

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ
ТЕОРЕТИЧЕСКИЙ ТУР
7-8 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и кейс-задания.

Время выполнения заданий теоретического тура 90 мин.

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.

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.

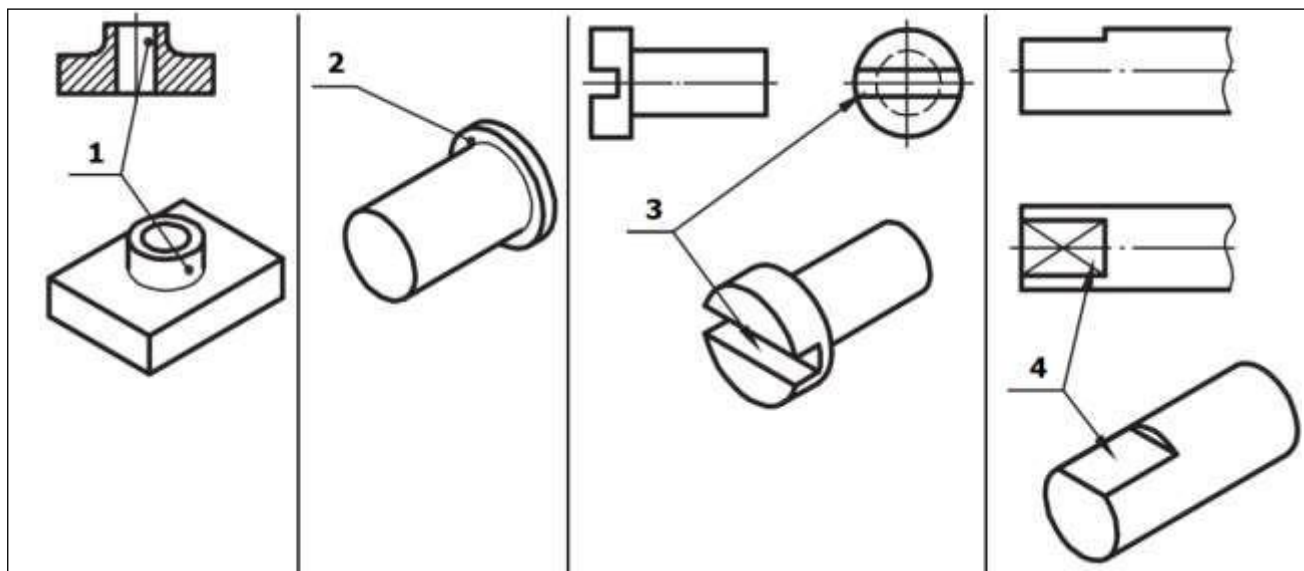
Содержащий материалы заданий черновик теоретического тура входит в комплект материалов участника и подлежит сдаче по окончании работы.

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

Общая часть

1. Входят ли в категорию наноматериалов объекты с размерами, минимальное значение которых не меньше 0,5 мкм? Напишите «ДА» или «НЕТ», поясните свой ответ.

2. Используя изображения, установите соответствие между номерами и их названиями.



- а. – лыска
- б. – буртик
- в. – шлиц
- г. – бобышка

3. Сведения о типе электроизмерительного механизма прибора, о возможности его работы в цепях постоянного или переменного тока и некоторые другие можно узнать по условным знакам, нанесённым на шкале прибора. Какой(ие) условный(е) знак(и), нанесённый(е) на шкале прибора указывае(ю)т на то, что прибор предназначен для работы в электрических цепях только переменного тока?

- а. —
- б. ~
- в. ≈

4. Определите направление деятельности человека по следующим терминам: бочка, колпак, шатёр, полица, повал. Выберите один вариант из предложенных.

- а. – деревянное зодчество
- б. – каменное зодчество
- в. – гончарное искусство
- г. – кузнечное дело

5. Установите соответствие между свойствами товаров и их характеристиками.

1	Качество
2	Оригинальность
3	Удобство
4	Практичность
5	Новизна

а	Надежность в использовании, полезность, соответствие назначению
б	Соответствие моде, современность
в	Совокупность технико-экономических и эстетических свойств, обуславливающих способность удовлетворять определенные потребности в соответствии с назначением
г	Способность создавать чувство комфорта в доме или в индивидуальных ощущениях
д	Нестандартность, своеобразие, соответствие индивидуальным вкусам потребителя

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 «день был солнечным и без ветра» будет кодировать последовательность «baaab ababb abbba aaaba abbba».

Далее каждую группу из 5 символов можно использовать в качестве 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».

Перед Вами текст, содержащий скрытое сообщение:

Мечта всегда была для меня стимулом для достижения высот. Я всегда был уверен, что преодоление трудностей помогает мне достичь моих целей.

6. Определите число букв в скрытом сообщении.
7. Определите количество вхождений буквы «В» в скрытом сообщении. Если этой буквы в сообщении нет, введите 0.
8. Определите количество вхождений буквы «А» в скрытом сообщении. Если этой буквы в сообщении нет, введите 0.
9. Восстановите скрытое сообщение. Впишите его без пробелов и знаков препинания.

Перед Вами шифртекст, полученный при зашифровании перехваченного сообщения нарушителя шифром простой замены (каждая буква открытого текста заменяется на некоторый единственный символ или обозначение – в данном случае на букву того же алфавита, возможно, ту же самую).

МЫЪЛС ЫШ ЫГЯЗ ЛЫЛ ЙЫХЗЛ МЫЩЭЛ ЫЛОБОЖЁПОО ЫХУЙКЗЩОЕ - ЛЁЭ ХЫАЁБО ЫГЯОЗ ЫАД. ЭЫХЁ ОА ЙДЬУ ЫГЗЪЛС, ГЛУ ТЛУ КЁЖКЫЯОЛ ЪКЗХЫ, Р ЭУЛУКУЕ АУВЫЛ ЪЫНЗЪЛРУРЁЛС КЗХЭОЗ О ЩЫШЩДЗ ШОРУЛЩДЗ. КЁЖРЗ ЙЫХЗЛ МУЪЪЗ ТЛУВУ ЛЫЛ ШОЛС ЩУКЭЁ ОБО ХКЫВУЕ МЫЯЩУЕ ЖРЗКС. ЩЗ ХУМЫЪЛОП УЪЫНЗЪЛРЪЗЩОБ ЫЭЁЖЁЩЩУВУ МКУЗЭЛЁ, АУЩУ МУЪЫГОЛС О ЭЫГЫ ХКЫВОЧ МКЗОАЫНЗЪЛР.

10. Определите, какую букву заменяет самый частый символ шифртекста.
11. Определите, какую букву открытого текста заменяет буква «З» в шифртексте
12. Определите, какой буквой в шифртексте заменяется буква «К» открытого текста
13. Определите, есть ли в открытом тексте слово «норка». Укажите номер символа (без учета пробелов и знаков препинания – считайте только буквы), с которого оно начинается. Если такого слова в открытом тексте нет, укажите в ответе 0.
14. Определите, какую букву открытого текста заменяет буква «Т» в шифртексте

В шифре, известном как шифр Виженера, для определения символа замены буквы открытого текста на каждом шаге зашифрования и расшифрования используется секретный ключ (пароль). Алфавиты замены построены с последовательными значениями сдвига — от 0 до 32 и выбираются на основе букв ключа. Их удобно представить в виде таблицы:

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

Буква открытого текста всегда определяет столбец на основе заголовочной строки, а строка определяется соответствующей буквой ключа на основе заголовочного столбца. Например, строка из 5 букв «А» при использовании ключа «ШЕСТЬ» будет зашифрована буквами алфавита, стоящими в первом столбце (потому что в заголовочной строке «А» стоит на первой позиции) в строках, в заголовочном столбце которых стоят буквы «Ш», «Е», «С», «Т» и «Ь» соответственно. Нетрудно удостовериться, что шифртекст будет совпадать с ключом – «ШЕСТЬ».

Таким шифром с некоторым (неизвестным) ключом зашифрован некоторый текст. Результат зашифрования перед Вами (здесь символ «|» отделяет десятки букв, а каждая строка содержит 50 букв):

ЧОПЪЖЕМЫЕЧ | ИЭЕГЩДЛВПД | ЯЙВЮЧБТЬМО | ЩФФЦБЛЛСЪВ | ЙЩКНМТЮРЫБ
 ЕСНСУСКБЗФ | ПФЮЦЗЭИЖТН | ЙИЬЩЮЬЩКДЪ | ИОЦЩВЪЧУА | ГКНХНЬЯКО
 ЪИРЙФКЛМЪЪ | ЖЪТЬЪФЮЧЫЁ | ЙФНЬЙЁЙЧЧ | СЙЮЧХМСУЙЮ | ПВИНСЦЪТДМ
 КПДЭЫЕЧЩЦ | БЮЮЧИАЧЦШУ | ЫМЭУПЫЕЩНЭ | ТЪШАЮЧБТНА | ИФЗИТЬЛЛСЪ
 ВЙЩУПЫЮЮЛЦ | ПНМЗЭЧНЫЪЧ | ИЯРЦЪМЫФК

15. В приведенном шифртексте имеется повторяющийся фрагмент «ЮЧБТ». Определите расстояние между соответствующими символами вхождений данного фрагмента в шифртекст.

16. Найдите в данном тексте еще один повторяющийся фрагмент длиной от 4 символов (впишите первые 4 символа найденного фрагмента).

17. Определите расстояние между соответствующими символами вхождений найденного фрагмента в шифртекст.

18. Определите длину ключа, использовавшегося для зашифрования приведенного текста.

19. В асимметричной схеме шифрования RSA каждый абонент имеет ключевую пару, в которую входит открытый ключ, используемый для зашифрования сообщений, и секретный ключ – для расшифрования. При этом любой желающий может зашифровать сообщение, используя открытый ключ адресата, а для прочтения сообщения потребуется знание секретного ключа, который, согласно схеме, известен лишь одному лицу.

Для обеспечения такой системы используются следующие математические операции.

- 1) Желающий сформировать ключевую пару абонент выбирает два простых числа – p и q . Далее вычисляется их произведение $N = p \cdot q$.
- 2) Для полученного произведения вычисляется значения функции Эйлера, $\varphi(n) = (p - 1)(q - 1)$.
- 3) Выбирается натуральное число e , большее 1 и меньшее $\varphi(n)$, не имеющее общих делителей (взаимно простое) с $\varphi(n)$. Это число e вместе с N составляет открытый ключ. Для зашифрования сообщения m , являющегося целым числом от 1 до n , отправителю требуется вычислить остаток от деления числа m^e на n (или найти m^e по модулю n , записывается $(\text{mod } n)$).

- 4) Получатель для прочтения этого сообщения должен возвести полученное сообщение m^e в степень d также по модулю n , значение которой является секретным ключом. Ее значение должно быть таким, чтобы выполнялось условие: $d * e \equiv 1 \pmod{\varphi(n)}$, то есть произведение e и d равнялось 1 по модулю значения $\varphi(n)$. Число d вместе с исходными p и q хранится в секрете и составляет секретный ключ.

Пусть $p = 7$ и $q = 11$.

А) Создайте открытый ключ по описанному выше алгоритму.

Б) Вычислите секретное значение d .

В) Зашифруйте сообщение $m = 19$ для другого абонента, чей открытый ключ: $(e, N) = (11; 143)$. Укажите зашифрованное сообщение и отразите ход зашифрования.