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 электронные адреса igor.bodiagin@gmail.com, m.kazlovski@gmail.com.

*Окончание приема решений задач заочного тура – **14 апреля 2019 г.***

Задача 1. Числовой ребус (2 балла)

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

EARTH + WATER + FIRE + AIR = NATURE.

В ответе укажите, какому числу соответствует слово TRUTH.

Задача 2. Телеграф (3 балла)

Некоторый алфавит состоит из шести букв, которые для передачи по телеграфу кодированы так: ·, –, · ·, – –, · –, – ·. При передаче одного слова не сделали промежутков, отделяющих букву от буквы, так что получилась сплошная цепочка точек и тире, состоящая из 12 знаков. Сколькими способами можно прочитать полученное слово?

Задача 3. Прогноз (5 баллов)

Суперкомпьютер предсказывает конкурс на бюджетную форму обучению ФПМИ БГУ на разные годы.

А) (2 балла) По его предсказаниям конкурс на ФПМИ в 2091 году составит 2.019(4) человека на место. Какое минимальное число абитуриентов должно поступать на ФПМИ согласно этому прогнозу?

Замечание: Запись (4) указывает то, что цифра 4 в дроби будет в периоде, т.е. 2.019(4) = 2.019444444…

Б) (3 балла) Согласно предсказаниям суперкомпьютера, конкурс на бюджет ФПМИ БГУ в 9102 году будет между 2.019042012 и 2.019042018 человека на место. Какое минимальное количество мест может быть на факультете?

Задача 4. Книжный шифр (5 баллов)

Книжный шифр – один из классических шифров. При его использовании каждый символ исходного сообщения заменяется на указание места, на котором этот же символ находится в тексте, играющем роль ключа. Одиннадцатиклассник Егор получил сообщение, которое было зашифровано книжным шифром. Егор не знает, какая именно книга использовалась для шифрования, но он имеет все основания предполагать, что это был один из школьных учебников за 11 класс, написанный на русском языке. Найти все подобные учебники в электронном виде можно здесь (https://uchebniki.by/rus/skachat). Помогите Егору расшифровать сообщение:

15-1-1	105-1-2	12-6-3	81-1-7	77-1-2	78-4-2	43-3-1	179-3-3
259-3-10	304-7-4	117-1-4	39-2-5	37-1-1	118-6-6	96-3-3	36-1-4
30-1-2	233-1-1	127-4-2	256-1-3	116-1-4	66-6-3	193-2-19	60-3-2
128-2-3	239-1-6	237-1-1	135-2-2	269-2-9	142-1-8	112-6-5	233-3-8
78-3-2	202-8-1	266-3-7	16-4-10	146-3-9	35-12-6	299-9-1	22-8-1
121-6-3	175-1-3	82-2-11	8-3-1	19-1-6	105-4-4	307-4-10	231-1-2
43-2-3	108-5-5	187-7-11	263-10-4	207-6-6	251-2-4	243-1-3	79-5-5
21-12-9	319-8-29	148-2-7	92-4-8	64-1-3	199-3-12	279-1-2	47-4-1
183-3-5	317-11-8						

Задача 5. Двойная перестановка (5 баллов)

Шифр двойной перестановки является разновидностью шифра перестановки. В нем текст записывается в прямоугольную таблицу, для которой задаются: порядок вписывания текста; порядок перестановки столбцов, порядок перестановки строк и порядок выписывания текста.

При этом вписывание и выписывание текста может осуществляться 8 способами: слева-направо или справа-налево, сверху-вниз или снизу-вверх, по строкам или по столбцам. Перестановка строк или столбцов задается в виде последовательности чисел от 1 до N, записанной в произвольном порядке, где N – количество строк или столбцов соответственно. Так, например, ключ вида (3, 1, 2, 4) для столбцов означает, что в шифртексте первым должен идти третий столбец, вторым – первый, третьим – второй и четвертым – четвертый.

А) (1 балл) Аналитик Иван зашифровал сообщение с помощью шифра двойной перестановки. Он использовал таблицу 4 × 6, в которую открытый текст был вписан слева-направо, сверху-вниз и по строкам, а шифртекст был выписан справа-налево, снизу-вверх и по столбцам. При этом перестановка для строк имела вид (4, 2, 3, 1), а для столбцов (3, 5, 2, 6, 4, 1). Полученное Иваном сообщение выглядит так: ВЗОЯШЕЕОМСЕ.НАТКЕЛЛТАВДР. Расшифруйте это сообщение.

Б) (4 балла) Разведчик Игорь получил сообщение, зашифрованное шифром двойной перестановки. К сожалению, он не обладает ключевой информацией, необходимой для расшифровки. Помогите Игорю расшифровать это сообщение, если он знает, что для шифрования использовалась таблица 6 × 6 и в самом конце исходного текста должен быть записан позывной агента, пересылавшего сообщение, – слово «павлин»: ЖПЙПСАЩВЕКОЕЕЛУИЧДВНЕАОТКИБДНУИАТОРМ.

Задача 6. Возвращение хакера Влада (6 баллов)

Хакер Влад пытается взломать сейф, код от которого он не знает. Код представляет собой 4 десятичные неповторяющиеся цифры. Влад может наугад ввести код и с помощью специального оборудования узнать:

- ✓ количество угаданных цифр, расположенных на своих местах;
- ✓ количество угаданных цифр, расположенных НЕ на своих местах.

А) (1 балл) Влад предпринял 4 попытки угадать код и получил следующие результаты:

1) 5634: угадано 0 цифр;
2) 3615: угадана 1 цифра, расположенная на своем месте;
3) 0265: угадано 2 цифры, расположенные НЕ на своих местах;
4) 9310: угадана 1 цифра, расположенная на своем месте, и 2 цифры, расположенные НЕ на своих местах.

Какой код сейфа?

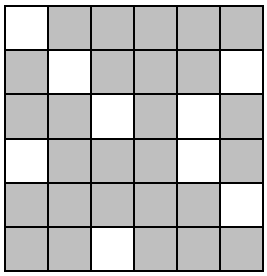
Б) (2 балла) В качестве первой попытки Влад ввел код 9876 и получил следующий результат: угаданы все 4 цифры, но они расположены НЕ на своих местах. Какое минимальное количество попыток (включая текущую) понадобится Владу, чтобы гарантированно открыть сейф?

В) (3 балла) В качестве первой попытки Влад ввел код 0123 и получил следующий результат: угаданы 3 цифры, которые расположены на своих местах. Какое минимальное количество попыток (включая текущую) понадобится Владу, чтобы гарантированно открыть сейф?

Задача 7. Решетка Кардано (7 баллов)

Решетка Кардано – широко известный способ, позволяющий скрыть секретное сообщение в некотором тексте. Решетка Кардано представляет собой лист прямоугольной формы, сделанный из картона, пергамента или тонкого металла, с вырезанными прямоугольными отверстиями. Шифрующий помещает решетку на лист бумаги и пишет сообщение в прямоугольных отверстиях, в каждое из которых помещается отдельный символ. Одна из разновидностей решетки Кардано – решетка квадратной формы $N \times N$ (N – четное число), в которой вырезано $N^2/4$ отверстий таким образом, чтобы при каждом повороте решетки на 90º в квадрате заполнялось $N^2/4$ новых символов. Тогда, заполнив символами каждое из 4 положений решетки, мы получим квадрат, полностью заполненный нашим сообщением, которое, по сути, будет зашифровано обычным шифром перестановки. Не каждая решетка, имеющая $N^2/4$ отверстий, подходит для шифрования (часто отверстия будут накладываться при повороте), однако показано, что, например, для $N = 8$ будет существовать 4^{16} таких решеток.

А) (1 балл) Помогите аспиранту Володе расшифровать сообщение НОИЕПЧГАЕРАЧСОИАНДАНАЯЙЦВИДНТТЮЯЕС.Р, если известно, что для шифрования использовалась следующая решетка Кардано (белые квадраты – вырезанные отверстия):



Б) (6 баллов) Криптоаналитик Сергей перехватил сообщение, зашифрованное с помощью решетки Кардано, которое приведено ниже. Кроме того, от агента Марии ему стало известно, что зашифрованное на решетке сообщение содержит в своем составе фрагмент «токены будут». Помогите Сергею расшифровать сообщение.

Е	Е	М	Н	Т	О	К	И
Н	Р	И	И	П	К	Е	Ы
И	П	Н	П	М	В	Т	О
Г	Э	Т	Ы	О	Р	А	И
Б	М	Г	Ф	И	И	Ч	О
Д	У	Е	У	Д	А	С	И
С	В	Е	У	Т	В	Л	В
Е	А	С	Т	К	Д	А	И

Задача 8. Шифр красной капеллы (7 баллов)

Шифр «Красной капеллы» использовался группами антинацистского движения Сопротивления для передачи секретных сообщений во время Второй мировой войны.

В качестве ключа в этом алгоритме выступают:

1) ключевое слово (для задания горизонтальных ключевых цифр);
2) условные цифры (для задания вертикальных ключевых цифр);
3) ключевой текст (для создания «случайных» ключевых цифр).

Алгоритм шифрования по нему имеет следующий вид:

1) Шаг 1. Строится матрица размера 4 × 9. В первую строку матрицы записывается ключевое слово, состоящее из 9 различных букв. Остальные строки матрицы заполняются оставшимися буквами в алфавитном порядке. Над буквами ключевого слова запишем числа, которые соответствуют порядку букв ключевого слова в алфавите. Слева от матрицы записываются 4 различные условные цифры. Так, если в качестве ключевого слова выберем «КНЯЖЕСТВО», а в качестве условных цифр «6742», то получим следующую матрицу (прочерки означают, что в соответствующих клетках нет никаких символов):

	4	**5**	**9**	**3**	**2**	**7**	**8**	**1**	**6**
6	К	Н	Я	Ж	Е	С	Т	В	О
7	А	Б	Г	Д	Ё	З	И	Й	Л
4	М	П	Р	У	Ф	Х	Ц	Ч	Ш
2	Щ	Ъ	Ы	Ь	Э	Ю	-	-	-

2) Шаг 2. Ставим в соответствие каждой букве открытого текста сначала ключевую цифру по вертикали, а затем ключевую цифру по горизонтали. Так слово «ПРИМЕР» будет записано как «54 94 87 44 26 94».
3) Шаг 3. Ставим в соответствие каждой букве ключевого текста ключевую цифру по вертикали. Так слово «АПЛОДИСМЕНТЫ» будет записано как «4 5 6 6 3 8 7 4 2 5 8 9» – это «случайные» ключевые цифры.
4) Шаг 4. Складываем цифры из шага 2 с цифрами из шага 3 по модулю 10 (то есть, находим остаток от деления их суммы на 10). Результат запишем группами по 5 цифр. Получим: «99501 51841 73».

А) (2 балла) Помогите научному сотруднику Валерию понять, какая фраза скрывается за цифрами «30493 72176 79502 29131 64390 5», если известно, что при шифровании использовалась матрица, полученная в примере для шага 1, а в качестве ключевого текста выступает начало 28-ой статьи Конституции РБ.

Б) (5 баллов) Криптограф Антон перехватил сообщение: «30747 33691 84619 66838 76646 49313 96375 59511». Помогите ему с расшифровкой, если известно, что при шифровании использовалась ключевое слово «МЕЗАЛЬЯНС», а в качестве ключевого текста выступают первые строки письма Татьяны к Онегину из романа в стихах А.С. Пушкина «Евгений Онегин».

Задача 9. Шифр нигилистов (9 баллов)

Шифр нигилистов – метод шифрования, который активно применялся движением нигилистов в России. В качестве ключа в этом алгоритме выступают:

1) первое ключевое слово (для построения квадрата);
2) второе ключевое слово (для сложения с числами, полученными на шаге 2).

Алгоритм шифрования по нему имеет следующий вид:

1) Шаг 1. Строится квадрат размера 6 × 6. В первую строку квадрата записывается первое ключевое слово, состоящее из 6 различных букв. Остальные строки квадрата заполняются оставшимися буквами в алфавитном порядке. В конец добавляются 3 символа: пробел, запятая и точка. Так, если в качестве первого ключевого слова выберем «ПРИВЕТ», то получим следующий квадрат:

	1	**2**	**3**	**4**	**5**	**6**
1	П	Р	И	В	Е	Т
2	А	Б	Г	Д	Ё	Ж
3	З	Й	К	Л	М	Н
4	О	С	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я		,	.

2) Шаг 2. Ставим в соответствие каждой букве открытого текста и второго ключевого слова сначала цифру по горизонтали, а затем цифру по вертикали. Так слово «ЗАДАНИЕ» будет записано как «31 21 24 21 36 13 15», а слово «МИР» как «35 13 12».
3) Шаг 3. Прибавляем числа, которые получились у второго ключевого слова к числам, полученным у открытого текста. Это и будет наш шифртекст. Так, если открытый текст был «ЗАДАНИЕ», а второе ключевое слово – «МИР», то получим «66 34 36 56 49 25 50»:

Числа, полученные из открытого текста	31	21	24	21	36	13	15
Второе ключевое слово	35	13	12	35	13	12	35
Шифртекст	66	34	36	56	49	25	50

А) (2 балла) Студент Борис получил сообщение: «65 45 67 63 79 63 77 67 64 48 106 74 72 85 77 75 49 71 65 102». Помогите ему расшифровать послание, если известно, что первое ключевое слово «РЕЗЬБА», а второе ключевое слово – «СЛОВО».

Б) (7 баллов) Нигилист Виктор передал двум агентурным группам одно и то же сообщение. Для первой группы он использовал шифрование по алгоритму, описанному выше, а для второй – по измененному алгоритму: на шаге 2 он ставил в соответствие каждой букве открытого текста сначала цифру по вертикали, а уже затем цифру по горизонтали. Сотрудник охранного отделения Юрий перехватил оба зашифрованных сообщения: «64 48 59 77 68 90 96 76 67 59 100 106 95 61 70 93 68 62 69 57 87 92 108 55 94 62 95 77 88 90 80 58 86 41 79 105 83 42 59 106 88 67 59 84 64 72 70 104 118 90» и «46 84 95 77 86 108 69 67 76 95 109 70 59 115 106 39 86 125 96 75 78 128 90 55 49 125 59 77 88 108 107 85 68 113 97 60 38 123 95 70 88 76 95 48 46 126 106 50 91 108». От агента Леонида он узнал, что второе ключевое слово – «ШИФР». Расшифрование сообщения Виктора – дело государственной важности!

Задача 10. Стеганография (10 баллов)

Стеганография – наука, изучающая способы сокрытия факта передачи информации. Специалист по информационной безопасности Максим, который любит представлять русский алфавит в двоичном виде («А» – 00000, «Б» – 00001, …, «Я» – 11111) и не любит букву «Ё», решил активно использовать простые приемы стеганографии в своей рабочей переписке. Попробуйте найти скрытую информацию в его сообщениях.

А) (1 балл) Криптография является одной из старейших наук, изучаемых людьми. Начиная с древнейших времен, человечеству приходилось обеспечивать конфиденциальность хранимой ими информации. Одним требовалось сохранить тайну, а другим – добыть ее. Криптографические методы использовалась в разных целях: начиная от получения личной выгоды торговцами, созданием интриг или передачей тайных любовных посланий, заканчивая такими важными вещами, как обеспечение конфиденциальности государственных тайн или ведением переговоров в сложных и трудных положениях для страны.

Б) (3 балла) Факультет прикладной математики и информатики БГУ – факультет Белорусского государственного университета, который готовит специалистов по следующим направлениям: прикладная математика (квалификация – «математик-программист»), информатика (квалификация – «математик-системный программист»), экономическая кибернетика (квалификация – «математик-экономист»), актуарная математика (квалификация – «математик-финансист»), компьютерная безопасность (квалификация – «математик, специалист по защите информации»), прикладная информатика (квалификация – «информатик, специалист по разработке программного обеспечения»).

В) (6 баллов) Следует отметить насыщенную студенческую жизнь факультета. Одним из важнейших событий являются проводимые в канун дня рождения факультета (первого апреля) "Дни ФПМИ". Программа этого праздника включает разнообразные традиционные развлекательные и спортивные конкурсы, соревнования и т.п., в которых участвуют студенты и преподаватели. Стоит также отметить туристическое спортивно-развлекательное мероприятие "Туртропа первокурсника", смотр-конкурс "Капустник", "Мисс ФПМИ" и "Мистер ФПМИ". Самые оперативные новости можно прочитать в красочном периодическом газетном издании "ФПМы".

Задача 11. Шифр непростой замены (11 баллов)

Шифр простой замены является одним из самых известных методов шифрования. В нем для каждой буквы открытого текста определена единственная соответствующая ей буква шифртекста. Данный метод прост в применении, но легко вскрывается с помощью частотного криптоанализа. Программист Михаил знает об этом недостатке, поэтому он решил усложнить данный метод шифрования. Алгоритм, которым он шифрует открытый текст, выглядит так:

1) Провести шифрование классическим шифром простой замены.
2) Поставить в соответствие каждой букве шифртекста двухзначное число, соответствующее ее порядковому номеру в алфавите (то есть, ‘А’ – «01», …, ‘Я’ – «33»).
3) Некоторые (случайно выбранные) из этих чисел записать в обратном порядке (например, вместо «01» – «10» или вместо «32» – «23»).

Попробуйте расшифровать текст, зашифрованный по этому алгоритму:

```
22 05 41 10 26 13 05 22 05 14 41 05 14 13 03 13 41 19 51 24 31 20 10 50
11 82 19 50 11 13 20 22 26 60 02 22 26 13 92 26 01 32 31 62 42 20 01 50
14 20 11 02 52 30 19 05 20 62 50 11 14 26 27 13 28 14 27 02 13 13 02 14
01 51 04 18 28 21 11 19 21 91 05 92 01 02 02 60 50 14 19 82 11 82 09 20
72 30 28 09 41 02 19 40 10 60 02 60 02 13 22 82 91 51 06 32 26 91 40 31
05 03 10 02 01 70 02 27 02 07 20 72 02 28 02 01 06 50 33 60 05 07 28 07
60 26 91 51 81 12 09 32 91 02 02 01 50 13 82 01 15 29 10 02 09 23 02 06
50 24 02 24 82 19 50 11 70 28 70 03 04 06 50 09 30 31 15 41 10 31 28 06
60 03 04 50 19 50 81 28 72 82 13 02 29 06 30 40 41 05 01 30 28 20 05 04
22 50 41 01 62 31 50 22 50 14 41 50 14 31 30 13 41 19 15 11 26 41 15 22
28 06 62 20 31 02 90 31 50 10 26 19 15 06 20 02 10 60 20 14 50 19 05 14
51 07 19 40 09 32 22 14 10 13 82 06 06 20 14 10 21 22 18 28 27 28 31 70
82 22 50 42 13 20 29 26 52 62 31 03 60 31 62 22 05 14 01 62 31 13 03 31
14 91 51 11 02 81 27 91 82 11 19 21 91 17 50 13 22 30 24 20 31 60 28 18
11 82 06 05 62 22 27 31 82 60 60 50 06 27 14 70 20 01 02 13 28 12 14 24
62 02 50 82 19 50 18 50 31 20 11 82 19 28 14 15 06 82 24 31 20 05 18 11
02 13 14 10 11 26 31 31 62 19 62 52 03 10 20 90 23 19 24 02 19 60 23 52
22 30 01 29 05 06 28 41 02 29 62 06 15 42 23 08 60 23 22 05 30 14 28 22
50 05 20 92 62 06 15 70 02 31 02 01 70 20 25 08 62 62 25 29 01 02 01 62
70 28 14 82 62 01 14 21 22 05 41 14 50 41 31 30 31 14 19 15 02 06 28 90
32 91 82 01 02 23 62 25 90 91 20 60 31 05 06 70 02 52 41 80 62 26 52 24
20 29 01 50 11 31 11 02 62 31 19 05 06 06 62 26 29 26 22 42 02 91 02 01
26 60 20 24 31 50 26 62 13 20 41 10 62 02 31 06 28 70 02 03 10 20 10 60
62 31 02 14 10 82 01 20 07 24 13 05 80 26 91 41 12 62 25 11 62 41 15 22
82 70 41 01 82 01 50 24 20 14 07 20 91 51 70 30 09 20 19 51 08 03 40 92
28 41 01 51 11 31 62 22 26 60 50 22 05 14 41 50 14 31 03 13 41 19 15 14
91 62 31 05 19 82 18 28 41 02 14 26 31 21 22 50 05 42 02 13 41 91 03 08
05 11 28 19 82 50 33 31 82 18 72 02 11 20 31 32 82 41 10 82 70 02 25 08
62 26 52 07 82 70 30 06 26 26 09 32 91 02 02 92 62 60 15 30 13 20 09 60
20 18 28 27 19 12 13 32 11 28 01 51 18 82 29 03 10 50 26 81 82 09 02 13
23 30 22 50 41 10 26 31 82 05 22 05 14 41 50 41 13 03 31 41 91 15 90 32
91 22 82 91 62 60 51 70 05 25 41 32 60 42 20 50 22 26 06 50 13 28 31 19
50 05 42 20 50 33 22 06 26 60 05 04 02 06 90 23 19 41 82 22 32 22 29 30
31 26 41 06 23 22 31 62 09 62 60 70 20 22 06 82 14 11 62 10 62
```