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 желаете или не можете, 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 m.kazlovski@gmail.com, igor.bodiagin@gmail.com.

Окончание приема задач заочного тура – ***06 апреля 2020 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 на умножение (звездочки поставлены взамен любых цифр, как одинаковых, так и неодинаковых):

```
                Ф  П  М  И
                Ф  П  М  И
             *  *  *  *  *
          *  *  *  *  *
       *  *  *  *  *
    *  *  *  *  *
-------------------------
*  *  *  *  Ф  П  М  И
```

В ответе укажите, какому числу соответствует слово МИФ.

Задача 2. Игорь и шифр гаммирования (4 балла)

Известно, что математик Игорь использует шифр гаммирования. Если на вход шифратора поступает открытый текст x_1, x_2, ..., x_n, то на выходе будет шифрованный текст y_1, y_2, ..., y_n:

$$y_i = (x_i + \gamma_i) \bmod 31,$$

где запись "... mod 31" означает нахождение остатка при делении на 31.

Функция выработки гаммы выглядит следующим образом:

$$\gamma_i = f(\gamma_{i-1}) = (a\gamma_{i-1}^2 + b\gamma_{i-1} + c) \bmod 31, \ i = 1, 2, \ldots.$$

где $a, b, c \in \{0, 1, \ldots, 30\}$ – секретные параметры, γ_0 – секретный параметр инициализации. Помогите шифровальщику Олегу узнать параметры a, b, c, если он перехватил открытый текст и соответствующий ему шифртекст:

ВСЕ_ГОТОВО
ЦЮФАХЧСДРЯ

В ответе укажите сумму $a + b + c$.

Учтите, что таблица соответствия символов алфавита и чисел имеет вид.

_	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	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Задача 3. Володя и Егор (6 баллов)

Атбаш – простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите. Для русского алфавита это выглядит следующим образом:

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

Старший научный сотрудник Володя и заведующий лабораторией Егор стали уделять особое внимание защите информации о своих планах. Для этого все свои сообщения они защищают шифром Атбаш. Вот и сегодня Володя получил следующее послание:

СРЧКТЫЧ Э ИЪОЭЪРЬ, ЭТЭТ. ИЯЦ СТСГЩФ Ч СЧРТШХЧ СТХНЖЯЪФ

Но вот беда – Егор очень рассеянный, поэтому он пропустил несколько букв, когда выписывал алфавит. Теперь у Володи не получается прочесть сообщение Егора с помощью стандартной замены для используемого шифра. Окажите содействие Володе и расшифруйте сообщение.

Задача 4. Перестановка с пробелами (7 баллов)

Криптоаналитик Сергей перехватил сообщение, которое было зашифровано шифром перестановки. В этом шифре используется прямоугольная таблица, число столбцов в которой равно длине ключа, а сообщение в нее записывается по строкам слева направо. Далее столбцы переставляются местами в соответствии с ключом. После этого шифртекст выписывается по строкам слева направо.
Например, сообщение СТУДЕНТБГУ при шифровании на ключе (3, 1, 4, 2) примет вид ТДСУНБЕТУГ.

А) (1 балл) От своей помощницы Анастасии Сергей получил информацию, что при шифровании очередного сообщения использовался ключ (2, 5, 8, 7, 9, 3, 6, 10, 4, 1). Помогите Сергею расшифровать сообщение:

ИСОЧРНЧОНАУНЭКАВТЙЕАЖАРУЦАЮИВГАЕМАРАДЯОА

Б) (6 баллов) Сергей получил очередное сообщение и хочет его расшифровать, но, к сожалению, ключ шифра перестановки неизвестен. Единственная подсказка была получена от агентессы Марии, которая сообщила, что перед шифрованием все пробелы между словами были заменены на слово «ПРОБЕЛ». Сергей рассчитывает на вашу помощь (учтите, что пробелы в шифртексте служат лишь для удобного восприятия и не обозначают пробелы между словами).

ЕБСОР МНАДП ЛООБО ЛРППТ РЕЬЕТ РЕБВО РПАВД ПЛЕРА ЗРАЛО ОБЕГП
ЛББОЛ РПБЕЛ ВЕЕСЕ СИЛЛЕ ЮЗПРБ КОЧЕБ ВОРОЕ НИПЛЯ ЗОРЕП ЕЛМОЖ
ОБННЛ ЕРБОЕ АМИРП ПДРПБ ОТЕПР ИЯОНЛ ЕДАЛЕ ЕИПРБ ЛОТОЛ НЕБАС
ЯПОДР КИНАЛ ЕКОПР БКОИА ГАЛЕН ХПРБР ОТЧЛО ЕБПИЙ ПОТРР СЫИЗА
ВОБЕР КЛАЕБ УОРДЕ МЫПЛХ АЕБВО РЗСТС ПЛЯЯС ЛГЕБО ТЬПОЕ РДИЛИ
ЕБПНЯ ПОЛРР ПЕОЖА БОБЕД РЛЕРП БАРЕЛ ЗАТОВ ЛЛЕПБ ОРНЕТ РИПОР
ПБЬТЕ БЕЛЫО БЛМЛЖ ЕБЕНЕ ПООРТ ОГОЕЛ ВПРОЕ РБЪ

Задача 5. Хакер Влад и представление числа (8 баллов)

Хакеру Владу удалось взломать телефон жертвы и выяснить код от сейфа. Довольный собой, хакер поспешил к сейфу, чтобы открыть его, но неожиданно столкнулся с серьезной проблемой: сейф имел только клавиши «0», «1» и «-1». Выяснилось, что сейф работает по следующим правилам:

1. При первом нажатии на клавишу число, соответствующее нажатой клавише, заносится в память сейфа.
2. При втором и последующих нажатиях на клавиши число, соответствующее нажатой клавише, умножается на 2 в степени на единицу меньше, чем номер нажатия (например, на $2^{(5-1)} = 16$ для пятого нажатия), и суммируются с числом в памяти сейфа.
3. Если число в памяти сейфа станет равным коду от сейфа, то сейф откроется.
4. Если в процессе ввода числа суммарное число нажатий клавиш «1» и «-1» будут больше некоторого значения, то содержимое сейфа будет уничтожено.
5. Известно, что сейф всегда можно открыть так, чтобы содержимое не было уничтожено.

Например, если бы кодом от сейфа было число 7, то его можно было бы открыть, нажимая клавиши следующим образом:

- $[1, 1, 1] = 1 + 1 \times 2^1 + 1 \times 2^2 = 1 + 2 + 4 = 7$;
- $[1, -1, 0, 1] = 1 - 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 = 1 - 2 + 0 + 8 = 7$;
- $[1, 1, -1, 1] = 1 + 1 \times 2^1 - 1 \times 2^2 + 1 \times 2^3 = 1 + 2 - 4 + 8 = 7$;
- $[-1, 0, 0, 1] = -1 + 0 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 = -1 + 0 + 0 + 8 = 7$.

Заметим, что содержимое сейфа гарантированно не будет уничтожено только при использовании последнего варианта, поскольку используя лишь одно нажатие «1» или «-1» получить 7 очевидно невозможно.

Помогите Владу открыть сейф и гарантированно сохранить его содержимое, если:

А) (2 балла) кодом от сейфа является число 61;

Б) (6 баллов) кодом от сейфа является число 110420.

В ответе надо указать последовательность нажатий клавиш сейфа.

Задача 6. Возвращение Максима (8 баллов)

Стеганография – наука, изучающая способы сокрытия факта передачи информации. Специалист по информационной безопасности Максим придумал несколько новых способов, которыми можно скрыть факт передачи информации в прозаических текстах писем. В них выбор нужных букв осуществляется по какому-либо правилу, например, читается только вторая буква каждого слова. Попробуйте найти скрытые им сообщения.

А) (2 балла) *В Хобитонее был переполох. Ггосподин Бильбо Сумниксс, хозяин Засумок объявил о намерении отпраздновать свое сттоодиннадцатилетие и пообещал очень щедрое угощение. Во всем Шире Бильбо слыл богатым чудаком с тех самых пор, как шестьдесят лет назад сначала запропал куда-то, а потом ввернулся, как снег на голову невесть откуда. О сокроовищах, добытых Бильбо за тридевять земель, ходилли неуутихающие легенды. Многие верили, что подземелья Засумок ломятся от кладов. Но не только предполагаемое богатство заставляло хоббитов поглядывать*

на Бильбо с недоверччивым удивлением. Годы шли и шли, а по господину Сумниксу этого было не заметить. В свои девяносто он выглядел едва ли на пятьдесят. В девяносто девять его называли «хорошшо сохранившшийся», хотя правильнее было бы сказать «ничуть не изменившиййся». Некоторые качали головами - дескать, многоввато для одного, нечестно быть и очень богатыым, и, очень здоровым одновременно. «Это даром не пройдет, - говорили они, — вот увидите, как ббы расплачиваться не пришлоось» Но пока об оплате не было и рречи.

Подсказка: исскуство

Б) (2 балла) *В доме № 4 по Тисавой улице во время завтрака разразился очередной скандал. Ранним утром мистер Вегнон Дурсль проснулся от громкого уханье совы, долетевшего из комнаты пленянника.*
— Третий раз за неделю! — проревел он, сатясь во главе стола. — Вышвырни ее немедленно, коль не сумеешь с ней управляться.
— Вове в клетке скучно, — в который раз пренялся объяснять Гарри. — Она вольная ртица. Хорошо бы выпускать ее хоть на ночь.
— Я что, по-твоему, идиот? Не знаю, что от сов именно ноччю жди неприятностей?
Дядя Вернон переглянулся с жоной и вытер усы, в которых запутались кусочки яичницы. Гарри хотел кто-то возразить, открыл выло рот, но кузен Дадли, смочно рыгнув, заяпил:
— Хачу еще бекона! — Возьми, сеточка, со сковородки. Нам еще много, — скозала тетя Сетунья, и глаза ее от умиления увлажнились. — Тушай на здоровье, пока есть возможность. Школьная еда просто отвратитильна!

В) (4 балла) *Коля тот, вчерашний, звонок пропустил. Между прочим, вместе сегодня забыли позвонить. В целом, ему зуб рвали. Никак не навещу. Я конфет ему принесу. Пока.*

Подсказка: оно.

Задача 7. Простой шифр простой замены (9 баллов)

Одним из самых известных методов шифрования является шифр простой замены. В нем для каждой буквы открытого (исходного) текста определена единственная соответствующая ей буква шифртекста. Данный метод прост в применении, но при этом легко вскрывается с помощью частотного криптоанализа. Единственная проблема при использовании данного шифра может быть связана с ключом, так как точно запомнить порядок 33 букв (для русского языка) достаточно непросто. Одним из способов решения этой проблемы является использование ключевого слова. В этом случае алгоритм формирования ключа может быть следующим:

1. Выбирается ключевое слово некоторой длины.
2. Слово побуквенно просматривается слева направо, если текущая буква уже встречалась ранее, то текущая буква удаляется.
3. Все буквы алфавита, которые так и не встретились в слове, дописываются после слова в алфавитном порядке.

Например, если ключевое слово – КРИПТОГРАФ, то ключом будет следующая строка: КРИПТОГАФБВДЕЁЖЗЙЛМНСУХЦЧШЩЪЫЬЭЮЯ. Это означает, что при шифровании буква "А" перейдет в букву "К", буква "Б" – в "Р" и т.д., "Я" – в "Я".

А) (1 балл) Лаборант Ольга получила зашифрованное с помощью шифра простой замены сообщение. Ей известно, что ключевое слово – «ИНСПЕКТОР». Помогите Ольге расшифровать сообщение:

ВЁИДКЕКМЗЙЖСКЙВИЁИЧАЁИБМКУЁАЧМЖОКЁАКУГАВ

Б) (7 баллов) Аналитик Иван перехватил зашифрованное с помощью шифра простой замены сообщение. Аудитор Полина сообщила ему, что ключ был сформирован по описанному выше алгоритму. Помогите Ивану расшифровать это сообщение (пробелы в шифртексте служат лишь для удобного восприятия и не обозначают пробелы между словами, перед шифрованием все пробелы и знаки препинания из сообщения были удалены).

ОЗМПЛ РКМНВ ЮЖЖРЭ ВДРМН ЪЙЮКЮ ХДРВК ПГАЗК ОРЖРЙ ЮНКЗО КРЛМГ
ЗОЗМЗ ВЮНРК РЕЗФА ТАМЗД ЛРНМГ АТЛЮЙ ПНРНЗ ВВЗЮЖ ЖЗКЮВ ЗДЬУА
ЗЖЖЗО ЗГЗЁА НЮНРМ НЗЭЧЮ ОЗВЗО ДРВЮЙ ЮНКЗО КРЛМГ ЗОЗЙК ЗДЮНР
КАРНР АОРКЖ АЯЗЖР ЛЮДЗЯ РГЗНЗ КЗЮЕЗ КЗДМЭ ЖРКЗЛ ЖЮЁЮЛ ДЮЖЖЗ
ЮЙКЮЛ ДЗИЮЖ АЮЛЮЁ ЗГКРН АФЮМГ ЗОЗЁА КРЗНЁ ЮЖРЙЗ ЁЮЧАФ ЪЮБМЗ
ЕМНВЮ ЖЖЗМН АЖРЯЮ ЁДЬКР ЕЗФАБ ГЗЖНК ЗДЪЖР ЛЙКЗА ЯВЗЛМ НВЗЁМ
ЗЯЛРЖ АЮМЗВ ЮНМГЗ ОЗЙКР ВАНЮД ЪМНВР ЫНЗЛЮ ДЗЗЕЮ МЙЮФЮ ЖЗ

В) (1 балл) Студенты Роман и Руслан спорят о том, в каком случаем количество различных ключей будет больше. Роман считает, что ключей будет больше при использовании латинского алфавита (26 букв), когда в качестве ключа выбирается случайная перестановка символов алфавита. Руслан же считает, что лучше использовать русский алфавит (33 букв), но при этом первые 8 букв ключа – случайное восьмибуквенное русское слово, в котором нет повторяющихся букв, а остальные 25 букв – оставшиеся буквы русского алфавита в случайном порядке. Кто из ребят прав?

Задача 8. Михаил и Unix-time (9 баллов)

Unix-time – одна из систем описания моментов во времени. Она определяется количеством секунд с полуночи (00:00:00 UTC) 1 января 1970. Так, например, полдень (12:00:00 UTC) 5 января 1970 года будет представлен числом 388800. Перед криптографом Михаилом встала задача – зашифровать определенное время в формате Unix-time. Недолго думая, он решил использовать шифр перестановки и получил результат 7404610914.

А) (3 балла) Укажите количество вариантов расшифровки указанного времени в формате Unix-time.

Б) (3 балла) (00:00:00 UTC) 1 января 2016 года описывается числом 1451606400. В 2016 году 366 дней. Укажите количество вариантов расшифровки указанного времени в формате Unix-time для 2016 года.

В) (3 балла) Укажите месяц зашифрованной даты, если дата соответствует полуночи (00:00:00 UTC) 30 числа искомого месяца 2016 года.

Задача 9. Роковые ошибки кодировщиков (10 баллов)

Кодировщик Артем передал сообщение с помощью азбуки Морзе. Однако при передаче он допустил ошибку, и поэтому сообщение было отправлено без пробелов (то есть исчезли пробелы как между буквами в одном слове, так и между словами). Кодировщик Егор, получив сообщение, записал его в виде строки из символов «0» и «1», но забыл указать, какой символ отвечает за точку, а какой – за тире. Помогите их начальнику Юрию восстановить исходное сообщение по полученной строке (пробелы в ней служат лишь для удобного восприятия и не обозначают пробелы между буквами/словами).

```
01110 11111 00000 00100 00101 11111 10101 11010 11110 10000
11100 00010 11111 10000 01011 10001 10010 00011 01100 00101
11100 10000 10000 11010 11000 00101 00001 00001 10101 10111
00010 11000 01101 01100 10100 01001 11100 00101 11101 0000
```

В ответе укажите ответ на вопрос, сформулированный в сообщении.

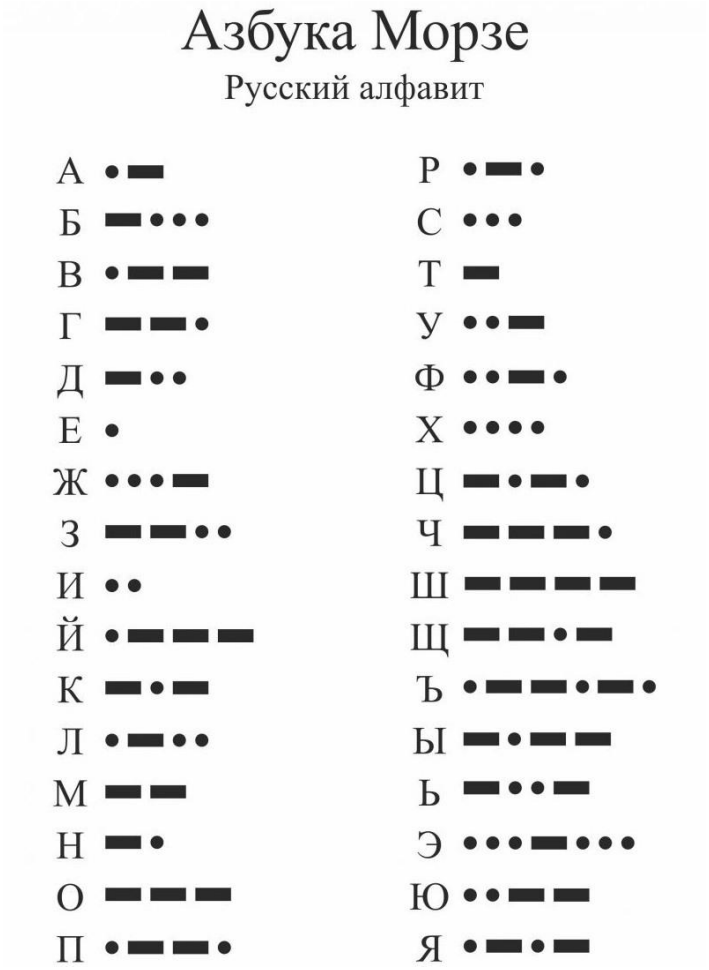

Рисунок 1. Таблица кода Морзе