Для участия в очном туре олимпиады все задачи решать не обязательно, однако чем больше задач Вы решите, тем выше шансы пройти дальше. После того, как Вы решите все задачи, или посчитаете, что больше задач решить Вы не в состоянии, перейдите по этой ссылке, где вам будет предложено заполнить электронную форму ответов.

В случае возникновения вопросов по условию задач или порядке проведения олимпиады, можете отправить вопрос на электронный адрес igor.bodiagin@gmail.com.

Окончание приема задач заочного тура – ***8 апреля 2018 г.***

Задачи заочного тура V Олимпиады по математике и криптографии БГУ

1) (1 балл) Простейшим примером шифрования являются числовые ребусы, когда в верном математическом выражении различные десятичные цифры заменяются различными буквами, а одинаковые цифры – одинаковыми буквами. Расшифруйте ребус:

СИНУС + СИНУС + КОСИНУС = ТАНГЕНС.

В ответе укажите значение **КОТАНГЕНС**.

2) (2 балла) Пусть a_1, a_2, a_3, … и b_1, b_2, b_3, … числовые последовательности периодов 70 и 2184 соответственно. Найти период последовательности a_1, b_1, a_2, b_2, a_3, b_3, … (Периодом последовательности x_1, x_2, x_3, … называется такое наименьшее натуральное число T, что для всех натуральных n выполнено $x_{n+T} = x_n$).

3) (3 балла) О пароле известно следующее: 1) он состоит из 10 цифр; 2) соседние цифры не повторяются; 3) цифры, стоящие на четных позициях (считая позиции слева направо), всегда нечетные; 4) цифры, стоящие на позициях со 2-й по 6-ю, не превосходят 5; 5) цифры, стоящие на позициях с 7-й по 10-ю, не меньше 6. Сколько существует таких паролей?

4) (5 баллов) Все большую популярность приобретают распределенные системы, основанные на технологии блокчейн. В данной технологии нет ничего сложного: данные группируются в блоки, причем каждый блок связан с предыдущим. В итоге получается своеобразная цепочка блоков, что в переводе на английский и означает блокчейн.

Для того, чтобы связать текущий блок с предыдущим, мы используем криптографию: включаем в заголовок текущего блока хэш-значение предыдущего блока. Хэш-значение – это полученная после преобразования массива входных данных произвольной длины выходная битовая строка фиксированной длины, которую мы можем интерпретировать как число. При этом во многих системах, основанных на блокчейн, на хэш-значение накладывается ограничение: оно не должно превышать некого наперед заданного числа (целевого значения). Это ограничение вводится для того, чтобы участники системы не могли создавать множество новых блоков за единицу времени. При этом целевое значение выбирается с учетом суммарной вычислительной мощности всех участников системы таким образом, чтобы каждый новый блок появлялся через определенное фиксированное время. В криптовалюте Bitcoin, например, это время составляет 10 минут. Чтобы получить блок с хэш-значением, не превышающим целевую сложность, в хэшируемые данные, помимо прочей информации, включается поле *nonce*, которое представляет собой обычное целое число. Изменяя *nonce*, мы рано или поздно получим хэш-значение, удовлетворяющее целевой сложности. Этот процесс называется майнингом.

В этом задании вам предлагается поучаствовать в некотором подобии майнинга. Пусть хэш-функция имеет следующий вид

h(x, *nonce*) = (x + *nonce*) g mod 2^32

При этом:

$x \in$ [0,2^32-1] – предварительное хэш-значение блока,

nonce ∈ [0,2^32-1] – изменяемый параметр,

g ∈ [0,2^32-1] – заданное число.

Запись mod 2^32 означает взятие остатка от деления на 2^32.

Пусть x = 20180312, g = 31415926.

Вам требуется найти наименьший *nonce*, при котором h < 2^30.

5) (7 баллов) Последовательность целых чисел x_1, x_2, x_3, … строится по правилу: x_n – последняя цифра в десятичной записи числа n^n.

Исходное сообщение, состоящее из букв русского алфавита и знака пробела (_) между словами, преобразуется в цифровое сообщение, заменой каждого его символа парой цифр согласно таблице:

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	э	ю	я	_
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Для зашифрования полученного цифрового сообщения длины 28 символов, используется отрезок последовательности x_n такой же длины, начинающийся с некоторого x_k. При зашифровании каждая цифра сообщения складывается с соответствующей цифрой отрезка и заменяется остатком от деления полученной суммы на 10. Было перехвачено сообщение **233986 721645 816067 061731 5588.**

а) (3 балла) Найдите период последовательности x_n.

б) (4 балла) Восстановите исходное сообщение.

6) (10 баллов) В 1550 году Джероламо Кардано предложил простой способ шифрования сообщений. Шифрующий помещает решётку (трафарет) на лист бумаги и пишет сообщение в прямоугольных отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделённым на большое число маленьких фрагментов. Затем решётка убирается и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью шифртекста. Такое заполнение требует известного литературного таланта. У получателя сообщения должна быть такая же решётка.

Володя перехватил телеграмму, в которой содержится сообщение, зашифрованное с помощью решетки Кардано. Он не знает точного расположения вырезанных отверстий на решетке, но ему удалось получить количество вырезанных клеток (не отверстий!) в каждой строке и в каждом столбце. Отверстие может состоять из нескольких клеток, в каждой клетке помещается только одна буква. В первом столбце для каждой строки указано, сколько клеток в ней вырезано. Аналогично, в первой строке для каждого столбца указано, сколько клеток в нем вырезано.

	0	**0**	**1**	**2**	**2**	**2**	**2**	**3**	**1**	**1**
4	Р	О	З	А	С	Е	Г	О	Д	Н
3	Я	У	Т	Р	О	М	Д	В	О	Р
0	Н	И	К	В	А	С	И	Л	И	Й
3	П	О	К	Р	А	С	И	Л	З	А
0	Б	О	Р	С	П	А	С	И	Б	О
4	З	А	О	Т	К	Р	Ы	Т	К	У
0	Ц	Е	Л	У	Ю	М	А	М	А	

а) (3 балла) Помогите Володе расшифровать сообщение.

б) (3 балла) Сколько всего различных решеток, удовлетворяющих указанному шаблону (количеству вырезанных клеток в строках и столбцах), можно построить?

Существует также квадратная решетка Кардано, для которой возможны четыре способа расположить её для шифрования текста – поворачивая её относительно центра на 90°. Решетка – квадрат N x N клеток, некоторые из которых вырезаны. Клетки должны иметь такой размер, чтобы в каждую помещалась ровно одна буква. Вырезанные клетки должны располагаться таким образом, чтобы никакие две из них не оказывались в одном и том же месте при поворотах решетки. Чтобы зашифровать сообщение, нужно разместить решетку на бумаге и вписать часть текста в вырезанные

клетки, затем повернуть решетку на 90° и вписать следующую часть и т. д. Если после завершения этого процесса на решетке остались пустые места (в них нужно вписать произвольные символы) – это шифрование с добавлением «мусора», а если пустых мест не осталось – это шифрование без добавления «мусора».

Влад перехватил сообщение, зашифрованное с помощью решетки Кардано без добавления «мусора»:

В	Е	Д	Е
Л	О	И	Р
Ь	А	!	П
Р	К	Т	Т

в) (2 балла) Помогите Владу расшифровать сообщение.

г) (2 балла) Сколько всего различных решеток без добавления «мусора» можно построить для квадрата со стороной 4? Различными будем называть решетки, которые отличаются друг от друга в начальном положении.

7) (10 баллов) ADFGX-шифр – один из самых известных шифров времён Первой мировой войны, который использовался немецкой армией на западном фронте. Особенность шифра заключается в том, что он построен на соединении базовых операций замены и перестановки. Своё название эта система получила из-за того, что её шифрограммы содержали только буквы «A», «D», «F», «G» и «X». Эти буквы были выбраны не случайным образом. Если их представить в виде точек и тире кода Морзе, то они будут существенно отличаться друг от друга. Таким образом, выбор этих букв минимизирует опасность появления ошибок во время телеграфной передачи.

	A	**D**	**F**	**G**	**X**
A	F	N	H	E	Q
D	R	D	Z	O	C
F	I/J	S	A	G	U
G	B	V	K	P	W
X	X	M	Y	T	L

Процесс шифрования начинается с рисования сетки размера 5×5, каждая ячейка которой заполняется 25 буквами латинского алфавита (I и J шифруются одинаково). Каждая строка и столбец сетки задается одной из 5 букв: «A», «D», «F», «G» и «X». Заполнение сетки осуществляется в произвольном порядке, поэтому получатель должен знать расположение каждого элемента, чтобы произвести расшифрование.

На первом шаге каждый символ сообщения заменяется на пару букв, обозначающих строку и столбец соответствующего символа в сетке. Например, A будет заменено на FF, а B – на GA.

Сообщение:	attackatdawn											
Открытый текст:	a	t	t	a	c	k	a	t	d	a	w	n
Шифртекст на первом шаге:	FF	XG	XG	FF	DX	GF	FF	XG	DD	FF	GX	AD

На втором шаге применяется перестановка, что значительно усложняет взлом. Перестановка осуществляется в зависимости от ключевого слова, которое должно быть известно получателю. Пусть, в нашем примере, таким словом будет «BATTLE». Процесс перестановки заключается в следующем. Вначале создается новая сетка, в верхней строке которой записываются буквы ключевого слова. Затем, под этим словом построчно записывается, полученный на первом шаге

зашифрованный текст. Далее, буквы ключевого слова переставляются в алфавитном порядке вместе с соответствующими им столбцами сетки.

B	A	T	T	L	E
F	F	X	G	X	G
F	F	D	X	G	F
F	F	X	G	D	D
F	F	G	X	A	D

A	B	E	L	T	T
F	F	G	X	X	G
F	F	F	G	D	X
F	F	D	D	X	G
F	F	D	A	G	X

После чего буквы каждого столбца выписываются поочередно сверху вниз:

FFFFFFFGFDDXGDAXDXGGXGX

а) (3 балла) Зашифровать сообщение «password», используя сетку из примера и ключевое слово «caps».

б) (7 баллов) Было перехвачено сообщение, про которое известно, что в качестве сетки для первого шага, использовалась сетка, приведенная в примере. Ключевое слово, использованное на втором шаге и состоявшее из 6 символов, неизвестно. Вам необходимо расшифровать сообщение:

XXADAX DFGFGA AAFGFD FFGGXF XDFDGA XGGGFX FADAGA FDFXAD GFXGFA.

8) (13 баллов) Шифр Виженера – классический полиалфавитный метод шифрования буквенного текста с использованием ключевого слова. Впервые этот метод описал Джовани Баттиста Беллазо в 1553 году, однако в 19 веке получил имя Блеза Виженера, французского дипломата. На протяжении трех столетий этот шифр считался абсолютно стойким.

Пусть нам необходимо зашифровать текст X длиной n символов. Ключом является некоторая секретная последовательность символов K длины m. Сперва буквы исходного текста X и ключа K заменяется на номера этих букв в алфавите начиная с нуля (А – 0, Б – 1 и т.д., Я – 32):

$$X \to (x_0x_1\ldots x_{n-1}),\ K \to (k_0k_1\ldots k_{m-1}),\ \text{где } x_i,\ k_i \in Z_{32}=\{0, 1,\ldots, 32\}.$$

Затем вычисляются значения $y_i = (x_i + k_{i \bmod m}) \bmod 33$, где $(\cdot) \bmod p$ означает нахождение остатка от деления на p. Результатом зашифрования является текст Y с номерами букв $(y_0y_1\ldots y_{n-1})$. Например, при зашифровании слова X = ПРИМЕР с ключом K = БГУ получим шифртекст Y = РУЬНЗД.

а) (3 балла) Зашифруйте шифром Вижинера сообщение X = ПЕРЕХВАТ с ключом K = МИР.

Поскольку ключ шифратора Виженера является периодическим, зашифрованный текст можно представить, как m текстов, зашифрованных с помощью шифра сдвига. В рассмотренном примере символы с позициями 0 и 3 шифровались шифром сдвига с ключом $k = 1$; символы с позициями 1 и 4~– с ключом $k = 3$; с позициями 2 и 5 – ключом $k = 20$. Таким образом, зная длину ключевого слова K шифра Виженера, можно произвести взлом шифртекста, выполнив анализ частот встречаемости символов в отдельности для каждого из m компонент шифртекста.

Одним из методов определения длины ключевого слова, использованного при шифровании текста по методу Виженера, является метод Касиски, названный в честь Фридриха Касиски, который первым опубликовал этот метод. Метод Касиски основан на предположении, что наличие повторяющихся l-грамм (l-символьных последовательностей) в зашифрованном тексте будет в большинстве случаев обусловлено наличием соответствующих повторяющихся l-грамм в исходном тексте. Предполагается, что случайное появление в шифртексте повторяющихся l-грамм маловероятно. Одинаковым l-граммам, присутствующим в исходном тексте, будут соответствовать одинаковые l-граммы, расположенные на тех же позициях в шифртексте, только в том случае, если при шифровании они будут преобразованы с использованием тех же l символов ключа. Это условие будет выполняться для всех повторяющихся l-грамм, расположенных друг от друга на расстояниях, кратных длине ключевого слова шифра.

Тест Касиски состоит из следующих шагов:

1. Анализируется шифртекст на предмет присутствия в нём повторяющихся l-грамм.

2. Для каждой из встретившихся в шифртексте более одного раза l-граммы вычисляются расстояния между её соседними вхождениями.

3. Вычисляется наибольший общий делитель полученного на предыдущем шаге множества расстояний с учётом того, что среди найденных повторений *l*-грамм могут в незначительном количестве присутствовать случайные повторения. Полученное значение и будет являться длиной ключевого слова.

Эксперименты показывают, что данный метод является достаточно эффективным при анализе зашифрованных текстов на русском и английском языках в случае, если в тексте присутствуют повторяющиеся *l*-граммы длиной в три и более символов.

Начинающий криптограф Егор зашифровал небольшой отрывок известного литературного произведения с помощью шифра Виженера:

ЙССГЯ ИИХТЯ ЙЧРАШ ЭЗПНХ БТЕЕЬ ЛХЯБЬ ЁЛНОА ЛЛРАЫ ЛРЛТМ ОГФНХ ЗМЛМТ ЁПЯЯЭ ЛРОЕУ НДРОЭ ЛСТРЯ ЁХШОФ ЁПЛЗВ ПДУИЮ КТМГД АИРОГ ООСЙВ ВРЯИЩ ЮЯОПБ ВКЖЕС ЛЖГТЮ ЛСЗУФ ЭЫЛСЬ ВЗСВР ЯЬЛЕЯ БСГЗР БФЦГЯ ЖЗСВХ ИМЗГЯ БТРИЙ ВЦЮЧГ ЛЕЮИШ ЮИЁНД ПАЦНЩ ДИРИЪ ОЁВЗР КСЮХВ МТХЕБ ВНДОУ ЭЦФТТ ЭТРПЯ ЗМРУЬ КТЕЫЪ ЛФОЕР КЖСРЯ БХЕОЩ ТУУЕФ ЗТЕИА ЛХЗЛЩ ИХВНР ОБОЛЩ ЯДРОТ ЛРССГ НТЕЕА ЛЕОИШ ЛХХИЯ ПЫГРЬ ОЦСНР ЯВЙНЯ ЖОГРЯ ИМРЕ

Помогите хакеру Владу расшифровать исходное сообщение.

б) (5 баллов) Определите длину ключа.

в) (5 баллов) Укажите автора и название произведения, отрывок из которого зашифровал Егор.

Таблица частот встречаемости символов русского языка в осмысленных текстах.

А 0.07821	Б 0.01732	В 0.04491	Г 0.01698	Д 0.03103	Е 0.08567	Ё 0.00070
Ж 0.01082	З 0.01647	И 0.06777	Й 0.01041	К 0.03215	Л 0.04813	М 0.03139
Н 0.06850	О 0.11394	П 0.02754	Р 0.04234	С 0.05382	Т 0.06443	У 0.02882
Ф 0.00132	Х 0.00833	Ц 0.00333	Ч 0.01645	Ш 0.00775	Щ 0.00331	Ъ 0.00023
Ы 0.01854	Ь 0.02106	Э 0.00310	Ю 0.00544	Я 0.01979		