

**ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ**  
**ТЕОРЕТИЧЕСКИЙ ТУР**  
**10-11 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 сдадите 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

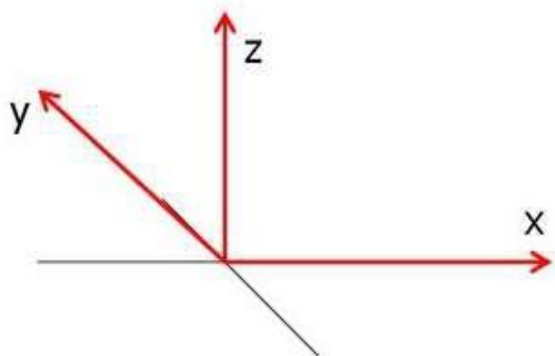
1. Установите соответствие между названием и определением двумерных(2D) наноматериалов.

1	силицен
2	графен
3	борофен

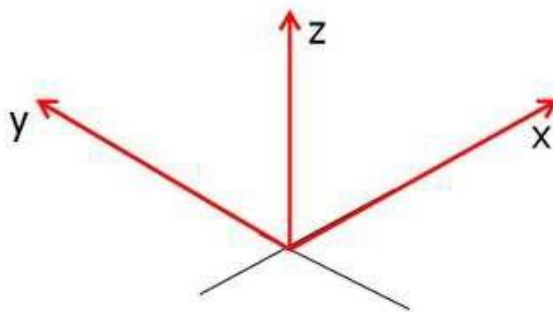
а – гофрированный двумерный наноматериал, изгибающийся вверх и вниз в зависимости от связей между атомами
б – двумерная аллотропная модификация кремния (материал имеет периодически деформируемую/изгибающуюся топологию)
в – двумерная аллотропная модификация углерода (плоский материал)

За новаторские эксперименты по исследованию какого двумерного наноматериала Константину Новоселову и Андрею Гейму вручена Нобелевская премия по физике за 2010 год? Выбрать наноматериал из перечисленных, указав в ответе цифру 1, 2 или 3.

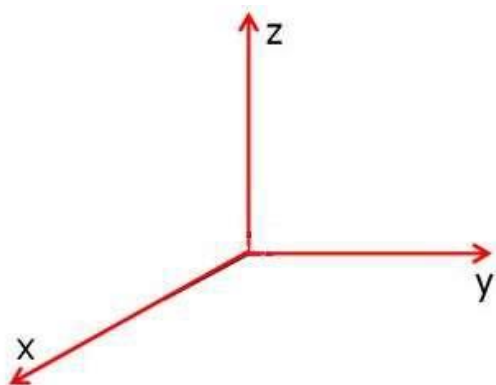
2. На каком рисунке показано правильное расположение осей, во фронтальной диметрической проекции?



а.



б.



в.

3. Развитие энергетической сферы является условием развития техники и технологий. Российские ученые совершили целый ряд открытий, став признанными лидерами в этой области. Сопоставьте перечисленные открытия с фамилиями ученых: Доливо-Добровольский М.О., Курчатов И.В., Пироцкий Ф.А., Яблочков П.Н.

- а. – ядерная энергетика (первый европейский ядерный реактор)
- б. – изобретение трансформатора
- в. – впервые осуществлена передача электроэнергии на расстояние до 1 км
- г. – разработана трёхфазная система токов

4. Эра электронных вычислительных машин началась с методики Дж. Фон Неймана, описанной в 1945 году в рамках доклада «Первый проект» о вычислительной машине EDVAC. Именно от первых устройств, построенных на архитектуре Фон Неймана, отсчитываются поколения ЭВМ. Установите соответствие между столбцами.

	<i>Изобретения и научные учреждения, в которых они созданы</i>		<i>Ученые, с чьими именами связаны разработки</i>
1	ЭВМ Сетунь, разработана в МГУ	а	С. А. Лебедев
2	МЭСМ (малая электронная счетная машина), Киевский институт электротехники (позднее - Институт электродинамики) БЭСМ-1 (большая электронно-счетная машина), Институт точной механики и вычислительной техники	б	Н. П. Брусенцов, Л. С. Соболев
3	ЭВМ «Стрела» (первый серийный советский компьютер), разработана в СКБ-245 (с 1958 года это НИИ электронных математических машин - НИЭМ, с 1968 года -НИЦЭВТ)	в	Ю. Я. Базилевский
4	Урал 1,2,3,4 (семейство советских цифровых ЭВМ общего назначения), разрабатывалась на предприятии п/я 24 в г.Пензе	г	Б. И. Рамиев

5. Выберите из перечисленных приборов и технических средств те, которые не создают микроклимат жилого помещения.

1. воздухоочиститель
2. ионизатор
3. климатизёр
4. кондиционер
5. озонатор

6. охранный извещатель
7. тепловой датчик
8. робот-пылесос

### **Специальная часть**

Анна (А), Борис (Б), Вера (В), Георгий (Г), Дмитрий (Д) и Евгения (Е) работают в одной организации. При планировании новой информационной системы руководство планирует предусмотреть следующие права доступа к ресурсам информационной системы:

договорам отдела клиентского обслуживания (1);

корпоративным договорам отдела работы с юридическими лицами (2);

настройкам прав пользователей базы данных договоров (3);

общим настройкам базы данных договоров (4);

общим настройкам базы данных сведений о сотрудниках (5).

- Борис должен иметь возможность работать с текущими договорами клиентов своего отдела;

- Вера должна иметь доступ к данным текущих клиентов, содержащихся в договорах, всех отделов;

- Георгию требуется работать со всеми договорами компании – не только с текущими;

- Администратор базы данных Анна будет настраивать права всех сотрудников, работающих с клиентскими договорами, поскольку они хранятся в базе данных;

- Дмитрий осуществляет установку и настройку всех информационных ресурсов организации;

- Евгения отвечает за соблюдение требований законодательства о персональных данных клиентов, когда-либо обращавшихся за услугами организации.

6. В случае, если будет принято решение строить систему разграничения доступа на основе мандатной модели, какое минимальное число уровней секретности объектов (и, соответственно, уровней доступа субъектов) потребуется для соблюдения всех сформулированных условий?

7. В случае реализации мандатной модели разграничения доступа, кто будет иметь более высокий уровень доступа – Вера (В) или Дмитрий (Д)? В ответе укажите одну букву, которой обозначен пользователь.

8. Укажите уровни доступа для всех перечисленных пользователей в алфавитном порядке при учете только условий, описанных в сформулированных руководством условиях. Ответ приведите в виде строки чисел, обозначающих уровни доступа для А, Б, В и т. д. Например: «3, 2, 3, 1, 4, 2».

9. В случае, если будет принято решение строить систему разграничения доступа на основе дискреционной модели, определите строку прав доступа (0 – нет права доступа к объекту, 1 – имеется право доступа к объекту) для Георгия (Г).

10. Определите, имеются ли среди пользователей те, чьи наборы прав можно представить в виде некоторой роли в ролевой модели разграничения доступа. В ответе укажите строку обозначений этих пользователей – например, «А, Б». Если таких пользователей нет, укажите в ответе «-» (минус).

Шифр, известный как “Два квадрата”, заключается в замене пар символов, стоящих один за другим, на пары символов того же алфавита. Замена происходит по следующему принципу: символы алфавита вносятся в две квадратные или прямоугольные таблицы в случайном порядке, например, так:

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

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

Далее в таблицах отыскиваются символы шифруемой пары: первая буква отыскивается в левой таблице, вторая – в правой. Зашифрование пары символов происходит по следующим правилам:

Если они стоят в разных строках и столбцах, то для определения символов замены требуется мысленно расположить символы открытого текста в противоположных углах прямоугольника, так, чтобы соединяющий их отрезок являлся его диагональю. Символы замены должны находиться в других углах прямоугольника, а записать их нужно, двигаясь по другой диагонали из правой таблицы в левую. Например, «ЗУ» – «ВЦ», «ОТ» – «.Е».

Если символы шифруемой пары стоят в одной строке, то для замены берется пара символов, расположенных в той же строке, но номера столбцов обмениваются местами. То есть, если первая буква стоит в столбце №2 левой таблицы, а вторая – в столбце №4 правой таблицы, то для замены нужно взять буквы той же строки из столбца №2 правой таблицы и столбца №4 левой таблицы. Например, «СВ» зашифровывается парой «ЛБ», «ЗЛ» – «ОС», «УМ» – «ЯП».

Если координаты символов шифруемой пары в соответствующих таблицах совпадают, то для получения пары замены символы обмениваются местами. Например, «ЗО» – «ОЗ», «ЖИ» – «ИЖ».

Обратите внимание, что символы пробела (или «\_»), точки и запятой являются полноправными символами алфавита, учитываемыми в открытом тексте и используемыми в шифртексте.

Таким шифром с таблицами размером 6х6, аналогичными приведенным в примере, но с произвольно выбранным расположением букв в каждой из них зашифрован открытый текст:

***Однажды, когда я смотрел в ночное небо, я задумался о том, что находится за пределами нашей планеты.***

В результате был получен следующий шифртекст:

ЛЯ.ЫЛГ\_ЕВУЪЦТКННТЕГ,Ш,ЛЕШСШБЕЛУУ,ЫЭЕММЙЪПЛЁЦМЧЫЦАОПЛ  
 ,ЛМ,ЙЭВЫМ,ШБКЙЛЯЪДНПМЫЙ.ДАЛНЛЕОСЪЛ.ЫЕШБ.ДШГСС\_АН

11. Определите букву, которая в обеих таблицах находится в одной строке или одном столбце с символом «\_» (пробел)

12. Укажите две пары букв, для которых положение первой в левой таблице совпадает с положением второй в правой таблице (аналогично «ЗО» или «ЖИ» в примере). Впишите их в алфавитном порядке первой буквы пары.

13. Определите, находится ли в левой таблице буква «О» в одном столбце с буквой «Е». (Укажите «1», если находится и «0», если не может находиться).

14. Определите, находится ли в левой таблице буква «О» в одной строке с буквой «Е». (Укажите «1», если находится и «0», если не может находиться).

15. Определите, находится ли в правой таблице буква «М» в одном столбце с буквой «Н». (Укажите «1», если находится и «0», если не может находиться).

16. Определите, находится ли буква «Е» в одной строке в обеих таблицах. (Укажите «1», если находится и «0», если не может находиться).

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. Известно, что в ключе присутствует слово «полнос». Результат зашифрования



перед Вами (здесь символ «|» отделяет десятки букв, а каждая строка содержит 50 букв):

ЩЪСНЭДНЫЧМ | ЕПНЬЮЦНТЦХ | ТИЛФЭОФБАЩ | МЦОАСЛИЯЪР | ИЭИЁГДЦМПА  
 ЦЩЧЫЪЗГРЁЗ | НМЦЯЭУЛЕРЙ | СРТЦЬЮЧВЙИ | ЩФШЭБИНАНР | ЙНЮЯАСТМТЭ  
 УЮЭЗГЪШЪУЭ | ОЪВОЯССРЛИ | ЪИЭЫСЖЩОУД | ШЩУЮМЦЁИВЗ | ДЩДБЪЯЧТХЖ  
 ЙЪДДКЙПЙЩС | ДЛПООМДННЗ | ЮПЧЧТТАУМЭ | НЫУЭЩГЪЫЩЕ | МРДЩДЩДЦЖИ  
 АГЯЦЗГЁЛСМ | ЦВРТТАЙДЁЙ | НДРЯДРУПДЗ | ЫЕЪЕХТПРУГ | АДФТЯЧРФУЫ  
 УЩЛАЙ

17. Определите, присутствует ли в ключе или открытом тексте слово «множество». В случае нахождения слова укажите номер позиции первой буквы этого слова, предварив его буквой «О», если это фрагмент открытого текста или буквой «К», если искомое слово присутствует в ключе, например «О128». Если данное слово в обоих текстах отсутствует, укажите в качестве ответа 0.

18. Определите, присутствует ли в ключе или открытом тексте слово «созвездия». В случае нахождения слова укажите номер позиции первой буквы этого слова, предварив его буквой «О», если это фрагмент открытого текста или буквой «К», если искомое слово присутствует в ключе, например «О128». Если данное слово в обоих текстах отсутствует, укажите в качестве ответа 0.

19. Определите, присутствует ли в ключе или открытом тексте слово «восток». В случае нахождения слова укажите номер позиции первой буквы этого слова, предварив его буквой «О», если это фрагмент открытого текста или буквой «К», если искомое слово присутствует в ключе, например «О128». Если данное слово в обоих текстах отсутствует, укажите в качестве ответа 0.

20. Определите, какое созвездие упоминается в одном из текстов (открытом тексте или ключе). Приведите ответ в форме «созвездие <название>»

21. Определите прилагательное, которым охарактеризована наша вселенная в открытом тексте. Приведите его в том падеже, в каком оно встречается в тексте.

22. В асимметричной схеме шифрования RSA, используемой в качестве электронной подписи, каждый абонент имеет ключевую пару, в которую входит секретный ключ, используемый для подписывания сообщений, и открытый ключ – для проверки подписей. При этом любой желающий может проверить подпись, используя открытый ключ адресата, а для корректной выработки подписи 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  $\varphi(n)$ .
- 4) Отправитель для выработки подписи сообщения  $m$  должен вычислить остаток от деления числа  $m^d$  на  $n$  (или найти  $m^d$  по модулю  $n$ , записывается  $(\text{mod } n)$ ), где  $d$  – секретная степень, вычисленная так, чтобы выполнялось условие:  $d \cdot e \equiv 1 \pmod{\varphi(n)}$ , 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.
- 5) Получатель для проверки подписи сообщения  $m$ , являющегося целым числом от 1 до  $n$ , должен возвести его подписанное значение  $m^d$  в степень  $e$  также по модулю  $n$ . Пара  $(e, n)$  составляет открытый ключ, служащий для проверки подписи.

Пусть  $p = 13$  и  $q = 23$ .

А) Создайте открытый ключ по описанному выше алгоритму.

Б) Вычислите секретное значение  $d$ .

В) Подпишите сообщение  $m = 17$  при помощи полученной ключевой пары. Проверьте получившуюся подпись, отразите ход подписи и проверки.