ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ

ТЕОРЕТИЧЕСКИЙ ТУР

9 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и кейс-задания.

Время выполнения заданий теоретического тура 90 минут.

Часть предложенных Вам заданий будет 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.

Кейс-задание выдано Вам на отдельном листе, содержащем условие и место для представления ответа. В данном задании при оценке учитывается решение, которое для получения максимального балла требуется оформить разборчиво, полно для понимания хода решения, а также в понятном для членов жюри порядке изложения, по возможности избегая значительных исправлений.

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.

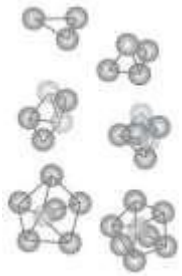
Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри.

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

Максимальная оценка – 25 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть

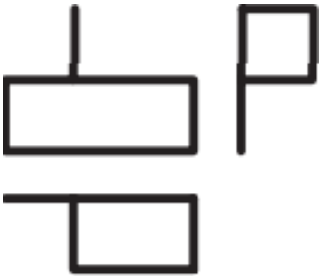
1. Установите соответствие между столбцами

Типы нанокристаллических материалов по размерности структурных элементов		
Изображение	Название	Тип материала
1) 	а – Нульмерные (0D)наноматериалы	W – это порошки, волоконные, многослойные и поликристаллические материалы
2) 	б – Одномерные (1D) наноматериалы	X – нанотрубки, волокна и прутки
3) 	в – Двумерные (2D) наноматериалы	Y – нанокластеры, нанокристаллы, нанодисперсии, квантовые точки
4) 	г – Трехмерные (3D) наноматериалы	Z – пленки (покрытия) нанометровой толщины

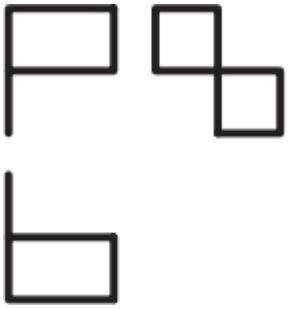
2. На рисунке представлена заготовка для моделирования из бумаги.

Заготовка

Используя изображения результатов моделирования из бумаги, установите соответствие между моделированием и проекциями.



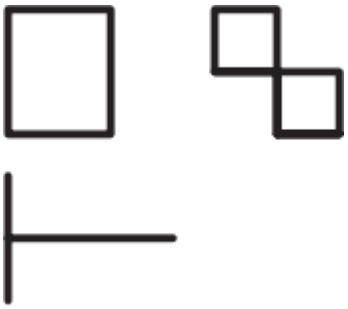
1



3

2

4



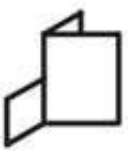
5

а

б

в

г



д

3. При передаче электрической энергии на большие расстояния значительная часть энергии теряется, расходуясь на нагревание проводов. По закону Джоуля-Ленца энергия, расходуемая на нагревание проводов, пропорциональна сопротивлению и квадрату силы тока. Как следует изменить силу тока и напряжение, чтобы уменьшить потери энергии на нагревание проводов в 400 раз?

4. Запишите заложенное в определении понятие.

Совокупность устройств, приборов и оборудования, которые обеспечивают комфортные условия жизнедеятельности человека в его жилище, помещении для работы, отдыха, развлечений и т.п. (системы отопления, водоснабжения, канализации, газо- и электроснабжение, линии связи).

5. Прочитайте описание этого предмета и выберите правильный ответ. «Форму этого изделия диктует тупой угол, под которым корень расположен к стволу. Поэтому ножка с лопаской, которую режут из ствола берёзы, стоит не под прямым углом к донцу, на которое шёл корень, а как бы наклоняясь вперёд. Это придаёт особенное изящество, грациозность предмету и делает его очень удобным для работы. Широкая у основания ножка постепенно сужается кверху и заканчивается маленькой лопастью с ажурной резьбой по краю, что ещё больше подчёркивает лёгкую, изысканную форму копыла». О каком изделии идёт речь в описании О.В. Кругловой, Заслуженного работника культуры РФ (1986 г.), и что можно было бы сделать на этом изделии, имевшем место в каждой крестьянской семье. Выберите правильный ответ.

а. – лавка и шитье
б. – прялка и прядение нити
в. – верстак и столярные работы
г. – мялка и обработка льна

Специальная часть

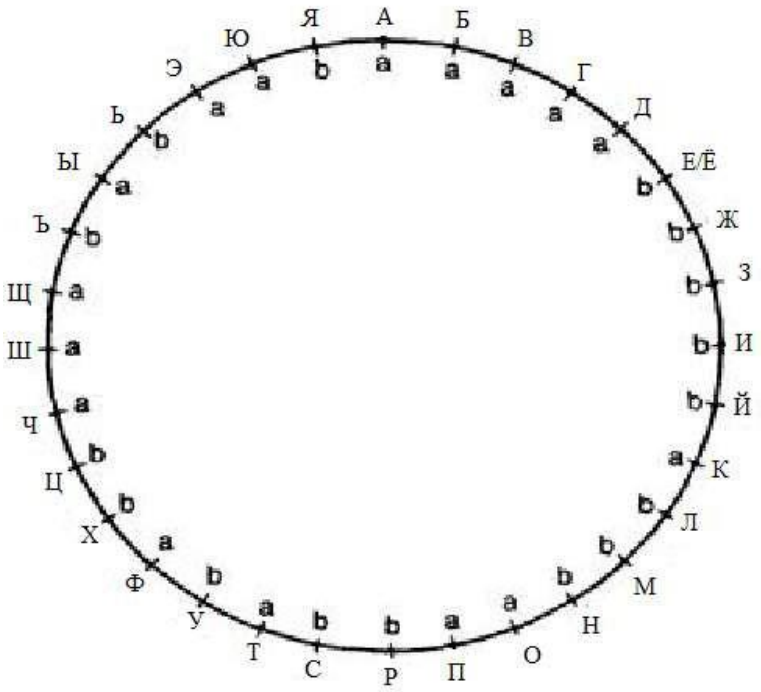
Способ сокрытия сообщения в произвольном тексте, известный как «Шифр Бэкона», основывается на кодировании букв сообщения сочетаниями букв «*a*» и «*b*». Для записи текста выбираются 2 варианта начертания букв (2 шрифта), при этом использование каждого из них кодирует «*a*» или «*b*». Например, запись «**д*ень б*ыл** **с*ол**нечн**ым и б*ез** **в*етр**а**» будет кодировать последовательность «baaab ababb abbba aaaba abbba».

Далее каждую группу из 5 символов можно использовать в качестве замены (кода) буквы сообщения. Например, на основе такой таблицы

aaaaa	**а**	aabbb	**з**	abbba	**о**	babab	**х**	bbbaa	**ь**
aaaab	**б**	abaaa	**и**	abbbb	**п**	babba	**ц**	bbbab	**э**
aaaba	**в**	abaab	**й**	baaaa	**р**	babbb	**ч**	bbbba	**ю**
aaabb	**г**	ababa	**к**	baaab	**с**	bbaaa	**ш**	bbbbb	**я**
aabaa	**д**	ababb	**л**	baaba	**т**	bbaab	**щ**		
aabab	**е/ё**	abbaa	**м**	baabb	**у**	bbaba	**ъ**		
aabba	**ж**	abbab	**н**	babaa	**ф**	bbabb	**ы**		

приведенная выше строка может быть декодирована в последовательность букв «с», «л», «о», «в», «о».

Для удобства записи замен букв последовательности букв «*a*» и «*b*» могут порождаться при помощи окружности:



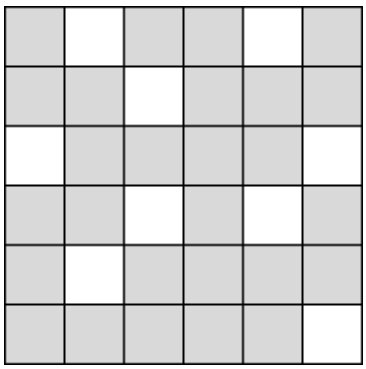
Такая последовательность может быть записана в виде строки символов «*a*» и «*b*» – «aaaaabbbbbabbbaabbababbaaababaab», которая затем записывается по окружности. Тогда замена каждой буквы определяется 5 символами при движении от этой буквы по часовой стрелки.

Пусть такая окружность задана последовательностью

«bbababbaaababaabaaaaabbbbbabbbaa».

6. Определите замену для буквы «О».
7. Определите букву, заменой которой является строка «babaa»
8. Определите замену на основе данной окружности для слова «сон».
9. Прочтите слово, закодированное строкой «**Т***у***т** *нет т***а***к***ой** *ж***ар***ы*»

Шифр, изветный 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 и 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.

Таким шифром с некоторым (неизвестным) ключом размером 8x8 клеточек получен шифртекст:

м	й	ы	й	л	п	и	е
л	с	с	а	в	н	р	ж
е	о	ж	ш	о	л	д	й
и	а	п	д	я	о	и	о
с	р	м	д	в	ь	л	п
о	и	р	з	о	о	г	г
н	у	д	е	н	у	н	о
х	а	л	о	с	к	м	о

10. Определите первую букву открытого текста.

11. Установите позицию (номер) в открытом тексте буквы, располагающейся в правом верхнем углу заполненного квадрата.

12. Проверьте, может ли в открытом тексте присутствовать слово «лесной». Укажите в ответе «1», если может, и «0», если нет.

13. Восстановите расположение прорезей в трафарете в позиции для вписывания первой четверти открытого текста. Ответ введите в виде номеров клеточек строки, в которых сделаны прорези, разделяя их запятой без пробела. Если в какой-то строке прорезей нет, введите 0. (Например, трафарет из описания шифра будет представлен в виде: 2,5; 3; 1,6; 3,5; 2; 6)

14. Восстановите открытый текст сообщения. Введите его в нижнем регистре (без заглавных букв) без знаков препинания и пробелов – только символы из шифртекста.

Шифр, известный как «ADFGVX», совмещает операции замены и перестановки. Зашифрование происходит в два этапа. На первом этапе символы алфавита вносятся в произвольном порядке в квадратную таблицу размером 6x6. Расположение букв в таблице – часть ключа шифра. Столбцы и строки квадрата помечаются буквами A, D, F, G, V и X. Например, так (символ «_» означает пробел):

	A	**D**	**F**	**G**	**V**	**X**
A	А	Ш	П	Ф	Г	З
D	Ы	Е	.	О	Ь	Ё
F	К	У	В	Я	Л	,
G	С	Ю	М	Т	Щ	Ж
V	Ч	И	Ъ	Н	Б	Х
X	Д	_	Р	Ц	Э	Й

Каждая буква открытого текста заменяется по такой таблице парой букв, задающищ строку и столбец, в которой находится эта буква. Например, буква «А» будет заменена на пару «АА», буква «Б» – на «VV», «Г» – «AV», «Д» – «XA» и т. д. Сообщение «текст» примет после этого вид строки «GGDDFAGAGG».

Далее такая строка вписывается посимвольно в прямоугольную таблицу, число столбцов которой задается другой частью ключа – длиной лозунга. Столбцы таблицы помечаются буквами лозунга. Например, так (в качестве лозунга взято слово «рука»):

Р	**У**	**К**	**А**
G	G	D	D
F	A	G	A
G	G	A	D

Поскольку число символов получилось не кратным 4, для дополнения до полного числа строк в таблицу вписаны 2 первые буквы, используемые в данном шифре – «A» и «D». Если бы потребовались 3 буквы, далее была бы использована «F», затем «G» и т. д.

Столбцы полученной таблицы переставляются в порядке, в каком буквы лозунга встречаются в алфавите, причем если какая-то буква присутствует в лозунге более одного раза, столбцы, помеченные этой буквой, берутся в порядке слева направо, то есть их взаимный порядок не изменяется. Таблица из примера будет после такого преобразования выглядеть так:

А	**К**	**Р**	**У**
D	D	G	G
A	G	F	A
D	A	G	G

Имеющиеся в ней символы выписываются по строкам слева направо сверху вниз для получения шифртекста. В рассматриваемом примере он будет таким: «DDGGAGFADAGG».

Таким шифром с аналогичной табицей размером 6x6, но с произвольно выбранным расположением букв в ней зашифрован следующий текст:

```
Я шёл по лесу и наслаждался красотой природы.Всё вокруг
было зелёным и свежим,весёлые птицы щебетали,а воздух пах
весной.По мере приближения к горам равнинный рельеф
сменялся небольшими холмами,и это сказывалось на окружающей
флоре.Я как раз закончил подъём на один из таких и теперь
мог оценить различия.
```

Известно, что после преобразования таблицы по описанному выше правилу, в ее заголовке оказались буквы «АЕИИЛМНПРТЯ», в результате чего получен шифртекст:

GVGGGVXGXGGAXFAAGDXGXGDVGXDXDXGDFFGDVFXXGFFAFXXGVGFDGDGDFAD
AFGXDXFDGFAVAFFAXGDFAXVDGAVDFAVXXXDFVGGAFADFDGAFDDDDXXFXFAG
DGGXGGFAXAXGVGGVGXFXFXGDXFAGGAVADDVFAXAGVGFXVDXFXGFXGAGAAVX
GXGDFAVDXAAVGXDFAGFFGXGFFDFVVAXDXDVGADDFXFXFGFFAXFAAXADFGVX
DFGAFXDGGGAXFAAFGGAXVAAGAAGDXVVGADGDAAFDXGGVGGGDAXDFGFDAFFG
FGAFFVGAFXGFDFFXXGFGFGAGGFGAAVXAGAVXAGGXFDGFGGGGDFXGXGXGGDX
DFGFAAVGGDDFFVVGVXGXXFGFFFGDGFVVXDFXGVDXDVGAXFFDXDFDAFFFDXF
AXGXFVFGFDXFXFGGFADVDGAXDDAVADAFGVFFGGVFGAADXXAGGGAGFXXGVFD
AXFAGGFGDXAXFDAGXDFAFFXDXGDVGXXAAFGGVXVGDDGFFFFXVFDGGVDDGAV
XGDXFGXFFDDGFVAVXFXGAFADVXVAGAAXFDGGVGFGFGXDGDFXFAAFDFVGVVF
GXGAAVXXFGXFXDVGDXVGAVDGFX

15. Определите использованный лозунг (осмысленное слово на русском языке).

16. Восстановите столбец таблицы, определяющей замену букв открытого текста на пары символов, помеченный символом «F». Перечислите через запятую с пробелом 6 символов, расположенных в нем, в порядке сверху вниз. Для обозначения пробела используйте символ «_» – например, «А, Б, В, Г, _, Д».

17. Восстановите полностью заполнение таблицы, определяющей замену букв открытого текста на пары символов.

18. Для совместной выработки общего секрета при обмене сообщениями только по общедоступному (незащищенному) каналу связи, два абонента могут воспользоваться протоколом Диффи-Хеллмана.

Для получения общего секрета абонентам нужно:

1) Выбрать простое число P и взаимно простое с ним меньшее число T.
2) Независимо выбрать произвольное число a и найти остаток от деления T^a на P (то есть найти T^a «по модулю P», записывается «mod P»).
3) Обменяться по общедоступному каналу связи полученными значениями $T^a \bmod P$.
4) Независимо возвести полученные значения в выбранные степени: $(T^{a2})^{a1} \bmod P$ (для второго абонента, соответственно, $(T^{a1})^{a2} \bmod P$).
5) Получившийся у обоих абонентов результат совпадет и будет общим секретом, который далее может использоваться в других криптографических алгоритмах.

Пусть P = 13 и T = 6.

А) Выберите число a и вычислите значение для передачи другому абоненту.

Б) От другого абонента Вами получено число 7. Вычислите общий секрет.

В) Во время выработки еще одного общего секрета с теми же открытыми параметрами Вами получено от другого абонента число 5. Известно, что в канале может действовать нарушитель, способный перехватывать отправляемые абонентами сообщения и подменять их своими (то есть реализовывать атаку «человек посередине»). Другой абонент при выборе произвольных значений обычно пользуется кубиком с 8 гранями. Проверьте, получено ли данное число от Вашего абонента или от нарушителя. Приведите аргументы в пользу предлагаемого ответа, а также все проделанные вычисления.