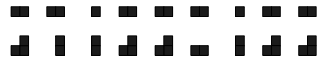
XVIII Межрегиональная олимпиада школьников по математике и криптографии

8-9 класс

Вариант 1

1. Цепочка ОДЕУПАРРЦ получена перестановкой букв в некотором слове. Имеется последовательность цифр, задающая порядок, в котором надо выписать буквы цепочки для получения исходного слова. Каждая цифра записывалась в прямоугольный шаблон размера 5 на 3 пикселей по образцу

При передаче часть пикселей на местах, одинаковых для каждой цифры, стерлись. Получилось вот что:



Восстановите исходное слово и перехваченную перестановку.

2. Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Табл. 1

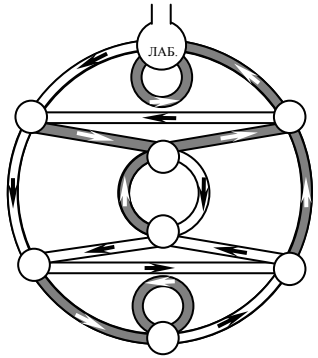
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей - **р**, четвертой - вновь **м** и т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

оутшякбёщысоахьббхфбнйоквуэкшхфщсёпръбшепянб

Восстановите исходное сообщение и ключевое слово.

3. На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошел сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещенными, возможно только по направлениям, указанным на схеме и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот.



Робот управляется командами из нулей и единиц, при этом 0 соответствует движению по освещенному коридору, а 1 – по неосвещенному. Передайте команду роботу, которая приведет его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более, чем на 5 минут.

4. В бесконечной последовательности цифр 5, 0, 4, 9, 3, 6 ... каждая цифра, начиная с четвертой, равна младшему разряду суммы трёх предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры 5, 0, 4.

5. Для наблюдения за страной Криптоландией запущен разведывательный спутник. Страна Криптоландия имеет форму прямоугольника. При этом спутник находится на расстоянии 700 км от одной вершины прямоугольника, на расстоянии 330 км от противоположной вершины прямоугольника и на расстоянии 650 км от третьей вершины прямоугольника. Найти расстояние от спутника до четвертой вершины прямоугольника.

6. Число n представляется в виде произведение двух чисел $n = p \cdot q$. Найти эти числа и привести решение, если известно, что

А. $n = 40003200063$, а $|p - q| = 2$.

Б. $n = 40000398401$, а p, q - простые и $|p - q| \le 100$.

XVIII

8-9 класс

РЕШЕНИЯ. ЗАПАД

Вариант 1

1. Исходя из характера стертых пикселей, нетрудно восстановить возможную перестановку, которой соответствуют варианты слов.
Ответы: слово - ПРОЦЕДУРА, перестановка – (571932486).

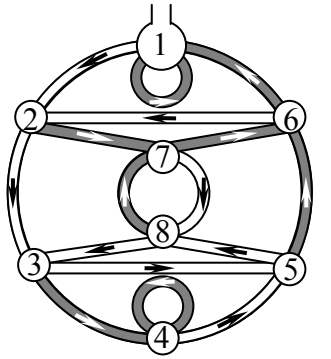
3			3	3			3	3	Е			Е	**Е**			Е	Е
5		1	5	5		4	5	5	**П**		У	П	П		**У**	П	П
6	7		6	6	2		6	6	А	**Р**		А	А	**Д**		А	**А**
8		4	8	8		1	8	8	Р		**О**	Р	Р		О	**Р**	Р
9			9	9			9	9	Ц			**Ц**	Ц			Ц	Ц

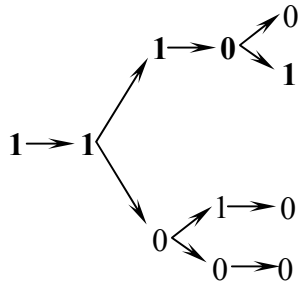
2. Убеждаемся, что шифрованный текст имеет длину 44. Осмысленная фраза имеет тогда длину 22. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв

о	**к**	**в**	**у**	**э**
о	**у**	**т**	**ш**	**я**
0	24	16	28	31

Если $x_1x_2x_3x_4x_5$ -ключевое слово, то для при первом шифровании использовалось оно само а при втором $x_3x_4x_5x_1x_2$. Таким образом, найденные разности равны соответственно $x_3 - x_1, x_4 - x_2, x_5 - x_3, x_1 - x_4, x_2 - x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формуле: $x_3 = x_1$, $x_5 = x_1 + 16$, $x_2 = x_1 + 14$, $x_4 = x_1 + 5$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: БОБЁР. При расшифровании получаем текст:
Н Е С Т О Й Т Е У К Р А Я П Л А Т Ф О Р М Ы Н Е С Т О Й Т Е У К Р А Я П Л А Т Ф О Р М Ы

3. На самом деле, граф, представленный на рисунке, является графом де Брейна некоторой равновероятной булевой функции и тогда задача сводится к поиску у данной функции полузапрета длины 5 такого, что в соответствующей системе сдвиговых уравнений определяться последние 3 неизвестные значениями (0,0,0). Однако, абитуриенты этого не знают и одним из возможных способов решения поставленной задачи будет нахождение путей длины 5, ведущих ИЗ заданной вершины (лаборатории, вершины №1), то есть куда и по каким коридорам за 5 шагов можно попасть из этой вершины, двигаясь ПРОТИВ стрелок. Сначала из нее можно попасть в вершины №1 и №6 и двигаться можно только по неосвещенным коридорам. Вершину №1 можно далее не рассматривать в связи с тем, что она образует цикл. Из вершины №6 можно попасть в вершины №7 и №5, двигаясь также по неосвещенным коридорам и т.д. Это приводит к построению следующего дерева, приведенного на рисунке. Остаётся перебрать 4 варианта, считывая последовательности справа налево. Истинный вариант: 10111 (выделен жирным).





XVIII

8-9 класс

РЕШЕНИЯ. ЗАПАД

Вариант 1

5. Решим задачу в общем виде. Пусть дана четырехугольная пирамида, основанием которой является прямоугольник. При этом расстояние от вершины пирамиды до одной вершины основания равно a, расстояние от вершины до противоположной вершины основания равно b, а расстояние до третьей вершины основания равно c. Найти длину четвертого бокового ребра d. Рассмотрим проекцию вершины пирамиды на основание точку P.

Пусть расстояние от точки P до сторон прямоугольника AB, BC, CD, AD равно x, y, z, v соответственно. Пусть также h - высота пирамиды. Тогда имеем следующие равенства для определения длин боковых ребер пирамиды:

$$x^2 + y^2 + h^2 = a^2$$
$$v^2 + z^2 + h^2 = b^2$$
$$y^2 + z^2 + h^2 = c^2$$

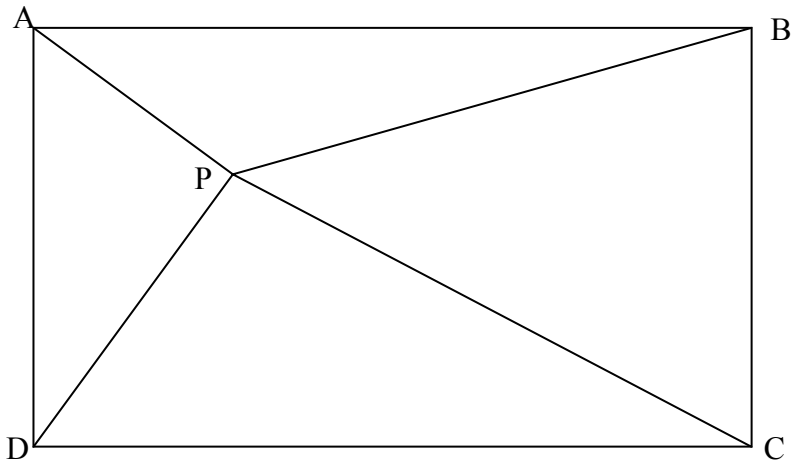
Длина четвертого (неизвестного) бокового ребра d выражается равенством

$$x^2 + v^2 + h^2 = d^2.$$

Из этих четырех равенств нетрудно получить равенство

$$a^2 + b^2 = c^2 + d^2,$$

то есть $d^2 = a^2 + b^2 - c^2$. Осталось подставить в полученное выражение известные значения a, b, c и найти $d = 420$ км.



6. для а): $p = x - 1,\ q = x + 1,\ 4003200063 = x^2 - 1,\ x^2 = 4003200064$. Нетрудно заметить, что $4003200064 = (200000 + z)^2$ и $z \in \{1, 2, \ldots, 9\}$ (небольшое). Число 4003200064 заканчивается на 64, следовательно $z = 8$.

(ответ: $p = 200007,\ q = 200009$)

для б): $n = x^2 - t^2,\ x^2 = n + t^2$. t - маленькое. $x > \sqrt{n}$. Из представленных чисел легко определяется целая часть корня $\sqrt{n}$ Это число – 200000. Оно увеличивается на единицу и возводится в квадрат (первый кандидат на x) и из полученного вычитается число n (кандидат для t^2). Проверяется, извлекается ли квадратный корень – он извлекается сразу же для первого кандидата и равен 40.

(ответ: $p = 199961,\ q = 200041$)

4. Последовательность состоит из цифр от 0 до 9. Так как число четверок (a,b,c,d) таких цифр конечно (и равно 10000), то в последовательности рано или поздно встретятся две повторяющиеся четверки. Пусть они встретились на i-м и j-м месте, $0 \le i < j$. Если i=0, то все доказано. Пусть i>0. (Сейчас доказано, что последовательность периодическая. Но нужно еще доказать, что она чисто периодическая.)

Закон рекурсии: $u_{i+4} = r_{10}(u_{i+3} + u_{i+2} + u_{i+1} + u_i)$ (*), где r_{10} – остаток от деления на 10. Заметим, что по заданным четырем членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если u_{i+4}, u_{i+3}, u_{i+2}, u_{i+1} известны, то существует единственное u_i, для которого выполняется рекуррентное соотношение (*). Поэтому если в последовательности совпали четверки на местах i и j, то совпадут четверки и на местах i–1 и j–1. И т.д. Поэтому совпадут четверки на местах 0 и j–i. Ч.т.д.

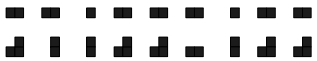
XVIII Межрегиональная олимпиада школьников по математике и криптографии

8-9 класс

Вариант 2

1. Цепочка ТСООВЕНЖМ получена перестановкой букв в некотором слове. Имеется последовательность цифр, задающая порядок, в котором надо выписать буквы цепочки для получения исходного слова. Каждая цифра записывалась в прямоугольный шаблон размера 5 на 3 пикселей по образцу

При передаче часть пикселей на местах, одинаковых для каждой цифры, стерлись. Получилось вот что:



Восстановите исходное слово и перехваченную перестановку.

2. Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Табл. 1

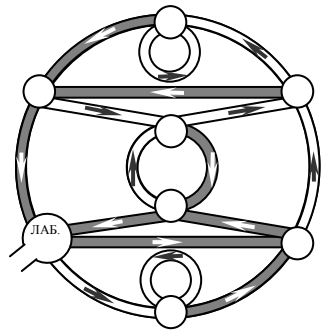
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей - **р**, четвертой - вновь **м** и т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

эущыёшоюнфкнрлжчерцкюммиёщсячшшдэйепдз

Восстановите исходное сообщение и ключевое слово.

3. На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошел сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещенными, возможно только по направлениям, указанным на схеме и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот.



Робот управляется командами из нулей и единиц, при этом 0 соответствует движению по освещенному коридору, а 1 – по неосвещенному. Передайте команду роботу, которая приведет его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более, чем на 5 минут.

4. В бесконечной последовательности цифр 7, 1, 2, 0, 3, 5 ... каждая цифра, начиная с четвертой, равна младшему разряду суммы трёх предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры 7, 1, 2.

5. Поместье Джеймса Бонда имеет прямоугольную форму. Для сохранения ключа к шифру, Джеймс Бонд закопал его в землю. При этом тайник оказался на расстоянии 46 м от одной вершины прямоугольника, на расстоянии 7 м от противоположной вершины прямоугольника и на расстоянии 22 м от третьей вершины прямоугольника. Найти расстояние от тайника до четвертой вершины прямоугольника.

6. Число n представляется в виде произведение двух чисел $n = p \cdot q$. Найти эти числа и привести решение, если известно, что

А. $n = 39996800063$, а $|p - q| = 2$.

Б. $n = 39999998911$, а p, q - простые и $|p - q| \le 100$.

XVIII

8-9 класс

РЕШЕНИЯ. ЗАПАД

Вариант 2

1. Исходя из характера стертых пикселей, нетрудно восстановить возможную перестановку, которой соответствуют варианты слов.
Ответы: слово – МНОЖЕСТВО, перестановка – (974862153).

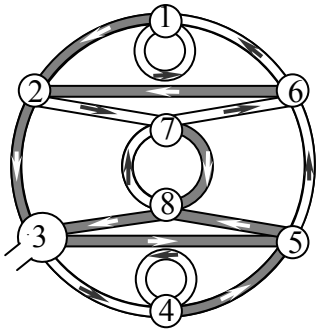
3			3	3			3	3		Ж			**Ж**	Ж			Ж	Ж	
5		1	5	5		4	5	5		О		Т	О	О		**Т**	О	**О**	
6	7		6	6	2		6	6		В	**Н**		В	В	**С**		**В**	В	
8		4	8	8		1	8	8		Е		**О**	Е	**Е**		О	Е	Е	
9			9	9			9	9		**М**			М	М			М	М	

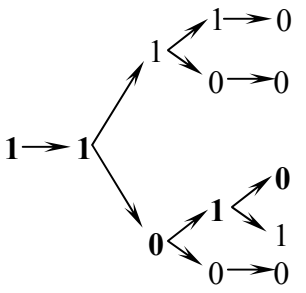
2. Убеждаемся, что шифрованный текст имеет длину 38. Осмысленная фраза имеет тогда длину 19. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв

к	**ю**	**м**	**м**	**и**
э	**у**	**щ**	**ы**	**ё**
14	11	20	18	3

Если $x_1x_2x_3x_4x_5$ -ключевое слово, то для при первом шифровании использовалось оно само а при втором $x_5x_1x_2x_3x_4$. Таким образом, найденные разности равны соответственно $x_5 - x_1, x_1 - x_2, x_2 - x_3, x_3 - x_4, x_4 - x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формуле: $x_5 = x_1 + 14$, $x_4 = x_1 + 17$, $x_3 = x_1 + 2$, $x_2 = x_1 + 22$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: КАМЫШ. При расшифровании получаем текст:
Т У М А Н Н О С Т Ь А Н Д Р О М Е Д Ы Т У М А Н Н О С Т Ь А Н Д Р О М Е Д Ы .

3. На самом деле, граф, представленный на рисунке, является графом де Брейна некоторой равновероятной булевой функции и тогда задача сводится к поиску у данной функции полузапрета длины 5 такого, что в соответствующей системе сдвиговых уравнений определяться последние 3 неизвестные значениями (0,1,1). Однако, абитуриенты этого не знают и одним из возможных способов решения поставленной задачи будет нахождение путей длины 5, ведущих ИЗ заданной вершины (лаборатории, вершины №3), то есть куда и по каким коридорам за 5 шагов можно попасть из этой вершины, двигаясь ПРОТИВ стрелок. Сначала из нее можно попасть в вершины №8 и №2 и двигаться можно только по неосвещенным коридорам. Из вершин №8 и №2 ведут пути только но неосвещенным коридорам в вершины №7, №5 и №1, 6 и т.д. Это приводит к построению дерева, приведенного на рисунке. Остаётся перебрать 6 вариантов, считывая последовательности справа налево. Истинный вариант: 01011 (выделен жирным).





РЕШЕНИЯ. ЗАПАД

Вариант 2

5. Решим задачу в общем виде. Пусть дана четырехугольная пирамида, основанием которой является прямоугольник. При этом расстояние от вершины пирамиды до одной вершины основания равно a, расстояние от вершины до противоположной вершины основания равно b, а расстояние до третьей вершины основания равно c. Найти длину четвертого бокового ребра d.
Рассмотрим проекцию вершины пирамиды на основание точку P.
Пусть расстояние от точки P до сторон прямоугольника AB, BC, CD, AD равно x, y, z, v соответственно. Пусть также h - высота пирамиды. Тогда имеем следующие равенства для определения длин боковых ребер пирамиды:

$$x^2 + y^2 + h^2 = a^2$$
$$v^2 + z^2 + h^2 = b^2$$
$$y^2 + z^2 + h^2 = c^2$$

Длина четвертого (неизвестного) бокового ребра d выражается равенством

$$x^2 + v^2 + h^2 = d^2 .$$

Из этих четырех равенств нетрудно получить равенство

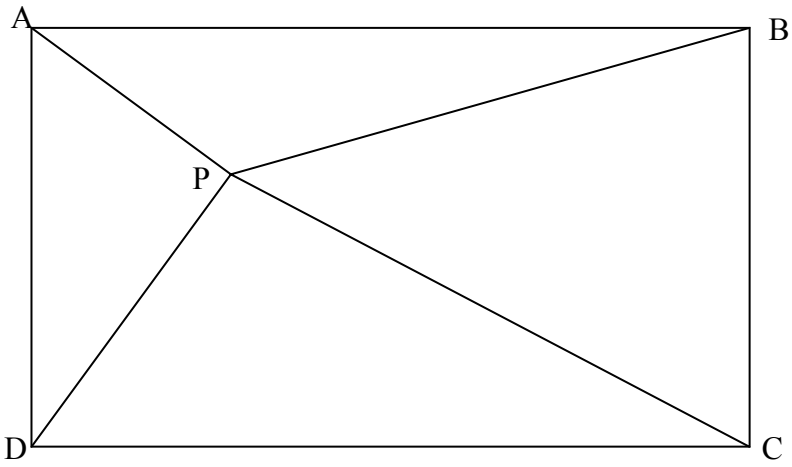
$$a^2 + b^2 = c^2 + d^2 ,$$

то есть $d^2 = a^2 + b^2 - c^2$.

Осталось подставить в полученное выражение известные значения a, b, c и найти $d = 41$ м.

6. для а): $p = x - 1,\ q = x + 1,\ 39996800063 = x^2 - 1,\ x^2 = 39996800064$. Нетрудно заметить, что $39996800064 = (200000 - z)^2$ и $z \in \{1, 2, \ldots, 9\}$ (не большое). Число 39996800064 заканчивается на 64, следовательно $z = 8$.
(**ответ:** $p = 199991,\ q = 199993$)

для б): $n = x^2 - t^2,\ x^2 = n + t^2$. t - маленькое. $x > \sqrt{n}$. Из представленных чисел легко определяется целая часть корня $\sqrt{n}$. Это число 199999. Оно увеличивается на единицу и возводится в квадрат (первый кандидат на x) и из полученного вычитается число n (кандидат для t^2). Проверяется, извлекается ли квадратный корень – он извлекается сразу же для первого кандидата и равен 33.
(**ответ:** $p = 199967,\ q = 200033$)



4. Последовательность состоит из цифр от 0 до 9. Так как число четверок (a,b,c,d) таких цифр конечно (и равно 10000), то в последовательности рано или поздно встретятся две повторяющиеся четверки. Пусть они встретились на i-м и j-м месте, $0 \le i < j$. Если i=0, то все доказано. Пусть i>0. (Сейчас доказано, что последовательность периодическая. Но нужно еще доказать, что она чисто периодическая.)
Закон рекурсии: $u_{i+4} = r_{10}(u_{i+3} + u_{i+2} + u_{i+1} + u_i)$ (*), где r_{10} – остаток от деления на 10. Заметим, что по заданным четырем членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если u_{i+4}, u_{i+3}, u_{i+2}, u_{i+1} известны, то существует единственное u_i, для которого выполняется рекуррентное соотношение (*). Поэтому если в последовательности совпали четверки на местах i и j, то совпадут четверки и на местах i–1 и j–1. И т.д. Поэтому совпадут четверки на местах 0 и j–i. Ч.т.д.

XVIII Межрегиональная олимпиада школьников по математике и криптографии

10 класс

Вариант 1

1. Делится ли число $2^{3^{2008}-1}-1$ на 165?

2. Число n представляется в виде произведение двух чисел $n=p\cdot q$. Найти эти числа и привести решение, если известно, что

А. $n=40003200063$, а $|p-q|=2$.

Б. $n=40000398401$, а p, q - простые и $|p-q|\le 100$.

3. В бесконечной последовательности цифр 2, 0, 0, 8, 0, 8, 6 ... каждая цифра, начиная с пятой, равна младшему разряду суммы четырех предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры 2, 0, 0, 8.

4. Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Табл. 1

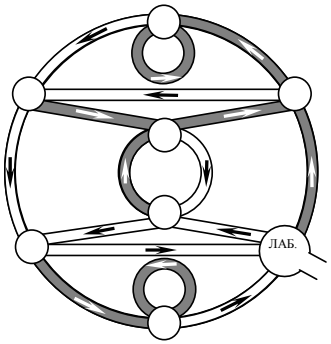
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей - **р**, четвертой - вновь **м** и т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

нпяхдйьичпулвниаугнисэемпутытмеугнисэещтбцытяичытртщъщтзпа

Восстановите исходное сообщение и ключевое слово.

5. На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошел сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещенными, возможно только по направлениям, указанным на схеме и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот.



Робот управляется командами из нулей и единиц, при этом 0 соответствует движению по освещенному коридору, а 1 – по неосвещенному. Передайте команду роботу, которая приведет его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более, чем на 6 минут.

6. Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо $1,2,...,L$. Зашифрование происходит путем перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b. Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a\cdot n+b$ на L (с одним исключением: если $a\cdot n+b$ нацело делится на L, то остаток полагается равным L). Например, если длина цепочки $L=25$ и $a=9, b=11$, то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (т.к. $9\cdot 3+11=38$, а число 38 дает остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

светитнезнакомаязвездасновамыоторваныотдома

была получена цепочка

ммаыасоявтзеовтреивзтадннаеысзоннтоадвкоаом

При этих же значениях a, b проведено зашифрование еще некоторой цепочки из 28 букв. Получилось вот что:

ыемхтвяксбаелкпосрнбоьейдлды

Найдите значения a и b и восстановите исходное сообщение.

XVIII

10 класс

РЕШЕНИЯ. ЗАПАД

Вариант 1

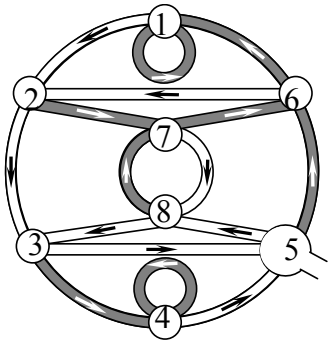
1. $165 = 3 \times 5 \times 11$. Число вида $2^k - 1$ делится на 3 тогда и только тогда, когда k четно, делится на 5 тогда и только тогда, когда k кратно 4, делится на 11 тогда и только тогда, когда k кратно 10. Число $3^{2008} - 1 = (3^{1004} - 1)(3^{1004} + 1)$ кратно 4. Число 3^{2008} в десятичной записи оканчивается на 1, поэтому $3^{2008} - 1$ делится на 10.

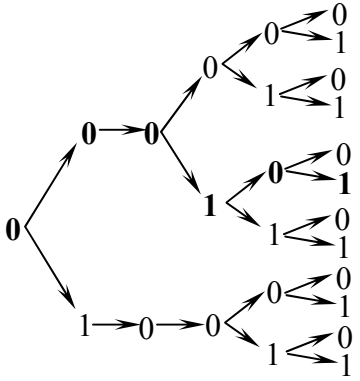
2. для а): $p = x - 1,\ q = x + 1,\ 4003200063 = x^2 - 1,\ x^2 = 4003200064$. Нетрудно заметить, что $4003200064 = (200000 + z)^2$ и $z \in \{1, 2, \ldots, 9\}$ (небольшое). Число 4003200064 заканчивается на 64, следовательно $z = 8$.
(ответ: $p = 200007,\ q = 200009$)

для б): $n = x^2 - t^2,\ x^2 = n + t^2$. t - маленькое. $x > \sqrt{n}$. Из представленных чисел легко определяется целая часть корня $\sqrt{n}$ Это число – 200000. Оно увеличивается на единицу и возводится в квадрат (первый кандидат на x) и из полученного вычитается число n (кандидат для t^2). Проверяется, извлекается ли квадратный корень – он извлекается сразу же для первого кандидата и равен 40.
(ответ: $p = 199961,\ q = 200041$)

3. Последовательность состоит из цифр от 0 до 9. Так как число четверок (a,b,c,d) таких цифр конечно (и равно 10000), то в последовательности рано или поздно встретятся две повторяющиеся четверки. Пусть они встретились на i-м и j-м месте, $0 \le i < j$. Если i=0, то все доказано. Пусть i>0. (Сейчас доказано, что последовательность периодическая. Но нужно еще доказать, что она чисто периодическая.)
Закон рекурсии: $u_{i+4} = r_{10}(u_{i+3} + u_{i+2} + u_{i+1} + u_i)$ (*), где r_{10} – остаток от деления на 10. Заметим, что по заданным четырем членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если u_{i+4}, u_{i+3}, u_{i+2}, u_{i+1} известны, то существует единственное u_i, для которого выполняется рекуррентное соотношение (*). Поэтому если в последовательности совпали четверки на местах i и j, то совпадут четверки и на местах i–1 и j–1. И т.д. Поэтому совпадут четверки на местах 0 и j–i. Ч.т.д.

5. На самом деле, граф, представленный на рисунке, является графом де Брейна некоторой равновероятной булевой функции и тогда задача сводится к поиску у данной функции полузапрета длины 6 такого, что в соответствующей системе сдвиговых уравнений определяться последние 3 неизвестные значениями (1,1,0). Однако, абитуриенты этого не знают и одним из возможных способов решения поставленной задачи будет нахождение путей длины 6, ведущих ИЗ заданной вершины (лаборатории, вершины №5), то есть куда и по каким коридорам за 6 шагов можно попасть из этой вершины, двигаясь ПРОТИВ стрелок. Сначала из нее можно попасть в вершины №3 и №4 и двигаться можно только по неосвещенным коридорам. Из вершины №3 можно попасть в вершины №2 и №8, двигаясь только по освещенным коридорам. Из вершины №4 можно попасть в вершины №4 и №3, двигаясь только по неосвещенным коридорам и т.д. Это приводит к построению следующего дерева, приведенного на рисунке. Остаётся перебрать 12 вариантов, считывая последовательности справа налево. Истинный вариант: 101000 (выделен жирным).





XVIII

10 класс

РЕШЕНИЯ. ЗАПАД

Вариант 1

4. Убеждаемся, что шифрованный текст имеет длину 58. Осмысленная фраза имеет тогда длину 29.
Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв

м	**е**	**у**	**г**	**н**
н	**п**	**я**	**х**	**д**
32	22	21	14	10

Если $x_1x_2x_3x_4x_5$ -ключевое слово, то для при первом шифровании использовалось оно само а при втором $x_5x_1x_2x_3x_4$. Таким образом, найденные разности равны соответственно $x_5 - x_1, x_1 - x_2, x_2 - x_3, x_3 - x_4, x_4 - x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формуле: $x_5 = x_1 + 32$, $x_4 = x_1 + 9$, $x_3 = x_1 + 23$, $x_2 = x_1 + 11$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: АКЦИЯ. При расшифровании получаем текст:
Н Е И М Е Й С Т О Р У Б Л Е Й А И М Е Й С Т О Д Р У З Е Й Н Е И М Е Й С Т О Р У Б Л Е Й А И М Е Й С Т О Д Р У З Е Й .

6. Для начала найдём в открытом тексте две уникальные буквы (по возможности близкие). Это например К и Я, стоящие соответственно на 12 и 16 позициях в открытом тексте. В шифрованном тексте они стоят соответственно на 39 и на 8.
Составляем систему уравнений

$$\begin{cases} 12a + b = 39 + 43k \\ 16a + b = 8 + 43l \end{cases}$$

Вычитая, получаем уравнение $4a = -31 + 43m$, при $m = 1$ находим $a = 3$, из первого уравнения находим $b = 3$.
Расшифровав второй текст, получим

всепройдеткаксбелыхяблоньдым

XVIII Межрегиональная олимпиада школьников по математике и криптографии

10 класс

Вариант 2

1. Делится ли число $3^{2^{2^{2008}-1}}-1$ на 143?

2. Число n представляется в виде произведение двух чисел $n=p\cdot q$. Найти эти числа и привести решение, если известно, что

А. $n=39996800063$, а $|p-q|=2$.

Б. $n=39999998911$, а p, q - простые и $|p-q|\le 100$.

3. В бесконечной последовательности цифр 1, 0, 2, 4, 7, 3, 6 ... каждая цифра, начиная с пятой, равна младшему разряду суммы четырех предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры 1, 0, 2, 4.

4. Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Табл. 1

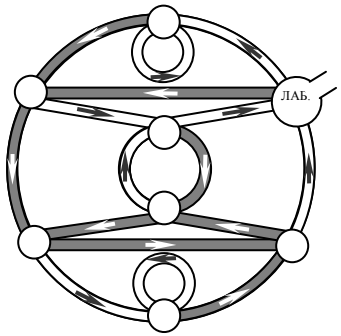
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей - **р**, четвертой - вновь **м** и т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

мхлщлифцбдюгишсптаивпбьдюолдьуэюыйемхл

Восстановите исходное сообщение и ключевое слово.

5. На космической станции, состоящей из отсеков (круглых комнат) и соединяющих их коридоров, произошел сбой электроснабжения, в результате чего связь с роботом, работающим на станции, прервалась. После восстановления работы станции выяснилось, что движение по коридорам, половина из которых оказались неосвещенными, возможно только по направлениям, указанным на схеме и занимает 1 минуту для каждого коридора. При этом неизвестно, в каком отсеке находится робот.



Робот управляется командами из нулей и единиц, при этом 0 соответствует движению по освещенному коридору, а 1 – по неосвещенному. Передайте команду роботу, которая приведет его из любой комнаты в лабораторию (где находится выход). С момента начала движения робота его энергоснабжения хватит не более, чем на 6 минут.

6. Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо $1,2,...,L$. Зашифрование происходит путем перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b. Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a\cdot n+b$ на L (с одним исключением: если $a\cdot n+b$ нацело делится на L, то остаток полагается равным L). Например, если длина цепочки $L=25$ и $a=9, b=11$, то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (т.к. $9\cdot 3+11=38$, а число 38 дает остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

светитнезнакомаязвездасновамыоторваныотдома

была получена цепочка

тмндоаарсксввонаемонтавыияаотзмтнвыдееоозз

При этих же значениях a, b проведено зашифрование еще некоторой цепочки из 43 букв. Получилось вот что:

явонныптомояйнсбветревуьточбккаоолгйшсрике

Найдите значения a и b и восстановите исходное сообщение.

XVIII

10 класс

РЕШЕНИЯ. ЗАПАД

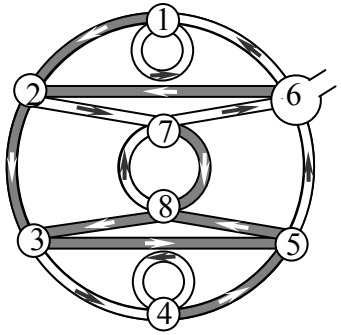
Вариант 2

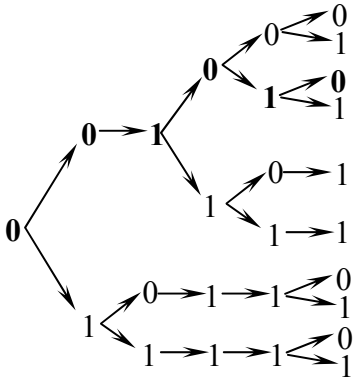
1. $143 = 11 \times 13$. Число вида $3^k - 1$ делится на 11 тогда и только тогда, когда k кратно 5, делится на 13 тогда и только тогда, когда k кратно 3. Число $2^{2008} - 1 = (2^{1004} - 1)(2^{1004} + 1)$ кратно 3, т.к. среди подряд идущих чисел $(2^{1004} - 1), 2^{1004}, (2^{1004} + 1)$ ровно одно делится на 3. Число 2^{2008} в десятичной записи оканчивается на 6, поэтому $2^{2008} - 1$ делится на 5.

2. для а): $p = x - 1,\ q = x + 1,\ 39996800063 = x^2 - 1,\ x^2 = 39996800064$. Нетрудно заметить, что $39996800064 = (200000 - z)^2$ и $z \in \{1, 2, \ldots, 9\}$ (не большое). Число 39996800064 заканчивается на 64, следовательно $z = 8$.
(**ответ:** $p = 199991,\ q = 199993$)

для б): $n = x^2 - t^2,\ x^2 = n + t^2$. t - маленькое. $x > \sqrt{n}$. Из представленных чисел легко определяется целая часть корня $\sqrt{n}$. Это число 199999. Оно увеличивается на единицу и возводится в квадрат (первый кандидат на x) и из полученного вычитается число n (кандидат для t^2). Проверяется, извлекается ли квадратный корень – он извлекается сразу же для первого кандидата и равен 33.
(**ответ:** $p = 199967,\ q = 200033$)

5. На самом деле, граф, представленный на рисунке, является графом де Брейна некоторой равновероятной булевой функции и тогда задача сводится к поиску у данной функции полузапрета длины 6 такого, что в соответствующей системе сдвиговых уравнений определяться последние 3 неизвестные значениями (0,0,0). Однако, абитуриенты этого не знают и одним из возможных способов решения поставленной задачи будет нахождение путей длины 6, ведущих ИЗ заданной вершины (лаборатории, вершины №6), то есть куда и по каким коридорам за 6 шагов можно попасть из этой вершины, двигаясь ПРОТИВ стрелок. Сначала из нее можно попасть в вершины №5 и №7 и двигаться можно только по освещенным коридорам. Из вершины №5 можно попасть в вершины №3 и №4, двигаясь только по неосвещенным коридорам. Из вершины №7 можно попасть в вершины №2, №8, двигаясь по освещенным коридорам и т.д. Это приводит к построению следующего дерева, приведенного на рисунке. Остаётся перебрать 10 вариантов, считывая последовательности справа налево. Истинный вариант: 010100 (выделен жирным).





3. Последовательность состоит из цифр от 0 до 9. Так как число четверок (a,b,c,d) таких цифр конечно (и равно 10000), то в последовательности рано или поздно встретятся две повторяющиеся четверки. Пусть они встретились на i-м и j-м месте, $0 \le i < j$. Если i=0, то все доказано. Пусть i>0. (Сейчас доказано, что последовательность периодическая. Но нужно еще доказать, что она чисто периодическая.)
Закон рекурсии: $u_{i+4} = r_{10}(u_{i+3} + u_{i+2} + u_{i+1} + u_i)$ (*), где r_{10} – остаток от деления на 10. Заметим, что по заданным четырем членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если u_{i+4}, u_{i+3}, u_{i+2}, u_{i+1} известны, то существует единственное u_i, для которого выполняется рекуррентное соотношение (*). Поэтому если в последовательности совпали четверки на местах i и j, то совпадут четверки и на местах i–1 и j–1. И т.д. Поэтому совпадут четверки на местах 0 и j–i. Ч.т.д.

XVIII 10 класс

РЕШЕНИЯ. ЗАПАД

Вариант 2

4. Убеждаемся, что шифрованный текст имеет длину 38. Осмысленная фраза имеет тогда длину 19. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв

в	**п**	**б**	**ь**	**д**
м	**х**	**л**	**щ**	**л**
22	27	22	3	25

Если $x_1x_2x_3x_4x_5$ -ключевое слово, то для при первом шифровании использовалось оно само а при втором $x_5x_1x_2x_3x_4$. Таким образом, найденные разности равны соответственно $x_5 - x_1, x_1 - x_2, x_2 - x_3, x_3 - x_4, x_4 - x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формуле: $x_5 = x_1 + 22$, $x_4 = x_1 + 14$, $x_3 = x_1 + 17$, $x_2 = x_1 + 6$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: КРЫША. При расшифровании получаем текст:
В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р В Е Р Б Л Ю Д Ы И Д У Т Н А С Е В Е Р.

6. Для начала найдём в открытом тексте две уникальные буквы (по возможности близкие). Это например К и Я, стоящие соответственно на 12 и 16 позициях в открытом тексте. В шифрованном тексте они стоят соответственно на 11 и на 27.
Составляем систему уравнений

$$\begin{cases} 12a + b = 11 + 43k \\ 16a + b = 27 + 43l \end{cases}$$

Вычитая, получаем уравнение $4a = 16 + 43m$, при $m = 0$ находим $a = 4$, из любого уравнения находим $b = 6$.
Расшифровав второй текст, получим

мневокошкопостучалсентябрьбагрянойветкойивы

XVIII Межрегиональная олимпиада школьников по математике и криптографии

11 класс

Вариант 1

1. Делится ли число $4^{2^{2008}+3^{2009}+1991}-1$ на 385?

2. На кодовом замке имеется круглый диск с риской. Вокруг диска нанесены числа от 0 до 99 по часовой стрелке. Для управления замком служат две кнопки: “вправо” и “влево”. При нажатии на кнопку “вправо” диск вращается на 43 деления по часовой стрелке, при нажатии на кнопку “влево” – на 20 делений против часовой стрелки. Каждая из этих операций выполняется за 1 секунду. Изначально замок установлен на число 0. Замок открывается при его установке на число 50 – ключ замка.

А. За какое наименьшее время можно открыть замок при данном ключе 50?

Б. Доказать, что замок можно открыть при любом ключе (ключ – число от 1 до 99).

В. За какое наименьшее время можно гарантированно открыть замок при любом ключе?

3. Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Табл. 1

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
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

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей - **р**, четвертой - вновь **м** и т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

оутшякбёщысоахьббхфбнйоквуэкшхфщсёпръбшепянб

Восстановите исходное сообщение и ключевое слово.

4. В бесконечной последовательности цифр 5, 0, 4, 9, 3, 6 ... каждая цифра, начиная с четвертой, равна младшему разряду суммы трёх предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры 5, 0, 4.

5. При каких значениях параметра a уравнение

$$a\cdot\left(x^6-2x^3+1\right)+\left(a+1\right)\cdot\left|x^3-1\right|-2a=2$$

имеет ровно четыре различных решения?

6. Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо $1,2,...,L$. Зашифрование происходит путем перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b. Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a\cdot n+b$ на L (с одним исключением: если $a\cdot n+b$ нацело делится на L, то остаток полагается равным L). Например, если длина цепочки $L=25$ и $a=9, b=11$, то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (т.к. $9\cdot3+11=38$, а число 38 дает остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

светитнезнакомаязвездасновамыоторваныотдома

была получена цепочка

завзавсанневмаызеыкодтоотаитмдстоаоннрямоев

При этих же значениях a, b проведено зашифрование еще некоторой цепочки из 29 букв. Получилось вот что:

иьлуснкиттоопвапрлкноаыотлбвн

Найдите значения a и b и восстановите исходное сообщение.

РЕШЕНИЯ. ЗАПАД

Вариант 1

1. $385 = 5 \times 7 \times 11$. Делится, т.к. число $4^k - 1$ делится на 5 тогда и только тогда, когда k кратно 2, на 7 – тогда и только тогда, когда k кратно 3, на 11 – тогда и только тогда, когда k кратно 5; показатель степени, очевидно, четен. Далее, число $2^{2^{2008}} + 3^{2^{2009}} + 1991 = 2^{2^{2008}} - 1 + 3^{2^{2009}} + 1992$ делится на 3, поскольку $2^k - 1$ делится на 3 при четных k и 1992 делится на 3 по известному признаку делимости. Числа 3^{2009} и 2^{2008} в десятичной записи оканчиваются на 3 и 6 соответственно, поэтому $2^{2^{2008}} + 3^{2^{2009}} + 1991$ оканчивается на 0, т.е. делится на 5.

2. А. При нажатии u раз на кнопку “вправо” и v раз на кнопку “влево” замок установится на деление с номером $r_{100}(43u - 20v)$, где r_{100} означает остаток от деления на 100. Таким образом, нужно подобрать числа u, v такие, что $r_{100}(43u - 20v)=50$.

Далее, понятно, что достаточно подобрать число u, для которого $r_{100}(43u)= 50, 70, 90$, так как после этого замок можно установить на ключ 50, вычитая 20 несколько раз.
Будем действовать перебором: 43, 86, 129, 172, 215, 258, 301, 344, 387, 430. Значит 10 вправо, 4 влево, итого *14 секунд*. Как видно из сделанного перебора, меньше чем за 14 секунд не получится.

Б. Продолжим перебор, показывающий, на какие деления можно установить замок только кнопкой “вправо”: 0, 43, 86, 129, 172, 215, 258, 301, 344, 387, 430, 473, 516, 559, 602, 645, 688, 731, 774, 817, 860. Далее кнопкой “влево” можно уменьшать эти числа на 20. Поэтому чтобы можно было открыть замок при любом ключе, достаточно, чтобы среди перечисленных чисел встречались все остатки от деления на 20. Непосредственно видно, что это так. Следовательно, замок можно открыть при любом ключе.

В. Нужно найти u, v такие, что $r_{100}(43u - 20v)=k$, где k – ключ. Если $u \geq 20$, то можно уменьшить u на 20 следующим образом: $43u–20v=43(u–20) –20(v–43)$. Следовательно, кнопку “ вправо” имеет смысл жать не более 19 раз. При этом получим все остатки от деления на 20, как видно и из перебора, сделанного в п.2. Затем кнопку “влево” жмем не более 4 раз. Таким образом, в выражении $r_{100}(43u – 20v)=k$ числа u, v заключены в пределах $0 \leq u \leq 19$, $0 \leq v \leq 4$. Итого 19+4=*23 секунд*.

4. Последовательность состоит из цифр от 0 до 9. Так как число четверок (a,b,c,d) таких цифр конечно (и равно 10000), то в последовательности рано или поздно встретятся две повторяющиеся четверки. Пусть они встретились на i-м и j-м месте, $0 \leq i < j$. Если i=0, то все доказано. Пусть i>0. (Сейчас доказано, что последовательность периодическая. Но нужно еще доказать, что она чисто периодическая.)
Закон рекурсии: $u_{i+4}=r_{10}(u_{i+3}+u_{i+2}+u_{i+1}+u_i)$ (*), где r_{10} – остаток от деления на 10. Заметим, что по заданным четырем членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если u_{i+4}, u_{i+3}, u_{i+2}, u_{i+1} известны, то существует единственное u_i, для которого выполняется рекуррентное соотношение (*). Поэтому если в последовательности совпали четверки на местах i и j, то совпадут четверки и на местах i–1 и j–1. И т.д. Поэтому совпадут четверки на местах 0 и j–i. Ч.т.д.

6. Для начала найдём в открытом тексте две уникальные буквы (по возможности близкие). Это например К и Я, стоящие соответственно на 12 и 16 позициях в открытом тексте. В шифрованном тексте они стоят соответственно на 19 и на 39.
Составляем систему уравнений

$$\begin{cases} 12a + b = 19 + 43k \\ 16a + b = 39 + 43l \end{cases}$$

Вычитая, получаем уравнение $4a = 20 + 43m$, при $m = 0$ находим $a = 5$, из первого уравнения находим $b = 2$.
Расшифровав второй текст, получим

кораблиплывутвконстантинополь

РЕШЕНИЯ. ЗАПАД

Вариант 1

3. Убеждаемся, что шифрованный текст имеет длину 44. Осмысленная фраза имеет тогда длину 22. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв

о	**к**	**в**	**у**	**э**
о	**у**	**т**	**ш**	**я**
0	24	16	28	31

Если $x_1x_2x_3x_4x_5$ -ключевое слово, то для при первом шифровании использовалось оно само а при втором $x_3x_4x_5x_1x_2$. Таким образом, найденные разности равны соответственно $x_3-x_1, x_4-x_2, x_5-x_3, x_1-x_4, x_2-x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формуле: $x_3=x_1$, $x_5=x_1+16$, $x_2=x_1+14$, $x_4=x_1+5$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: БОБЁР. При расшифровании получаем текст:

Н Е С Т О Й Т Е У К Р А Я П Л А Т Ф О Р М Ы Н Е С Т О Й Т Е У К Р А Я П Л А Т Ф О Р М Ы

5. Сделаем замену переменных $y=\left|x^3-1\right|$.. Во-первых, рассмотрев график функции $y=\left|x^3-1\right|$ (или любым другим стандартным способом), можно сделать вывод, что

- минимальное значение величины $y=\left|x^3-1\right|$ равно 0 (при $x=1$),
- множество значений величины $y=\left|x^3-1\right|$ имеет вид $[0;+\infty)$,
- для любого $c\in(0;+\infty)$ уравнение $y=\left|x^3-1\right|$ имеет ровно два решения.

Теперь решим уравнение $a\cdot y^2+(a+1)\cdot y-2(a+1)=0$.

Нам необходимо найти значения параметра a, при которых данное уравнение имеет ровно два решения, лежащие в множестве $(0;+\infty)$. (Только при таких условиях исходное уравнение будет иметь четыре решения).

1) Если $a=0$, то данное уравнение имеет единственное решение $y=2$. В этом случае исходное уравнение имеет два решения.
2) Пусть теперь $a>0$. В этом случае искомое множество значений параметра a описывается системой условий

$$\begin{cases}(a+1)^2+8a(a+1)>0\\ a\cdot 0^2+(a+1)\cdot 0-2(a+1)>0\\ -\dfrac{a+1}{2a}>0\end{cases}.$$

(Здесь применяются факты о расположении корней квадратного трехчлена)

Продолжение решения задачи 5.

Решим эту систему при условии, что $a>0$.

$$\begin{cases}9a^2+10a+1>0\\ a<-1\\ -\dfrac{a+1}{2a}>0\end{cases}.$$

Второе неравенство в системе противоречит условию $a>0$.

3) Пусть теперь $a<0$. В этом случае искомое множество значений параметра a описывается системой условий

$$\begin{cases}(a+1)^2+8a(a+1)>0\\ a\cdot 0^2+(a+1)\cdot 0-2(a+1)<0\\ -\dfrac{a+1}{2a}>0\end{cases}.$$

(Здесь также применяются факты о расположении корней квадратного трехчлена)

Решим эту систему при условии, что $a<0$.

$$\begin{cases}9a^2+10a+1>0\\ a>-1\\ -a-1<2a\end{cases},\ \begin{cases}(9a+1)(a+1)>0\\ a>-1\\ a>-\dfrac{1}{3}\end{cases},\ \begin{cases}a>-\dfrac{1}{9}\\ a>-\dfrac{1}{3}\end{cases}$$

Ответ: $a\in\left(-\dfrac{1}{9};0\right)$.

XVIII Межрегиональная олимпиада школьников по математике и криптографии

11 класс

Вариант 2

1. Делится ли число $5^{2^{2^{2008}+3^{2009}+1991}}-1$ на 616?

2. На кодовом замке имеется круглый диск с риской. Вокруг диска нанесены числа от 0 до 99 по часовой стрелке. Для управления замком служат две кнопки: “вправо” и “влево”. При нажатии на кнопку “вправо” диск вращается на 33 деления по часовой стрелке, при нажатии на кнопку “влево” – на 20 делений против часовой стрелки. Каждая из этих операций выполняется за 1 секунду. Изначально замок установлен на число 0. Замок открывается при его установке на число 44 – ключ замка.

А. За какое наименьшее время можно открыть замок при данном ключе 44?

Б. Доказать, что замок можно открыть при любом ключе (ключ – число от 1 до 99).

В. За какое наименьшее время можно гарантированно открыть замок при любом ключе?

3. Осмысленная фраза на русском языке записана два раза подряд без пробелов и знаков препинания и зашифрована шифром Виженера. Зашифрование состоит в следующем. Выбирается *ключевое слово*, например, **мир**. Для изменения первой буквы шифруемого сообщения создается таблица следующего вида

Табл. 1

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
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

В нижней строке алфавит циклически сдвинут влево так, чтобы первая буква ключевого слова **м** оказалась под буквой **а**. Буква открытого текста (например, **п)** отыскивается в верхней строке и заменяется стоящей под ней буквой (для **п** – это **ь**). Для зашифрования второй буквы аналогичным образом используется буква **и,** третьей - **р**, четвертой - вновь **м** и т.д. Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

эущыёшоюнфкнрлжчерцкюммиёщсячшшдэйепдз

Восстановите исходное сообщение и ключевое слово.

4. В бесконечной последовательности цифр 7, 1, 2, 0, 3, 5 ... каждая цифра, начиная с четвертой, равна младшему разряду суммы трёх предыдущих цифр. Доказать, что в этой последовательности вновь встретятся подряд идущие цифры 7, 1, 2.

5. При каких значениях параметра a уравнение

$$4(4a-1)x^2+2(4a+1)(x^2+1)x+(a+1)(x^2+1)^2=0$$

имеет ровно четыре различных решения?

6. Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. Заглавные буквы заменяются на строчные. В получившейся цепочке буквы нумеруются слева направо $1,2,...,L$. Зашифрование происходит путем перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b. Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a\cdot n+b$ на L (с одним исключением: если $a\cdot n+b$ нацело делится на L, то остаток полагается равным L). Например, если длина цепочки $L=25$ и $a=9, b=11$, то третья буква исходной цепочки будет тринадцатой в зашифрованной цепочке (т.к. $9\cdot 3+11=38$, а число 38 дает остаток 13 при делении на 25). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

светитнезнакомаязвездасновамыоторваныотдома

была получена цепочка

таытоеонсоовзмевтрадазедвмаянтоаысзаимнонвк

При этих же значениях a, b проведено зашифрование еще некоторой цепочки из 38 букв. Получилось вот что:

видхьврлмаояооаоддсемдроиввоеозтообнзо

Найдите значения a и b и восстановите исходное сообщение.

XVIII 11 класс

РЕШЕНИЯ. ЗАПАД

Вариант 2

1. $616 = 7 \times 8 \times 11$. Делится, т.к. число $5^k - 1$ делится на 7 тогда и только тогда, когда k кратно 6, на 8 – тогда и только тогда, когда k кратно 2, на 11 – тогда и только тогда, когда k кратно 5; показатель степени, очевидно, четен. Далее, число $2^{2^{2008}} + 3^{2^{2009}} + 1991 = 2^{2^{2008}} - 1 + 3^{2^{2009}} + 1992$ делится на 3, поскольку $2^k - 1$ делится на 3 при четных k и 1992 делится на 3 по известному признаку делимости. Числа $3^{2^{2009}}$ и $2^{2^{2008}}$ в десятичной записи оканчиваются на 3 и 6 соответственно, поэтому $2^{2^{2008}} + 3^{2^{2009}} + 1991$ оканчивается на 0, т.е. делится на 5.

2. А. $r_{100}(33u - 20v)=44$. Перебор: 33, 66, 99, 132, 165, 198, 231, 264. Значит 8 вправо, 1 влево, итого *9 секунд*.

Б. Перебор: 0, 33, 66, 99, 132, 165, 198, 231, 264, 297, 330, 363, 396, 429, 462, 495, 528, 561, 594, 627, 660 – есть все остатки от деления на 20.

В. $r_{100}(33u - 20v)=k$, $0 \le u \le 19$, $0 \le v \le 4$. Итого 19+4=*23 секунды*.

(подробнее – см. вариант 1 для 11 класса)

3. Убеждаемся, что шифрованный текст имеет длину 38. Осмысленная фраза имеет тогда длину 19. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв

Если $x_1x_2x_3x_4x_5$-ключевое слово, то для при первом шифровании использовалось оно само а при втором $x_5x_1x_2x_3x_4$. Таким образом, найденные разности равны соответственно $x_5 - x_1, x_1 - x_2, x_2 - x_3, x_3 - x_4, x_4 - x_5$. Тогда при известной первой букве x_1 остальные вычисляются по формуле: $x_5 = x_1 + 14$, $x_4 = x_1 + 17$, $x_3 = x_1 + 2$, $x_2 = x_1 + 22$. Перебирая 33 варианта для буквы x_1 получаем 33 варианта ключевого слова, среди которых находится единственное осмысленное слово: КАМЫШ. При расшифровании получаем текст:
Т У М А Н Н О С Т Ь А Н Д Р О М Е Д Ы Т У М А Н Н О С Т Ь А Н Д Р О М Е Д Ы .

к	ю	м	м	и
э	у	щ	ы	ё
14	11	20	18	3

4. Последовательность состоит из цифр от 0 до 9. Так как число четверок (a,b,c,d) таких цифр конечно (и равно 10000), то в последовательности рано или поздно встретятся две повторяющиеся четверки. Пусть они встретились на i-м и j-м месте, $0 \le i < j$. Если i=0, то все доказано. Пусть i>0. (Сейчас доказано, что последовательность периодическая. Но нужно еще доказать, что она чисто периодическая.)
Закон рекурсии: $u_{i+4}=r_{10}(u_{i+3}+u_{i+2}+u_{i+1}+u_i)$ (*), где r_{10} – остаток от деления на 10. Заметим, что по заданным четырем членам последовательности можно однозначно восстановить предыдущий член. Другими словами, если u_{i+4}, u_{i+3}, u_{i+2}, u_{i+1} известны, то существует единственное u_i, для которого выполняется рекуррентное соотношение (*). Поэтому если в последовательности совпали четверки на местах i и j, то совпадут четверки и на местах i–1 и j–1. И т.д. Поэтому совпадут четверки на местах 0 и j–i. Ч.т.д.

6. Для начала найдём в открытом тексте две уникальные буквы (по возможности близкие). Это например К и Я, стоящие соответственно на 12 и 16 позициях в открытом тексте. В шифрованном тексте они стоят соответственно на 43 и на 28. Составляем систему уравнений

$$\begin{cases} 12a + b = 43k \\ 16a + b = 28 + 43l \end{cases}$$

Вычитая, получаем уравнение $4a = 28 + 43m$, при $m = 0$ находим $a = 7$, из первого уравнения находим $b = 2$.
Расшифровав второй текст, получим :
морозвоеводадозоромобходитвладеньясвои

РЕШЕНИЯ. ЗАПАД

Вариант 2

5. Поскольку x^2+1 не обращается в ноль, то можно разделить обе части уравнения на выражение $\left(x^2+1\right)^2$. Получим уравнение

$$(4a-1)\cdot\left(\frac{2x}{x^2+1}\right)^2+(4a+1)\cdot\frac{2x}{x^2+1}+(a+1)=0.$$

Сделаем замену переменных $y=\frac{2x}{x^2+1}$.. Во-первых, рассмотрев график функции $y=\frac{2x}{x^2+1}$ (или любым другим стандартным способом), можно сделать вывод, что

- минимальное значение величины $y=\frac{2x}{x^2+1}$ равно -1 (при $x=-1$), максимальное значение величины $y=\frac{2x}{x^2+1}$ равно 1 (при $x=1$),
- множество значений величины $y=\frac{2x}{x^2+1}$ имеет вид $[-1;1]$,
- для любого $c\in(-1;0)\cup(0;1)$ уравнение $\frac{2x}{x^2+1}=c$ имеет ровно два решения.
- Для $c\in\{-1;1;0\}$ уравнение $\frac{2x}{x^2+1}=c$ имеет единственное решение.

Теперь решим уравнение $(4a-1)\cdot y^2+(4a+1)\cdot y+(a+1)=0$.

Нам необходимо найти значения параметра a, при которых данное уравнение имеет ровно два решения, лежащие в множестве $(-1;0)\cup(0;1)$. (Только при таких условиях исходное уравнение будет иметь четыре решения).

1) Если $a=-1$, то данное уравнение имеет решения $y=-\frac{3}{5}$, $y=0$. В этом случае исходное уравнение имеет три решения. Кроме того, при $a\neq-1$ значение $y=0$ не является решением уравнения.
2) Если $a=\frac{1}{4}$, то данное уравнение имеет решение $y=-\frac{5}{8}$. В этом случае исходное уравнение имеет два решения.
3) Пусть теперь $a>\frac{1}{4}$. В этом случае искомое множество значений параметра a описывается системой условий

$$\begin{cases}(4a+1)^2-4(4a-1)(a+1)>0\\(4a-1)\cdot(-1)^2+(4a+1)\cdot(-1)+a+1>0\\(4a-1)\cdot1^2+(4a+1)\cdot1+a+1>0\\-1<-\frac{4a+1}{2(4a-1)}<1\end{cases}.$$

Продолжение решения задачи 5.

(Здесь применяются факты о расположении корней квадратного трехчлена).

Решим эту систему при условии, что $a>\frac{1}{4}$.

$$\begin{cases} 5-4a>0 \\ a-1>0 \\ 9a+1>0 \\ -2(4a-1)<-1-4a<2(4a-1) \end{cases},\begin{cases} a<\frac{5}{4} \\ a>1 \\ 4a>3 \\ 12a>1 \end{cases},\begin{cases} a<\frac{5}{4} \\ a>1 \end{cases}.$$

4) Пусть теперь $a<\frac{1}{4},\quad a\neq -1$. В этом случае искомое множество значений параметра a описывается системой условий

$$\begin{cases} (4a+1)^2-4(4a-1)(a+1)>0 \\ (4a-1)\cdot(-1)^2+(4a+1)\cdot(-1)+a+1<0 \\ (4a-1)\cdot 1^2+(4a+1)\cdot 1+a+1<0 \\ -1<-\frac{4a+1}{2(4a-1)}<1 \end{cases}.$$

(Здесь также применяются факты о расположении корней квадратного трехчлена).

Решим эту систему при условии, что $a<\frac{1}{4},\quad a\neq -1$.

$$\begin{cases} 5-4a>0 \\ a-1<0 \\ 9a+1<0 \\ -2(4a-1)>-1-4a>2(4a-1) \end{cases},\begin{cases} a<\frac{5}{4} \\ a<-\frac{1}{9} \\ 4a<3 \\ 12a<1 \end{cases},\begin{cases} a<-\frac{1}{9} \\ a\neq -1 \end{cases}.$$

Ответ: $a\in(-\infty;-1)\cup\left(-1;-\frac{1}{9}\right)\cup\left(1;\frac{5}{4}\right)$.