
Максимальная оценка – 30 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть

1. (1 балл) Установите соответствие между типами лазеров по виду активной среды (в левом столбце) и их примерами (в правом столбце). Ответ запишите в виде сочетания цифр и букв, например: 1А2Б3В4Г

Тип лазера	Пример
1 – Твёрдотельные	А – квантово-каскадный лазер
2 – Жидкостные	Б – гелий-неоновый лазер
3 – Газовые	В – лазер на красителе родамин 6G
4 – Полупроводниковые	Г – рубиновый лазер

2. (1 балл) Укажите название линий, представленных на чертеже. В чём основное назначение линии номер 3?
Наименование линий: *штриховая, сплошная тонкая, сплошная толстая основная, штрихпунктирная тонкая, сплошная тонкая с изломами, штрихпунктирная с двумя точками тонкая.*



3. (1 балл) В каком году и кем впервые было продемонстрировано миниатюрное радиоуправляемое судно? Ответ запишите в виде сочетания цифры и буквы, например: 1А

Изобретатель	
1	Бенджамин Франклин
2	Иван Ползунов
3	Николай Жуковский
4	Никола Тесла
5	Норберт Винер

Год	
А	1752
Б	1766
В	1898
Г	1904
Д	1922

4. (0,5 балла) Прочитайте внимательно текст из приложения к журналу «Прогрессивное Садоводство и Огородничество» за 1908 год. Напишите название двигателя, о котором идёт речь в тексте, и укажите, в чём его главное отличие от современных двигателей такого типа?

Только колѣнчатый валъ, съ двумя парами подшипниковъ, требующій болѣе или менѣе точной работы въ изгибѣ колѣна и обточкѣ шейки и осей, желательно бы сдѣлать на какомъ-либо заводѣ, который бы могъ отлить и всѣ ролики.

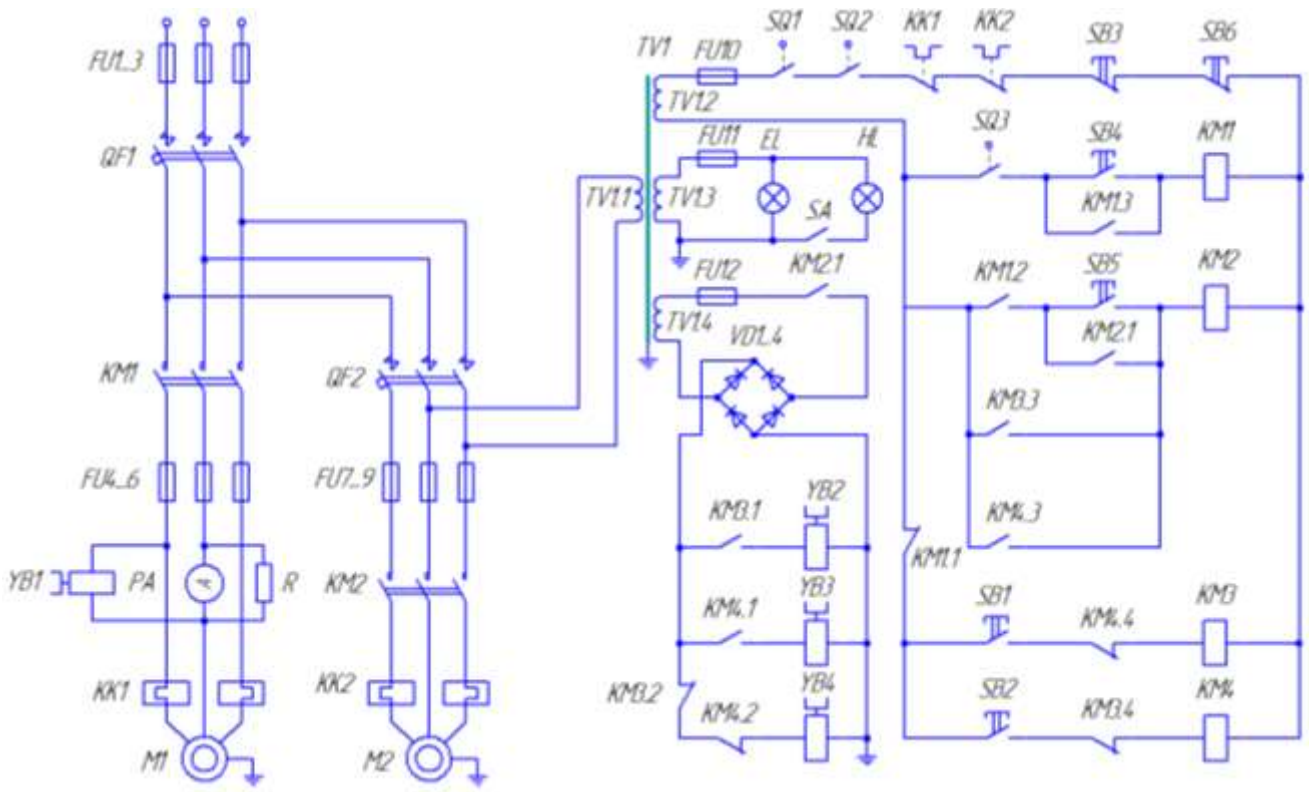
Эти части обойдутся относительно недорого, а остальное можно сдѣлать дома также сравнительно дешево. Во всякомъ случаѣ стоимость всего двигателя нашей системы будетъ далеко ниже стоимости подобныхъ двигателей, предлагаемыхъ различными фирмами.

Нашъ _____ двигатель предположенъ небольшихъ размѣровъ, всего лишь 10-ти футовъ въ діаметрѣ, какъ достаточный для приведенія въ дѣйствіе насоса среднихъ размѣровъ. Этимъ же двигателемъ можно привести въ дѣйствіе небольшую динамо-машину и т. п.

5. (0,5 балла) Области применения этого металла разнообразны: он служит компонентом для изготовления перламутровой краски, металлизированных текстильных материалов, а также используется при производстве оборудования для переработки масел, изготовления сладостей, сахара и пива. В народе порошок из этого металла называют «серебрянка». Напишите название этого металла.

6. (1 балл) Компания купила товар на сумму 300 руб. (с НДС 20%) и продала его за 450 руб. (с НДС 20%). Сколько останется у компании после уплаты (вычета) НДС? Ответ запишите в рублях.

7. (1 балл) На рисунке представлена электрическая принципиальная схема обрабатывающего станка, определите, от какого напряжения питается силовая цепь станка, и выберите правильный ответ.



а – 110 V
б – 127 V
в – 220 V
г – 380 V

8. (2 балла) Вася создал необитаемый подводный аппарат с нулевой плавучестью (рис. 1). Задача аппарата собирать объекты со дна водоёма. Для этого НПА необходимо наклоняться на угол 45 градусов по тангажу против часовой стрелки вокруг некоторого центра. Помогите Васе с расчётами, хватит ли тяги движителей для удержания угла? Выберите все правильные утверждения. Ответ запишите в виде последовательности цифр по возрастанию без пробелов, например, 1234.

1) Тяги не хватит.
2) Если сдвинуть движители на высоту манипулятора, то тяги хватит для удержания угла.
3) Если центр тяжести поднять выше на 150 мм, центр плавучести опустить на 150 мм, то тяги двигателей хватит для удержания угла.
4) Тяги хватит.

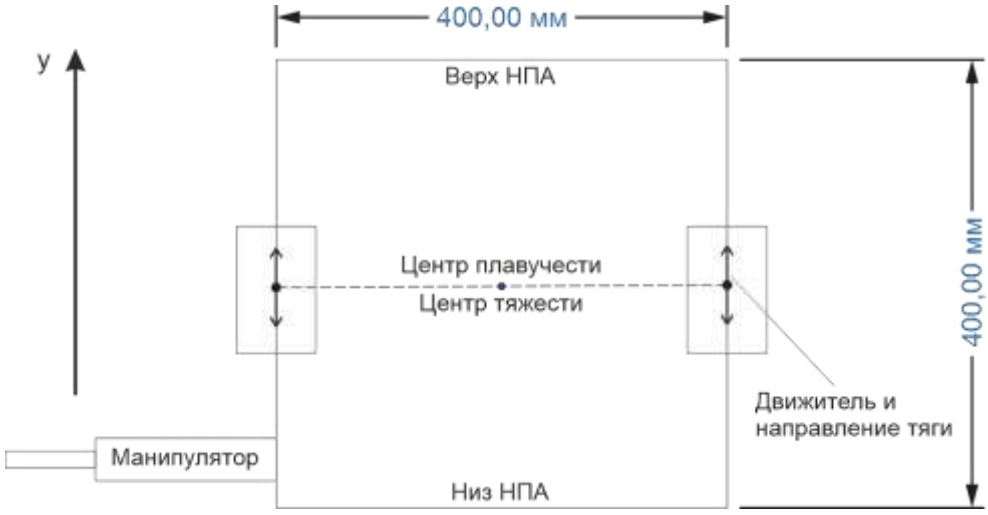


Рис. 1. Необитаемый подводный аппарат

Масса НПА – 9 кг.

Движитель. Тяга в прямом направлении (совпадает с направлением оси y): 0,2 кгс (при номинальном напряжении). Тяга при реверсе: 0,15 кгс (при номинальном напряжении).

Справочная информация.

1 килограмм-сила (кгс) равен 9,80665 ньютона (Н).

Центр плавучести – это местоположение внутри твердого объекта, погруженного в жидкость, где сумма всех сил давления распределяется в направлении, противоположном направлению силы тяжести.

Специальная часть

Кодирование – это отображение $\varphi: I \to B$ из множества информационных слов I в множество двоичных последовательностей B.

Образ $\varphi(i)$ информационного слова $i \in I$ называется **кодовым словом**.

Множество всех кодовых слов, соответствующих информационным словам из множества I называется **кодом**.

Длина кодового слова – это длина двоичной последовательности, которой оно является.

Двоичный блочный (n, k)-код преобразует двоичные последовательности длины k (информационные слова) в двоичные последовательности длины n (кодовые слова).

Пример: (7,3)-код: информационное слово – 110 (3 бита), кодовое слово – 0111110 (7 бит).

Подобное преобразование позволяет обнаруживать и исправлять ошибки (искажения битов), которые происходят при передаче кодовых слов по каналу связи.

Расстоянием Хэмминга $d(x,y)$ между двумя двоичными последовательностями одинаковой длины x и y называется число позиций, в которых они различаются.

Пример: $x = 11101$, $y = 01100$, $d(x,y) = 2$, кодовые слова различаются в двух двоичных позициях.

Декодирование по методу максимального правдоподобия – поиск среди всех исходных кодовых слов того, которое имеет минимальное расстояние Хемминга с искаженным.

Пример:

Искаженное кодовое слово 001.

Множество кодовых слов: {000, 111}.

Расстояние Хемминга с первым кодовым словом равно 1, расстояние Хемминга со вторым кодовым словом равно 2. Значит, в качестве исправленного выбирается первое кодовое слово.

Код обнаруживает ошибку, если при декодировании подается сигнал об отличии принятой двоичной последовательности от отправленного по каналу связи кодового слова (то есть, если это искаженное кодовое слово не является элементом множества кодовых слов).

Код исправляет ошибку, если при декодировании двоичной последовательности (искаженного кодового слова) удается верно установить отправленное кодовое слово.

Кратность обнаруживаемых ошибок T – это максимальное количество ошибок (искаженных бит) в кодовом слове, которое гарантированно может обнаружить код (то есть вне зависимости от того какое изначально было кодовое слово и вне зависимости от тех позиций, в которых произошли искажения).

Пример: код {00, 01, 10, 11} не обнаруживает ни одной ошибки, а код {00, 11} обнаруживает одну ошибку.

Кратность исправляемых ошибок t – это максимальное количество ошибок (искаженных бит) в кодовом слове, которое гарантированно может исправить данный код (то есть вне зависимости от того какое изначально было кодовое слово и вне зависимости от тех позиций, в которых произошли искажения).

Пример: код {00, 01, 10, 11} не обнаруживает ни одной ошибки, а код {000, 111} исправляет одну ошибку.

Пусть в информационном канале возможны только ошибки вида $0 \to 1$. Для произвольного двоичного слова $u = x_1 x_2 \dots x_n$ составим сумму вида:

$$S(u) = \sum_{i=1}^{n} i \cdot x_i$$

Возьмем $n = 5, l = 7$ и рассмотрим код, состоящий из всех таких слов v таких, что $S(v) \equiv 0 \ (mod\ l)$. Обозначим полученный код за $V_{n,l}$.

Данный код исправляет любые одиночные ошибки вида 0→1.

9. Исправьте ошибку в закодированном данным кодом и полученном из канала связи сообщении 11110. Запишите отправленное сообщение. (1,5 балла)

10. Такие коды обладают способностью исправлять еще один тип искажений, а именно «выпадение» (пропуск) символа. На вход пришло кодовое слово 101 из $V_{4,5}$ Восстановите исходное кодовое слово (1,5 балла)

Девочка Вера в компании друзей начала изучать правовое регулирование в Российской Федерации. Теперь они часто адаптируют разные игры под эту тему, чтобы прогресс обучения шёл быстрее. Сегодня она нашла в своем почтовом ящике письмо:

Б	Я	Л	Й	Ш	Р	З	Д	К	Т	Ф	Ц	П	И	О	У	А	Ю	Ч	Ж	Н	Е	Ё	С	Х	Г	В	Щ	Ы	К
Е	Л	С	Ц	М	Ф	У	Щ	Ъ	Х	И	Д	Г	Б	Ж	О	О	В	Т	Ё	Э	А	Н	Р	Ь	Ч	П	Ю	З	Я
В	З	Б	Ч	Ю	Т	Н	Ъ	М	Ё	У	Ы	Л	Ь	Р	Ж	Я	Ш	Г	О	Э	Н	Х	К	П	Ц	Й	И	Д	А
Щ	У	Г	Э	Ъ	Ю	Ь	Ы	И	Н	С	Л	Д	Й	Ч	А	Е	З	Х	П	С	Р	Ж	Ф	Т	В	Б	О	Ц	М
М	Ю	Ш	Х	К	Я	Ф	А	З	Ж	Ч	Г	У	П	И	Т	О	Н	Й	Д	Е	Б	Щ	Ь	Ъ	Ё	Ц	С	Ы	Т
Ъ	У	М	Ш	Э	Щ	Р	Ч	О	П	Т	Б	Ы	С	Ю	Н	Я	З	Е	Й	В	Х	Г	И	Ф	И	Ж	Ь	Ё	Л
Д	П	Т	Ж	Е	Ш	Ю	Э	У	Ц	Ф	С	Щ	Ъ	М	Ь	З	Ё	Х	Й	О	В	И	Ы	Б	Т	А	Я	Н	Р
Ф	Ц	С	Д	К	З	Ж	Я	Э	Г	Ъ	Р	Ч	Е	Ь	Б	М	П	Ё	У	Й	Т	Ю	Щ	Н	Л	И	О	В	У
И	Х	Г	П	Л	А	Т	Е	Ц	Ц	Ы	В	С	З	Ж	Э	Д	Ь	Б	О	Ч	У	Я	Ш	Н	К	Й	Ё	Ф	Ъ
Ь	Д	Ц	Ы	А	Ш	Г	З	Э	Р	Е	М	Ж	Л	К	Х	И	Б	Ч	Ё	У	И	Щ	В	Я	О	С	Ю	Ф	Ъ
З	Э	Н	Х	Ц	В	М	У	П	Ы	Л	И	О	Ш	Ё	Д	Ь	Ч	Ю	А	Г	Я	К	Т	Р	Щ	Б	Ж	Е	Я

На днях она вместе с друзьями прочитала в молодёжном журнале статью про стеганографию. Очевидно, кто-то из друзей применил новые знания на практике.

Известно, что скрытое сообщение связано с изучаемой Верой и её друзьями темой.

11. Определите число символов в скрытом сообщении. (1 балл)
12. Восстановите скрытое сообщение. (3 балла)

Матрица — это прямоугольная таблица чисел, расположенных в строках и столбцах. Матрица обычно обозначается большой буквой и имеет размер m × n, где m — количество строк, а n — количество столбцов. Например, матрица A размера 2 × 3 выглядит так:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

Вектор — это упорядоченный набор из n чисел. Длиной вектора называется число n. Например

$$a = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

— вектор длины 2. Таким образом, под вектором можно понимать мат-

рицу размера n × 1.

Единичная матрица — матрица с единицами в ячейках с одинаковыми индексами и нулями в остальных. Пример единичной матрицы 2 × 2:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Обратимая матрица — это квадратная матрица A размера n × n, для которой существует другая матрица B такая, что произведение A × B = B × A = I, где I — это единичная матрица. Если такая матрица B существует, то A называется обратимой, а B — обратной к A.

Умножение матриц — это операция, при которой две матрицы A и B размера n × m и m × k соответственно (з умножаются друг на друга, и результатом является новая матрица C размера n × k (для этого важно, чтобы «соседние» размеры матриц (число столбцов в первой матрице и число строк во второй, равное m в данном примере) совпадали – только в этом случае их можно умножать). Каждый элемент c_{ij} матрицы C вычисляется как сумма произведений элементов i-й строки матрицы A на соответствующие элементы j-го столбца матрицы B:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdot\cdot\cdot + a_{in}b_{nj}$$

Например, для матрицы A размера 2 × 2 и B размера 2 × 1:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} \\ b_{21} \end{pmatrix}, \quad C = A \times B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} \\ a_{21}b_{11} + a_{22}b_{21} \end{pmatrix}$$

Шифр Хилла – шифр замены, в котором последовательность символов длины n заменяется на последовательность той же длины n. Каждой букве алфавита сопоставляется число по модулю 31 (будем считать, что и=й, е=ё). Блок из n букв открытого текста рассматривается как вектор длины n и умножается по модулю 31 на матрицу размера n×n. Элементы данной матрицы являются ключом. Буквы открытого текста переводятся в числа, согласно таблице. Аналогично числа, полученные в результате шифрования, преобразуются в буквы.

Вам дана следующая таблица соответствий:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф
9	30	29	17	20	21	5	12	2	3	0	25	14	19	28	10	7	13	26	24

Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
23	18	15	6	8	16	4	11	1	27	22

Известно, что при шифровании использовались блоки дины n = 2. Это означает, что процесс шифрования можно представить как умножение матриц следующим образом:

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \pmod{31},$$

где mod 31 – взятие числа «по модулю 31», то есть нахождение остатка от деления каждого значени на 31, а

$$P = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \text{ и } C = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

— векторы длины 2, представляющие открытый текст и зашифрованный текст соответственно, K — матрица 2 × 2, представляющая ключ шифрования.

13. Вы смогли перехватить зашифрованный текст ЪЯХЫ и ключ

$$K = \begin{pmatrix} 1 & 5 \\ 6 & 4 \end{pmatrix}$$

Найдите исходный текст. *(1,5 балла)*.

14. Зная открытый текст из предыдущего задания и новый перехваченный шифротекст ЮЖЮШ, восстановите ключ шифрования. (2 балла)

15. Сколько необходимо перехватить попарно-различных пар биграмм (пар блоков букв длины 2 открытого текста и соответствующих им блоков шифртекста), чтобы гарантированно восстановить ключ? (1,5 балла)

Системный администратор некоторой компании «SuperIT», занимающийся также и вопросами безопасности, прочитал, что хранение паролей на сервере в открытом виде небезопасно. Решение с функциями хэширования показалось ему слишком сложным, поэтому он решил поступить иначе. На самом сервере он

задал регулярное выражение и далее создал и раздал пользователям пароли, которые этому регулярному выражению соответствовали.

Регулярные выражения – это формальный язык задания шаблонов, по которым можно искать в тексте некоторые подстроки. Например, можно искать фрагмент, являющийся адресом электронной почты (зная, что это несколько символов, затем символ @, затем доменное имя, состоящее из 2 частей, разделенных точкой), телефонным номером (последовательность из определенного числа цифр, причем при известной стране можно указать в шаблоне соответствующий код), номером банковской карты, адресом и т. п.

Регулярное выражение, использованное системным администратором, может включать следующие фрагменты (условно назовем их блоками):

- Один символ из некоторого множества заданных. Например, выбор из букв “a”, “b” или “c”. Совпадением будет считаться любая из этих букв. В регулярном выражении такой выбор записывается так: [ab]
- Один любой символ кроме заданных. Например, любой символ кроме букв “a” и “b”. Такой выбор записывается так: [^ab]
- Любой одиночный символ. Соответствующая запись – символ точки (без кавычек): «.»
- Один из двух символов – например, “a” или “b”. Соответствующая запись: a|b.
- Необязательный символ (может присутствовать или отсутстовать). Соответствующая запись: a? – ровно один символ “a” или его отсутствие.
- Несколько одинаковых символов, число которых попадает в заданный диапазон. Например, “aaa”. Соответствующая запись: a{1,3} – от 1 до 3 символов “a”
- Любая одна цифра. Соответствующая запись: \d

В случае, если в подстроке нужно искать какой-то символ, являющийся частью описания блока (например, открывающаяся и закрывающаяся скобка, символ «^»), то перед ними ставят символ «\». В этом случае они не воспринимаются как часть описания блока. Некоторые блоки требуют заключения в круглые скобки, чтобы считаться частью общего шаблона.

Например, регулярное выражение Hello, [Ww]orld[!?] означает

• “Hello, “ — фиксированный фрагмент текста,

• [Ww] — буква “W” или “w”,

• “orld” — фиксированный фрагмент текста,

• [!?] — строка должна заканчиваться либо “!”, либо “?”

Этому шаблону соответствуют следующие строки:

• Hello, World!

• Hello, world!

• Hello, World?

• Hello, world?

Но не соответствует

• Hello, World$ (последний символ не входит в набор [!?])

Тогда, например, задав регулярное выражение (здесь отдельные блоки выделены разными цветами)

[abcde](\#|\$)[fgh](\(|\))\dg?Run

администратор может создать для пользователей пароли

- a#g(1gRun
- c$g)7Run
- e#h)4gRun
- b$f)9gRun

и другие, соответствующие тому же шаблону.

Нарушитель узнал, что аутентификация на сервере происходит на основе некоторого (недавно измененного администратором) шаблона. Ему также удалось приобрести несколько ранее использовавшихся паролей:

- Xy-42Q@e!
- Xz-73W@a?
- Xa-91X@o$

- Xw-18E@i%
- Xx-29Q@u!
- Xy-85X@a?
- Xz-67W@i$
- Xa-34X@e%
- Xw-59Q@e!
- Xx-73W@o?

Сейчас эти пароли уже признаны администратором скомпрометированными и заблокированы.

16. Определите количество блоков в регулярном выражении, которому соответствуют приобретенные нарушителем пароли (считайте блоками фрагменты регулярного выражения, проводящие одну проверку). (1 балл)

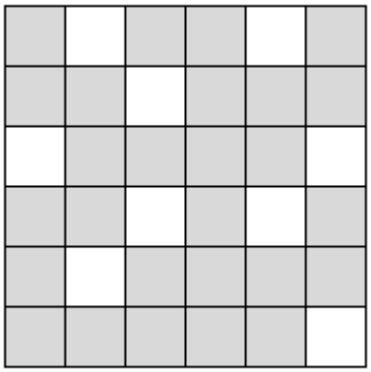
17. Установите, сколько различных паролей, соответствующих действующему шаблону, может задать администратор, исходя только из информации, имеющейся в доступных паролях. (1,5 балла)

18. Установите, сколько различных символов может встретиться в паролях, соответствующих действующему шаблону, 2 раза. (1 балл)

19. Составьте любой пароль, с помощью которого возможно авторизоваться в системе при действующем шаблоне (1,5 балла)

Кейс-задание

20. Шифр, известный как «решетка Кардано» или «поворотная решетка» - шифр перестановки, основанный на использовании квадратного трафарета, пример которого приведен на иллюстрации.



Здесь белым выделены прорези в трафарете, открывающие место для вписывания и прочтения букв. Расположение прорезей является секретным и выбирается абонентами.

Для зашифрования части текста число символов которого совпадает с числом клеточек таблицы, на нее накладывается трафарет, после чего первая четверть символов вписывается в открывшиеся прорези. Вписывание происходит по строкам слева направо сверху вниз. После этого трафарет поворачивается на 90 градусов по часовой стрелке и в прорези вписываются символы следующей четверти. Данная операция повторяется затем еще дважды, так что все клеточки таблицы оказываются заполненными. Шифртекст получается выписыванием букв из таблицы по строкам слева направо сверху вниз.

В распоряжении криптоаналитика оказался значительный объем открытых текстов и соответствующих им зашифрованных текстов, полученных одним и тем же шифром, что можно представить в виде двух бесконечных последовательностей символов, в которых могут встретиться любые интересующие комбинации. В такой ситуации криптоаналитики стремятся проверить, мог ли быть использован именно шифр «поворотная решетка» с некоторым известным размером стороны трафарета n. Для проверки этого в открытом и зашифрованном текстах ищут некоторые комбинации символов, характерные для определенного шифра или закономерности связи между открытым текстом и шифртекстом. Например, для известной шифровальной машины «Энигма» характерной особенностью является то, что никакой символ открытого текста не может быть зашифрован тем же символом. Тогда можно построить критерий проверки, записав его, например, так:

Если $E(x_i) = x_i$, то доказано, что для зашифрования использована не «Энигма»; здесь x_i – произвольный символ открытого текста, $E(x)$ – функция зашифрования.

Сформулируйте аналогичные критерии проверки того, был ли для зашифрования применен шифр «поворотная решетка» с одним (неизвестным) ключом-трафаретом с количеством клеточек $n \times n$. Для получения максимального балла сформулируйте не менее 5 корректных критериев такой проверки, позволяющих утверждать, что используется указанный шифр или что он не мог быть использован (т. е. использован неопределенный иной шифр). Критерии могут быть описаны в любой форме – например, в виде формальных условий (как в примере выше) в текстовой форме или иначе. *(5 баллов)*