Разбор заданий школьного тура олимпиады по криптографии.

Занятие 5

В школьном туре олимпиады предлагалось 4 варианта заданий, при этом 1,2 и 3,4 соответственно варианты были однотипными.

Разберем задания из первого варианта, решение второго аналогично.

Вариант 1

1. Криптограмма

ЖЗЕЩЕ ЬАКУЖ ЭЗЭЫЕ ЩЕЗТЖ ЕФБЕД ЕГАПЭ ИБЕАИ
АКЛЧО ААЩЗЕ ИИААА ЭЩЗЕИ ЕХЯЭ

получена при использовании сдвигового шифра в русском алфавите:

Таблица 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	Ы	Ъ Ь	Э	Ю	Я
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

Для удобства восприятия шифртекст разбит на пятиграммы. Необходимо найти ключ расшифрования и прочитать сообщение.

Ответ: *проводить переговоры по экономической ситуации в России и Евросоюзе; k=22.*

Решение:

Попробуем установить какая из букв представленного шифртекста соответствует наиболее часто встречающейся в русском языке букве О (см. гистограмму частот, представленную ранее). Для этого подсчитаем частоты встречаемости букв в шифртексте (см. таблицу).

Е	А	Э	З	И	Щ	…
11	9	5	5	5	4	…

Предположим, что буква О переходит при зашифровании в букву Е, тогда ключ k = Е – О = 6-14 = -8 = 22 (берем остатки при делении на 30). Попробуем расшифровать данный шифртекст на таком ключе. Получим следующее начало открытого текста: ПРОВОДИТ… Как видим текст

получается читаемым, остается расшифровать оставшуюся часть шифртекста и убедиться, что $k = 22$ действительно ключ рассматриваемого шифра.

Отметим, что в тестовом задании вовсе нет необходимости полностью расшифровывать текст, поскольку в задании спрашивается 7-ая буква с конца открытого текста. Убедившись, что при расшифровании на ключе 22 получается осмысленное начало текста, можно расшифровать указанную букву и таким образом ответить на вопрос теста.

2. Сообщение

ТЯИБРЕЕСЬВВ

зашифровано с помощь шифра вертикальной перестановки на ключе

1 2 3 4 5 6
6 4 3 2 1 5

Прочитайте данный текст.

Ответ: ВЕРИТЬ В СЕБЯ.

Решение:

Известна длина ключа. В данном случае, число столбцов в ключевой таблице равна 6. Всего букв шифрованного текста 11. 11=6+5. Таким образом, приходим к выводу, что в таблице, в которую записывался изначально текст, находится две строки, последняя самая короткая, содержит 5 символов. В частности это означает, что в каждом из столбцов содержится по две буквы, за исключением последнего 6 столбца - в нем по одна буква.

В условии задачи дан ключ зашифрования, поэтому можно выписать ключ расшифрования, просто поменяв его строки местами:

1 2 3 4 5 6
5 4 3 2 6 1

Так как первый столбец согласно ключу расшифрования должен стать пятым, а он является «длинным» (то есть в нем 2 буквы), то его содержимое: ТЯ. Далее, второй столбец должен стать четвертым, а он является «длинным» (то есть в нем 2 буквы), то его содержимое: ИБ и т.д. Получим следующую разбивку на столбцы.

ТЯ ИБ РЕ ЕС Ь ВВ

5	4	3	2	6	1
Т	И	Р	Е	Ь	В
Я	Б	Е	С		В

Теперь переставим столбцы в соответствии с их номерами, получим:

1	2	3	4	5	6
В	Е	Р	И	Т	Ь
В	С	Е	Б	Я	

3. Число $N = 100712603$ является произведением двух простых чисел p и q, причем $|p - q| \leq 500$. Разложить это число на простые множители.

Ответ: 10259, 9817.

Решение:

Для решения воспользуемся методом Ферма.

Пусть $p = z - t$, а $q = z + t$. Тогда

$$N = p \cdot q = (z - t)(z + t) = z^2 - t^2,$$

$$z^2 = N + t^2,$$

$$z = \overline{N + t^2},$$

$$z > \overline{N}.$$

Причем отметим, в силу того, что p и q - близкие простые числа, $p - q \leq 500$, то значение z близко к значению $\overline{N}$, но немного его превосходит. Будем проводить подбор значения для этого числа. В данном случае, нетрудно подсчитать (на калькуляторе, или заметив, что 10 035< $\overline{N}$<10 036), что целая часть корня $\overline{N}$ - это 10 035. Тогда первое возможное значение для z - 10 036.

— Пусть $z = 10\,036$. Тогда $t^2 = z^2 - N = 100721296 - 100712603 = 8693$, но значение $\overline{8693}$ - число не целое.

— Пусть $z = 10\,037$. Тогда $t^2 = z^2 - N = 100741369 - 100712603 = 28766$, но значение $\overline{28766}$ - тоже не целое.

— Пусть $z = 10\,038$. Тогда $t^2 = z^2 - N = 100761444 - 100712603 = 48841$ и $t = \sqrt{48841} = 221$

Подставив полученные значения для z и t, получаем, что $p = 10\,038 - 221 = 9817$, $q = 10\,038 + 221 = 10259$.

4. Для зашифрования натурального числа m используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединенные друг с другом, называют *соседними*. Зашифрование состоит в выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна m.

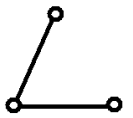

Рис. 1

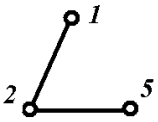

Рис. 2

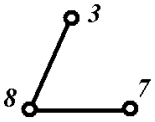

Рис. 3

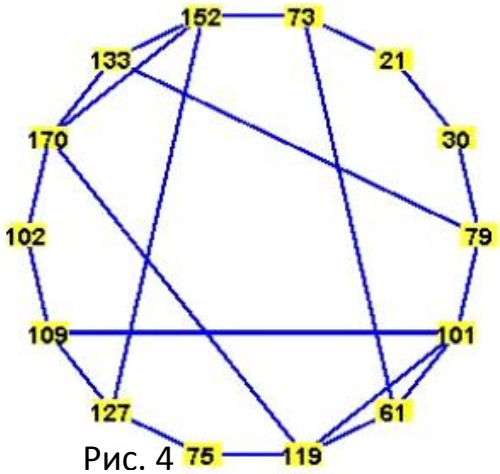

Рис. 4

Затем к числу в каждой вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число m. Пример: для зашифрования числа 8 будем использовать граф на рис. 1. В его вершины поместим числа, сумма которых равна 8 (рис. 2). Затем к каждому числу прибавим числа в соседних вершинах. Результат зашифрования указан на рис. 3. На рис. 4 приведен результат зашифрования некоторого числа. Найдите его.

Ответ: 329.

Решение:

Граф, используемый в задаче, обладает следующим свойством: из множества всех его вершин можно выделить такое подмножество V (отмеченное на рис. 5 кружочками), что любая вершина графа лежит в

окрестности ровно одной вершины из *V*. Окрестностью вершины графа называют множество соседних с ней вершин, включая её саму. Очевидно, что искомое число равно сумме чисел, расположенных в вершинах из множества *V*: 102+75+79+73 = 329.

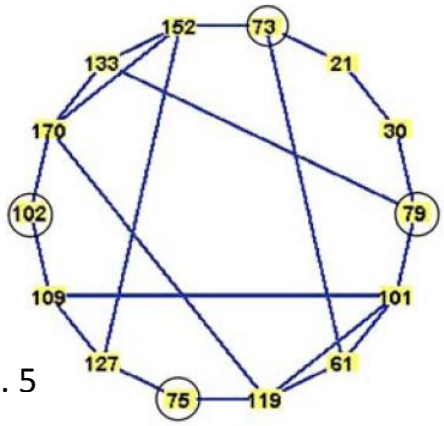

Рис. 5

Разберем задания из третьего варианта, решение четвертого аналогично.

Вариант 3

1. Имеется криптограмма

ЁПДЗМЁТХЦТО

Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x_1, x_2 - корни трехчлена $x^2 + 3x + 1$. К порядковому номеру каждой буквы в русском алфавите (33 буквы) прибавлялось значение многочлена

$$f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 5$$

вычисленное либо при $x = x_1$, либо при $x = x_2$ (в неизвестном порядке), а затем полученное число заменялось соответствующей ему буквой.

Ответ: ВЛАДИВОСТОК.

Решение:

Разделим $f(x)$ на $x^2 + 3x + 1$ с остатком:

$$f(x) = (x^4 + x + 1)(x^2 + 3x + 1) + 4.$$

Поэтому, и при $x = x_1$, и при $x = x_2$ значение $f(x) = 4$. Таким образом, данное преобразование осуществляет не что иное, как сдвиговый шифр с параметром k=4. Если теперь шифрованное сообщение представить в виде цифровом виде, получим

7 17 5 9 14 7 20 23 24 20 16

Отнимем от каждого значение 4, получим:

3 13 1 5 10 3 16 19 20 16 12,

приводим обратно к буквенному виду, получаем

ВЛАДИВОСТОК

2. Осмысленная фраза на русском языке записана **два раза подряд** без пробелов и знаков препинания и зашифрована шифром Виженера.

Сообщение было зашифровано с использованием ключевого слова из пяти букв. Результат зашифрования выглядит так:

ОРАЦЕ КЭЙШР ФМГОЙ БФДОЙ ТЮЁНР

ФУЬУН ЁФДОЙ ТЮЁЪУ ВЧЬУА ЙШЬУС УЪЫЪУ ИРБ

Восстановите исходное сообщение и ключевое слово, если известно, что 4-ой буквой ключевого слова является одна из четырех: И, М, П, Н.

Табл. 2

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
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	31	32	33

Ответ: *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; АКЦИЯ.*

Решение:

Убеждаемся, что шифрованный текст имеет длину 58. Осмысленное предложение имеет тогда длину 29. Выписываем друг под другом известные 5 первых знаков второй и первой половины шифрованного текста и находим разность позиций соответствующих букв, исходя из отождествления, указанного в таблице.

н	**ё**	**ф**	**д**	**о**
о	**р**	**а**	**ц**	**е**
32	22	21	14	20

Получаем: 32 22 21 14 20 ... . Если $\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$ - ключевое слово, то при первом шифровании использовалось оно само, а при втором - $\gamma_5, \gamma_1, \gamma_2, \gamma_3, \gamma_4$. Таким образом, найденные разности равны соответственно:

$$r_{33}(\gamma_5 - \gamma_1), r_{33}(\gamma_1 - \gamma_2),\ r_{33}(\gamma_2 - \gamma_3),\ r_{33}(\gamma_3 - \gamma_4), r_{33}(\gamma_4 - \gamma_5).$$

$$\begin{array}{l} \gamma_5 - \gamma_1 = 32; \\ \gamma_1 - \gamma_2 = 22; \\ \gamma_2 - \gamma_3 = 21; \\ \gamma_3 - \gamma_4 = 14; \\ \gamma_4 - \gamma_5 = 20. \end{array} \Longrightarrow \begin{array}{l} \gamma_1 = 24 + \gamma_4; \\ \gamma_2 = 2 + \gamma_4; \\ \gamma_3 = 14 + \gamma_4; \\ \gamma_5 = 23 + \gamma_4. \end{array}$$

Тогда при известной 4-ой букве гаммы γ_4 остальные вычисляются по формулам, указанным выше. Далее перебирая все 4 варианта для первой

буквы γ_4 (указанных в условии задачи), приходим к одному осмысленному слову АКЦИЯ.

Далее остается расшифровать текст на данном слове, получим:

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

3. Число $\mathrm{N} = 202879393$ является произведением двух простых чисел p и q, при этом известно, что количество чисел, меньших N с ним взаимнопростых равно 202849200. Разложить число N на простые множители.

Ответ: 10093, 20101.

Решение:

Пусть так же $\varphi(N)$ – количество натуральных чисел, меньших N и взаимнопростых с ним. Тогда $\varphi(N) = (p-1)(q-1)$. Получим следующую систему уравнений с двумя неизвестными.

$$\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}$$

Раскроем скобки во втором уравнении и подставим в него первое уравнение. Получим следующую равносильную систему.

$$\begin{cases} pq = N \\ p+q = N+1-\varphi(N) \end{cases}.$$

В силу теоремы обратной теореме Виета, числа p и q являются решением квадратного уравнения.

$$x^2 - (N+1-\varphi(N))x + N = 0$$

$$x^2 - 30194x + 202879393 = 0$$

Решим его, для этого посчитаем дискриминант.

$$D = 911677636 - 811517572 = 100160064 = 10008^2$$

Итак:

$$x_1 = \frac{30194 + 10008}{2} = 20\,101$$

$$x_2 = \frac{30194 - 10008}{2} = 10\,093$$

4. Для открытия подземелья в волшебной стране надо правильно назвать три целых числа a,b,c, служащих коэффициентами квадратичной функции $f(x)=ax^2+bx+c$. Представителям четырёх рас были переданы следующие значения функции: троллям – значение $f(17)$, эльфам – $f(20)$, гномам – $f(21)$, оркам – $f(24)$. Когда представители рас встретились, чтобы совместно найти a,b,c и открыть подземелье, один из представителей, чтобы сорвать мероприятие, предъявил неверное значение. Выясните, кто это был, если известно, что тролли предъявили число 99, эльфы – 212, гномы – 251, орки – 386.

Ответ: *эльфы сообщили неверное значение*.

Решение:

Докажем тот факт, что разность значений квадратичной функции должна делиться на разность значений аргументов.

Пусть $u \neq v$ и $f(x) = ax^2 + bx + c$. Рассмотрим разность:

$$f(u) - f(v) = au^2 + bu + c - (av^2 + bv + c) = a(u^2 - v^2) + b(u - v)$$
$$= (u - v)(a(u + v) + b).$$

Из данного равенства видно, что $f(u) - f(v)$ делится на $u - v$.

Проверим выполнение этого факта для различных пар значений:

- для первого и второго: 212-99=113 не делится на 20-17= 3, следовательно, значение исказили либо эльфы, либо тролли;
- для третьего и четвертого: 386-251=135 делится на 24-21=3;
- для первого и третьего: 251–99=152 делится на 21-17=4;
- для второго и четвертого: 386–212=174 не делится на 24-20= 4, следовательно, значение исказили либо эльфы, либо орки.

Таким образом, исказить значение могли только эльфы.