XXIX
Межрегиональная олимпиада школьников им. И. Я. Верченко по математике и криптографии

Москва 2020

Всего пронумеровано 32 стр.
Подписано к печати __.01.20
Авт. л. 1,17 Усл. печ. л. 1,75
Заказ № _____.
Тираж 400 экз.

www.cryptolymp.ru

Приветствие главного учёного секретаря Академии криптографии Российской Федерации Владимира Николаевича Сачкова участникам XXIX Межрегиональной олимпиады школьников имени И.Я. Верченко по математике и криптографии

Дорогие друзья!

Приветствую участников XXIX Межрегиональной олимпиады школьников имени И.Я. Верченко по математике и криптографии!

Математика на протяжении всей истории человечества привлекает к себе лучшие умы и в значительной степени влияет на развитие наук о природе и технических наук. Криптография, возникшая в глубокой древности вместе с письменностью как искусство защиты сообщений от непосвящённых, прошла большой путь развития и сегодня представляет собой обширную научно-техническую область, которая опирается на достижения математики, физики, информатики, теории связи и многих других наук.

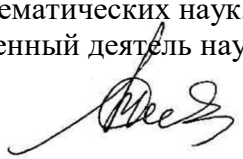
Отечественная криптография развивается вместе с нашей страной и является существенной частью системы обеспечения национальной безопасности, защиты информационных ресурсов каждого гражданина, общества и государства. В 2019 году мы отметили 70-летие важных государственных решений, их выполнение обеспечило настоящую научно-техническую революцию в

отечественной криптографии, по-прежнему обеспечивающей в этой области стратегический паритет с другими державами. В 1949 году были заложены основы и современной системы подготовки специалистов по криптографии, образованы закрытое отделение механико-математического факультета Московского государственного университета им. М.В. Ломоносова и Высшая школа криптографов – родоначальники Института криптографии, связи и информатики.

Для решения актуальных задач современной криптографии нужны в первую очередь специалисты с высоким уровнем математического образования. Олимпиады школьников играют важную роль в поиске и привлечении талантливых молодых людей, которые смогут проявить свои лучшие качества в трудном, но удивительно красивом мире математики и криптографии.

Вам, юным участникам и будущим победителям и призёрам Межрегиональной олимпиады, принадлежит будущее. Желаю всем участникам олимпиады удачи и творческих успехов!

Главный учёный секретарь Академии криптографии Российской Федерации,
доктор физико-математических наук,
профессор, заслуженный деятель науки РФ



В.Н. Сачков

Информация о проведении олимпиады

XXIX Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии проводилась в два тура.

Первый тур проводился в дистанционной форме на интернет-сайте **www.cryptolymp.ru**.

Второй тур проводился в очной форме на базе Академии ФСБ России и во многих городах и вузах России: Архангельск – САФУ, Астрахань – АГУ, Астрахань – АГТУ, Барнаул – АлтГТУ, Белгород – БГТУ им. В.Г. Шухова, Владивосток – ДВФУ, Владимир – ВлГУ, Волгоград – ВолГУ, Ижевск – УдГУ, Иркутск – ИГУ, Йошкар-Ола – ПГТУ, Казань – КНИТУ-КАИ, Калининград – БФУ им. И. Канта, Кострома – КГУ, Краснодар – КубГТУ, Красноярск – СибГУ им. М.Ф. Решетнева, Курск – ЮЗГУ, Липецк – ЛГПУ имени П.П. Семенова-Тян-Шанского, Москва – Академия ФСБ России, Нефтекамск – НФБашГУ, Нижний Новгород – ННГУ им. Н.И. Лобачевского, Новосибирск – НГУЭУ, НГТУ, Озерск – ОТИ НИЯУ МИФИ, Омск – ОмГУ, Оренбург – ОГУ, Пермь – ПНИПУ, Пятигорск – ПГУ, Ростов-на-Дону – ДГТУ, Самара – Самарский университет, Санкт-Петербург – СПб НИУ ИТМО, СПбПУ, Саратов – СГТУ им. Гагарина Ю.А., Севастополь – СевГУ, Ставрополь – СКФУ, Сыктывкар – СГУ имени Питирима Сорокина, Таганрог – ЮФУ, Тамбов – ТГТУ, Томск – ТУСУР, Тюмень – ТюмГУ, Хабаровск – ДВГУПС, Челябинск – ЧелГУ, Череповец – ЧГУ, Ярославль – ЯрГУ.

Межрегиональная олимпиада школьников им. И. Я. Верченко по математике и криптографии включена в Перечень олимпиад школьников на 2019/2020 учебный год (2 уровень), что дает право предоставлять

льготы победителям и призерам при поступлении в государственные и муниципальные учреждения высшего образования (Приказ Минобрнауки России от 04.04.2014 № 267). Решения о льготах принимаются вузами самостоятельно и должны быть объявлены к 1 июня 2020 года.

УСЛОВИЯ И РЕШЕНИЯ ЗАДАЧ

Задача 1 (8-9, 10 классы)

На билетах в кинотеатры Криптоландии проставляется шестизначный номер от (0,0,0,0,0,0) до (8,8,8,8,8,8). При этом используются только цифры 0,1,2,3,4,5,6,7,8. Билет считается «счастливым», если остатки от деления на 9 суммы первых трех цифр и суммы последних трех цифр отличаются на фиксированное число $k = 2$. Например, билеты с номерами 123026 и 123661 – счастливые, а с номерами 123000 и 876111 – нет. Найдите число счастливых билетов.

Решение

Количество трёхзначных чисел $x_1x_2x_3$, у которых остаток от деления на 9 суммы цифр равен фиксированному значению $t \in \{0,1,\dots,8\}$, равно $9^2 = 81$, поскольку любые две цифры однозначно определяют третью из соотношения $r_9(x_1 + x_2 + x_3) = t$. Приведём возможные варианты для значений остатков для первой и последней тройки цифр:

$$(0,2), (1,3), \dots, (6,8),$$
$$(2,0), (3,1), \dots, (8,6)$$

их число равно $2 \times 7 = 14$, и тогда общее число счастливых билетов равно $2 \times 7 \times 9^2 \times 9^2 = 2 \times 7 \times 9^4 = 91854$.

Ответ: 91854.

Комментарий

При передаче информации по каналам связи важными аспектами являются обеспечение ее *конфиденциальности* и *целостности*. Конфиденциальность (т.е. секретность) достигается криптографическими методами, путем шифрования информации. Целостность информации означает отсутствие изменений в передаваемой/хранимой информации по сравнению с ее первоначальной записью. Говоря о целостности сообщения, по-другому говорят о его *аутентичности*.

Существует множество методов проверки целостности передаваемого сообщения. В частности, для этого широко используется теория кодирования информации. С точки зрения этой теории множество всех наборов цифр (x_1, x_2, x_3), для которых выполнено соотношение $r_m(x_1 + x_2 + x_3) = t$, является кодом с расстоянием два по Хэммингу. Этот код способен обнаруживать одну ошибку, которая может произойти при передаче набора (x_1, x_2, x_3) по каналу связи. Например, если ошибка произошла в первом символе, и было принято сообщение (x'_1, x_2, x_3), в котором $x'_1 \neq x_1$, то $r_m(x'_1 + x_2 + x_3) \neq t$ и этот факт будет обнаружен. Задача нацелена на нахождение мощности такого кода, т.е. числа всех комбинаций цифр (x_1, x_2, x_3), удовлетворяющих условию $r_m(x_1 + x_2 + x_3) = t$. Эта мощность равна m^2, поскольку при задании любых двух цифр в комбинации третья цифра определяется однозначно.

Задача 2 (8-11 классы)

Известно, что p, p_1, p_2, p_3 – различные простые числа, и $p^3 - 2p^2 - 16p = p_1 \cdot p_2 \cdot p_3 - 32$. Найдите все такие числа p, p_1, p_2, p_3. Ответ обоснуйте.

Решение

Пусть $p_1 < p_2 < p_3$. По условию $p^3 - 2p^2 - 16p + 32 = p_1 \cdot p_2 \cdot p_3$. Разложим левую часть на множители:

$$(p-2)(p-4)(p+4) = p_1 \cdot p_2 \cdot p_3. \qquad (1)$$

Непосредственной проверкой убеждаемся, что $p \neq 2,3,5$. Значит $p > 5$. Следовательно, числа в левой части (1) различны и отличны от 1. Поэтому $p - 4 = p_1$, $p - 2 = p_2$, $p + 4 = p_3$. Поскольку p на 3 не делится, возможны случаи:

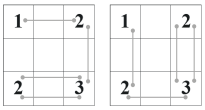
- число p при делении на 3 дает остаток 1. Тогда на 3 делится число $p - 4$. Такое возможно только, когда $p - 4 = 3$, так как число $p - 4$ простое. Отсюда $p = 7, p_1 = 3, p_2 = 5, p_3 = 11$.
- число p при делении на 3 дает остаток 2. Тогда на 3 делится $p + 4$. Значит $p + 4 = 3$, что невозможно.

Ответ: $p = 7, p_1 = 3, p_2 = 5, p_3 = 11$ (при условии $p_1 < p_2 < p_3$).

Задача 3 (8-9, 10 классы)

Сообщение передается в виде таблицы 7×7 клеток. В каждой клетке записана либо буква, либо цифра. Чтобы прочитать сообщение, необходимо зачеркнуть отрезками лишние символы. Отрезки проводят по следующим правилам (см. примеры): 1) концы отрезков лежат только в клетках с цифрами, причем цифра показывает сколько

концов в этой клетке лежит, 2) отрезки могут проходить только горизонтально или вертикально, 3) две цифры могут быть соединены не более, чем двумя отрезками. Прочитайте сообщение, которое получается выписыванием каждой третьей незачеркнутой буквы.



3	с	з	**4**	е	м	**3**
ю	с	е	р	д	е	у
ш	в	в	н	**2**	ь	**5**
о	г	д	р	б	о	ф
а	а	о	к	д	х	л
я	ж	н	т	ц	и	у
1	я	к	**2**	т	е	**2**

Решение

3	=	=	**4**	—	—	**3**
|	**с**	е	|	д	**е**	‖
|	в	в	|	**2**	=	**5**
|	**г**	д	|	б	**о**	|
|	а	о	|	**д**	х	|
|	ж	**н**	|	ц	и	|
1	**я**	к	**2**	—	—	**2**

Для решения задачи следует для каждого числа рассматривать количество соседей – чисел, с которыми оно может соединяться отрезками.

Если число равно удвоенному количеству своих соседей, то с каждым из них оно соединяется как минимум одним отрезком.

Начинать можно с рассмотрения угловых клеток таблицы, это позволяет провести первые отрезки. Затем возможно рассмотреть клетки по краям таблицы. По мере проведения отрезков между числами, начинает уменьшаться количество возможных вариантов построения новых отрезков. Если к числу приходит необходимое

количество отрезков, значит, оно уже не может соединяться с другими своими соседями.

В условии написано, что сообщение составляет каждая третья буква, но не указано, с какой буквы следует начинать чтение. Выписывая три возможных варианта, получаем, что читаемый текст будет лишь в случае чтения каждой третьей незачёркнутой буквы, начиная с первой.

Ответ: сегодня.

Задача 4 (8-9, 10 классы)

Для зашифрования сообщении каждая его буква заменяется числом по таблице. В результате получается числовая последовательность $x_1, \dots, x_n$. Затем вырабатывают последовательность $\gamma_1, \gamma_2, \dots$ по следующему правилу: γ_1 – некоторое натуральное число, γ_2 – сумма цифр квадрата γ_1, увеличенная на 1, и т.д. Например, если $\gamma_1 = 7$, то $\gamma_2 = 14$, $\gamma_3 = 17$ и т.д. После этого выбирается некоторое натуральное t и формируется зашифрованное сообщение по правилу: $r_{32}(x_1 + \gamma_t), \dots, r_{32}(x_n + \gamma_{t+n-1})$, где $r_{32}(a)$ – остаток от деления числа a на 32. Известно, что для $\gamma_1 = 2019$ и некоторого t получился следующий шифртекст: 10, 6, 26, 22, 15, 13, 20, 13, 29, 13, 28, 23, 4. Восстановите исходное сообщение.

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
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	31

Решение:

Будем перебирать возможные значения t, а затем, «раскрутив» последовательность $\gamma_t, \dots, \gamma_{t+n-1}$, попробуем расшифровать на ней текст. Занесем в таблицу

последовательность $\gamma_1, \gamma_2, \ldots$ и соответствующий открытый текст (ОТ), который получается если расшифровать шифртекст с помощью последовательности $\gamma_t, \ldots, \gamma_{t+n-1}$.

t	γ_i	ОТ		ОТ		ОТ		ОТ		ОТ	
1	2019	7	З								
2	28	10	К	14	О						
3	20	6	Ж	18	Т	22	Ц				
4	5	17	С	21	Х	1	Б	5	Е		
5	8	7	З	14	О	18	Т	30	Ю	2	В
6	11	2	В	4	Д	11	Л	15	П	27	Ы
7	5	15	П	8	И	10	К	17	С	21	Х
8	8	5	Е	12	М	5	Е	7	З	14	О
9	11	18	Т	2	В	9	Й	2	В	4	Д
10	5	8	И	24	Ш	8	И	15	П	8	И
11	8	20	Ф	5	Е	21	Х	5	Е	12	М
12	11	12	М	17	С	2	В	18	Т	2	В
13	5	31	Я	18	Т	23	Ч	8	И	24	Ш
14	8			28	Ь	15	П	20	Ф	5	Е
15	11					25	Щ	12	М	17	С
16	5							31	Я	18	Т
17	8									28	Ь

Нетрудно из таблицы заметить, что последовательность $\{\gamma_i\}$ периодическая с периодом (5, 8, 11) и подходом (2019, 28, 20), поэтому для расшифрования сообщения достаточно начинать расшифровывать при $t = 1, \ldots, 6$. . Осмысленный текст получается при $t = 5$.

Ответ: выходим в шесть.

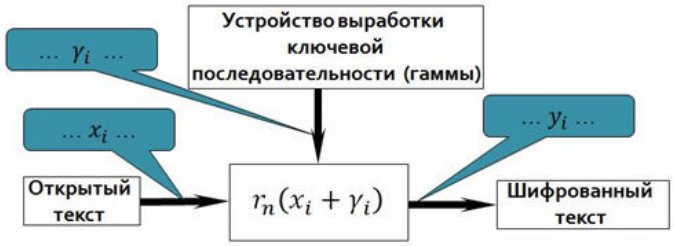
Комментарий

Здесь в качестве способа преобразования открытого сообщения использовался *шифр модульного гаммирования,* устроенный следующим образом. Пусть открытое сообщение $x_1, \dots, x_t$ состоит из символов алфавита $X = \{0, \dots, n-1\}$. Выберем некоторую последовательность (*гамму*) $\gamma_1, \dots, \gamma_t \in X$ и вычислим

$$y_i = r_n(x_i + \gamma_i), i = 1, \dots, t.$$

Сформированная последовательность $y_1, \dots, y_t$ и будет шифртекстом.

Общий принцип работы шифра гаммирования пояснен на рис. ниже:



Стойкость такого шифра существенным образом определяется выбором последовательности $\gamma_1, \dots, \gamma_t$. Эта последовательность должна быть, как говорят, *случайной* и *равновероятной*. Для ее выработки используют так называемые *генераторы псевдослучайных последовательностей* (ГПСЧ). В настоящей задаче гамма не являлась случайной и равновероятной, и, в частности, по этой причине удалось восстановить по шифрованному тексту исходное сообщение.

Задача 5 (8-11 классы)

Для зашифрования осмысленного слова его буквы переводят в числа $x_1, x_2, \dots, x_n$ по таблице. Затем выбирают натуральные числа x_0 и k. Далее число x_0 приписывают в начало последовательности $x_1, x_2, \dots, x_n$, а число $x_{n+1} = x_0 + 19^{n+4}$ (где n – длина слова) – в ее конец. Получившаяся в результате последовательность $x_0, x_1, \dots, x_n, x_{n+1}$ затем преобразуется в последовательность $y_0, y_1, \dots, y_n, y_{n+1}$ по формуле $y_i = r_{32}(x_i + 6x_i \cdot k^3 + k)$, $i = 0,1, \dots, n+1$, где $r_{32}(a)$ – остаток от деления числа a на 32. Затем числа $y_0, y_1, \dots, y_{n+1}$ заменяют буквами согласно таблице. В результате получили вот что: **КЙЫЦНБНЦЛ**. Какое слово было зашифровано?

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
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	31

Решение

Нетрудно понять, что длина слова $n = 7$, а также несложно найти остаток $r_{32}(19^{11}) = 11$.

Преобразуем зашифрованный текст в последовательность чисел:

$$y_0 = 10, y_1 = 9, y_2 = 27, y_3 = 22, y_4 = 13, y_5 = 1,$$
$$y_6 = 13, y_7 = 22, y_8 = 11.$$

Из условия следует, что $x_8 - x_0 = 11$. Рассмотрим разность

$$r_{32}(y_8 - y_0) = r_{32}(x_8 + 6x_8 \cdot k^3 + k - x_0 - 6x_0 \cdot k^3 - k) =$$
$$= r_{32}\big((1 + 6k^3) \cdot (x_8 - x_0)\big) = r_{32}\big(11 \cdot (1 + 6k^3)\big).$$

Имеем:

$$r_{32}\big(11 \cdot (1 + 6k^3)\big) = 1.$$

Заметим, что $r_{32}(3 \cdot 11) = 1$. Откуда находим $r_{32}(1 + 6k^3) = 3$. Значит,

$$1 + 6k^3 = 3 + 32t \Leftrightarrow 3k^3 = 1 + 16t \Leftrightarrow$$
$$\Leftrightarrow 33k^3 = 11 + 11 \cdot 16t$$

Значит, $r_{16}(33k^3) = r_{16}(k^3) = 11$. В итоге

$$k^3 = 11 + 16p.$$

При $p = 1$ получим $k^3 = 27$. Отсюда $k = 3$. Опробуем полученное значение. Согласно правилу зашифрования

$$y_1 = 9 = r_{32}(x_1 + 6x_1 \cdot 27 + 3) = r_{32}(x_1 \cdot 3 + 3),$$
$$\Leftrightarrow 3x_1 + 3 = 9 + 32t \Leftrightarrow 3x_1 = 6 + 32t$$

Т.е. $r_{32}(3x_1) = 6 \Longrightarrow r_{32}(x_1) = 2$. Продолжая дальше получим:

$$y_2 = 27 = r_{32}(x_2 + 6x_2 \cdot 27 + 3) = r_{32}(x_2 \cdot 3 + 3),$$
$$\Leftrightarrow 3x_2 + 3 = 27 + 32t \Leftrightarrow 3x_2 = 24 + 32t$$

Т.е. $r_{32}(3x_2) = 24 \Longrightarrow r_{32}(x_2) = 8$. В итоге получим

Ответ: ВИСОКОС.

Комментарий

Если каждому элементу множества X поставлен в соответствие ровно один элемент множества Y так, что при этом любой элемент множества Y окажется сопоставлен ровно одному элементу множества X, то говорят, что между данными множествами установлено *взаимно-однозначное, или биективное, соответствие (отображение)*. Биективное отображение множества X в себя называется *подстановкой элементов множества X*.

Идея предложенной задачи заключается в следующем наблюдении. Если целые числа a, b – нечетные, c – четное, $m, k, l \in \mathbb{N}, m > 1$, то функция

$$f(x, y) = r_{2^m}(a \cdot x + c \cdot x^k \cdot y^l + b \cdot y)$$

будет задавать подстановку по каждой переменной на множестве $\{0,1,\dots,2^m-1\}$ – остатков от деления на 2^m. Сказанное означает, что для любого фиксированного $x \in \{0,1,\dots,2^m-1\}$ функция $g(y)=f(x,y)$ задает подстановку элементов множества $\{0,1,\dots,2^m-1\}$. Аналогичное справедливо при любом фиксированном $y \in \{0,1,\dots,2^m-1\}$.

Данный факт имеет наглядную интерпретацию. Если записать таблицу значений указанной функции $f(x,y)$,

$x\backslash y$	0	1	…	j	…	2^m-1
0	$f(0,0)$	$f(0,1)$	…	$f(0,j)$	…	$f(0,2^m-1)$
1	$f(1,0)$	$f(1,1)$	…	$f(1,j)$	…	$f(1,2^m-1)$
…	…	…	…	…	…	…
i	$f(i,0)$	$f(i,1)$	…	$f(i,j)$	…	$f(i,2^m-1)$
…			…		…	
2^m-1	…	…	…	…	…	…

то можно заметить, что в каждой ее строке (и в каждом ее столбце) присутствуют все элементы $\{0,1,\dots,2^m-1\}$ при этом в точности по одному разу. Таблицы, обладающие указанным свойством, называются в математике *латинскими квадратами (латинскими прямоугольниками)*. Впервые латинские квадраты (4-го порядка) были опубликованы в книге «Шамс аль Маариф» («Книга о Солнце Гнозиса»), написанной Ахмадом аль-Буни в Египте приблизительно в 1200 г. Свое название латинские квадраты получили благодаря математику Леонарду Эйлеру, который вместо чисел в подобные таблицы записывал буквы латинского алфавита.

Латинские квадраты находят свое применение в криптографии. В частности предложенный в задаче способ зашифрования сообщения основан на использовании как раз латинского квадрата. Данный способ называют *табличным гаммированием.*

Задача 6 (8-11 классы)

Каждому из четырех абонентов A_1, A_2, A_3, A_4 надо выдать по два уравнения вида $aw + bx + cy + +dz = t$, где $a, b, c, d, t, w, x, y, z \in \{0,1\}$. Значения секретных битов w, x, y, z одинаковы для всех абонентов и им заранее неизвестны. Приведите хотя бы один пример уравнений, которые надо выдать этим четырем абонентам, чтобы каждая пара $\{A_1, A_3\}, \{A_1, A_4\}, \{A_2, A_3\}$ могла достоверно вычислить w, x, y, z, но чтобы при этом: 1) ни одна другая пара абонентов не могла бы достоверно вычислить более одного секретного бита; 2) ни один абонент в одиночку не был в состоянии достоверно вычислить даже один секретный бит. Например, если абонент A_1 получит уравнения $\{w + x + y + z = 1;\ w + x + 0 \cdot y + 0 \cdot z = 1\}$, а A_2 – $\{w + 0 \cdot x + y + 0 \cdot z = 0;\ w + x + 0 \cdot y + +z = 0\}$. Тогда, объединившись, из имеющихся в их распоряжении четырех уравнений они однозначно найдут, что $w = 1, x = 0, y = 1, z = 1$. При этом будем говорить, что пара абонентов $\{A_1, A_2\}$ может *достоверно вычислить* секретные биты w, x, y, z. Здесь традиционно полагается, что 1+1=0.

Решение

Пусть w_0, x_0, y_0, z_0 – значения секретных битов w, x, y, z. Решим прежде задачу, предполагая, что все

секретные биты равны нулю: $w_0 = x_0 = y_0 = z_0 = 0$. Затем в уравнениях можно будет сделать замену $w \to w + w_0, \dots, z \to z + z_0$ и тем самым получить решение задачи в общем случае.

Запишем теперь какую-нибудь систему из четырех уравнений, которой удовлетворяют *только* нулевые значения. Например,

$$w + x = 0 \quad (1) \qquad y + z = 0 \quad (3)$$
$$x + y = 0 \quad (2) \qquad w + x + y = 0 \quad (4)$$

Запишем еще одно уравнение, сложив эти четыре:

$$x + y + z = 0 \quad (5)$$

Система из *любых* четырех уравнений из набора (1) – (5) имеет только нулевое решение.

Далее идея в следующем. Если пара абонентов должна уметь находить все биты, то этой паре выдадим четыре *различные* уравнения из набора (1) – (5), если же нет, то хоть одно уравнение у этой пары должно быть общим.

Замечание. *Здесь нет четких алгоритмов и успех заранее не гарантирован. Возможно, следовало выбрать какие-то другие уравнения (1) – (4). Заметим, например, что абонентам, которые не должны уметь находить секрет, нельзя выдать уравнения (1), (2) и (4), так как значение бита* z *они не найдут, но определят, что* $w = x = y = 0$, *а это по условию недопустимо. Никакому абоненту нельзя выдать уравнения (2) и (5), так как из них следует, что* $z = 0$.

Абонентам раздать уравнения можно так: A_1: (1), (2); A_2: (1), (5); A_3: (3), (4); A_4: (4), (5).

Выполнив замену, запишем ответ в общем случае.

Ответ: Например,

$$A_1: w + x = w_0 + x_0,\ x + y = x_0 + y_0;\ A_2:\ w + x = w_0 + x_0,\ x + y + z = x_0 + y_0 + z_0;$$
$$A_3: y + z = y_0 + z_0,\ w + x + y = w_0 + x_0 + y_0;$$
$$A_4: w + x + y = w_0 + x_0 + y_0,\ x + y + z = x_0 + y_0 + z_0.$$

Комментарий

В данной задаче описывается более общий случай разделения секрета по сравнению с пороговой схемой Шамира, при которой доступ к секрету получают определенные группы абонентов, которых называют *уполномоченными*. Здесь в точности задаются конкретные абоненты, которые могут получить секрет (вообще говоря соответствующие группы могут различаться по числу участников). Такие схемы разделения секрета называют *структурами доступа*.

Существует общий незамысловатый алгоритм построения структуры доступа для разделения одного бита секрета между заданными группами абонентов с помощью дополнительных битов *забеливания*, которые складываются с секретным битом, при этом для каждой группы используются разные забеливающие биты. Однако этот подход не позволяет получать эффективные структуры доступа. Под понятием *информационная эффективность* структуры доступа понимается отношение числа распределенных секретных битов в структуре доступа к длине самой длинной доли (числу выданных бит абоненту).

Можно доказать, что эффективность не превосходит 1. Задача построения таких структур доступа до сих пор в общем случае не решена.

Сама постановка в предложенной для решения задаче несколько усложняется: необходимо распределить 3 секретных бита (для 8-10 классов) или 4 секретных бита (для 11 класса) между 4-мя абонентами и выдать при этом каждому абоненту не более 2-ух бит. То есть эффективность такой структуры доступа будет больше 1 ($3/2$ в задаче для 8-10 классов и $4/2$ в задачах для 11 класса)! Здесь нет обмана – просто в предложенной задаче разрешено не уполномоченным группам абонентов получать суммы секретных бит, а в задаче для 11 класса – еще и один секретный бит при условии, что остальные 3 бита по-прежнему должны для них оставаться в секрете.

Задача 7 (11 класс)

Саша решил отправить Маше записку. Для этого каждую букву сообщения он заменил комбинацией из 0 и 1 согласно таблице (А – 00000, Б – 00001, …, Я – 11111). Взяв день "Д" и номер месяца "М" своего рождения Саша вычислил $u_1 = Д^2 + М^2, u_2 = Д \cdot М, u_3 = Д - М$. Далее Саша вычислил четвертое $u_4 = r_{32}(u_1 + u_2 u_3)$, пятое $u_5 = r_{32}(u_2 + u_3 u_4)$, …, n-ое число $u_n = r_{32}(u_{n-3} + +u_{n-2}u_{n-1})$, где $r_{32}(a)$ – остаток от деления числа a на 32. К i-му биту символу исходного сообщения (0 или 1) он прибавил число u_i и взял остаток от деления на 2. Полученную последовательность из 0 и 1 он вновь преобразовал в буквы по таблице и получил следующее

сообщение: **ЖДУЛЩБШЛТВШЩЧ**. Помогите Маше прочитать его.

А	Б	В	Г	Д	Е	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
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Решение

По условию числа u_k прибавляются к битам открытого текста, а результат заменяется остатком от деления на 2 (то есть на 0 или 1). Поэтому сразу заменим u_k его остатком от деления на 2: считаем, что $u_k = 0$ (если изначально u_k было четным) или $u_k = 1$ (если оно было нечетным). Вычисление остатка от деления на 32 при построении последовательности $u_1, u_2, \ldots$ никакой роли не играет (четные числа дают четный остаток, а нечетные – нечетный).

Оказывается, в зависимости от четности чисел Д, М могут быть получены всего три различные последовательности $u_1, u_2, \ldots$, а именно:

1. Числа Д, М нечетные. Тогда $u_1 = 0, u_2 = 1, u_3 = 0, \ldots$
2. Числа Д, М имеют разную четность. Тогда $u_1 = 1, u_2 = 0, u_3 = 1, \ldots$
3. Числа Д, М четные. Тогда $u_1 = u_2 = \cdots = u_{32} = 0$. В этом случае текст Машиной записки остался бы без изменения, что, очевидно, не так.

Далее необходимо в первых двух случаях вычислить последовательность $\{u_n\}$ полностью, вычесть ее из

зашифрованного текста (**ЗТ**) и убедиться, что читаемый вариант получается во втором случае (см. таблицу).

	Ж	Д	У	Л	Щ	Б	Ш	Л	У	В	Ш	Ц	Ч
	00110	00100	10011	01011	11001	00001	11000	01011	10011	00010	11000	10110	10111
Д, М **нечетные**													
u_n	01001	00100	10010	01001	00100	10010	01001	00100	10000	01001	00100	10010	01001
ЗТ -u_n	01111	00000	00001	00010	11101	10011	10001	01111	00011	01011	11100	00100	11110
	П	А	Б	В	Э	У	С	П	Г	Л	Ь	Д	Ю
Д, М **разной четности**													
u_n	10111	01110	11101	11011	10111	01110	11101	11011	10110	01110	11101	11011	10111
ЗТ -u_n	10001	01010	01110	10000	01110	01111	00101	10000	00101	01100	00101	01101	00000
	С	К	О	Р	О	П	Е	Р	Е	М	Е	Н	А

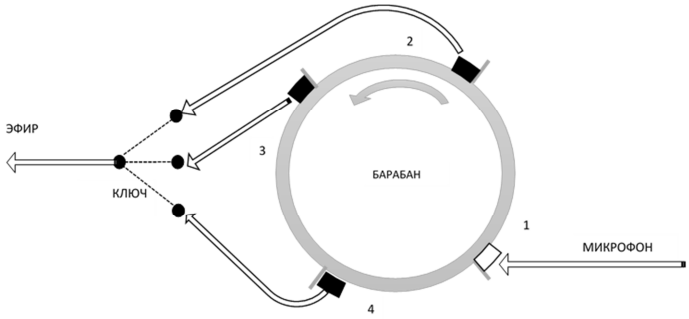
Ответ: **СКОРОПЕРЕМЕНА**

Комментарий

Представленная задача также относится к шифрам гаммирования, представленным ранее в задаче 4.

Задача 8 (11 класс)

Звук записывается на магнитный слой барабана (см. рис.), который вращается с постоянной скоростью, совершая один оборот за 4 секунды. Рядом с барабаном по окружности через равные расстояния размещены записывающая (1) и три читающие головки (2), (3), (4). В каждый момент времени в телефонную линию передается сигнал с одной из читающих головок. Устройство спроектировано так, что каждый участок сигнала будет передан в линию один раз, а сама передача стартует, как



только начало записи окажется у 3-й читающей головки.Сколько различных вариантов звука, переданного в линию, может получиться, если сообщение длилось 20 секунд?

Решение

Решим задачу в общем случае, когда передача длилась n секунд. Так как переключение между читающими головками происходит раз в секунду, весь звук можно разбить на n фрагментов по 1 секунде и тогда звук, переданный в линию, будет перестановкой этих фрагментов. Обозначис количество возможных перестановок $T(n)$.

Представим весь процесс в виде таблицы, элементами которой являются номера фрагментов. Например, на второй секунде, с которой начинается передача, на пишущей головке будет 3-ий фрагмент звука, 2-ой фрагмент будет на (2)-ой читающей головке, а 1-ый фрагмент на (3)-ей читающей головке. Передача закончится на $n + 1$ секунде.

Сек.	Пишущая головка	Читающая головка			В линию передан
		2)	3)	4)	
0	1	–	–	–	–
1	2	1	–	–	–
2	3	2	1	–	2 или 1
3	4	3	2	1	3,2 или 1
4	5	4	3	2	4,3 или 2
…	…	…	…	…	
$n-1$	n	$n-1$	$n-2$	$n-3$	
n	–	n	$n-1$	$n-2$	
$n+1$	–	–	n	$n-1$	n или $n-1$

На $n+1$ секунде в линию может быть передан n или $n-1$ фрагмент звука. По очереди рассмотрим оба случая.

1. Пусть на $n+1$ секунде в линию был передан -ый фрагмент (см. таблицу). Тогда -ый фрагмент не мог быть передан на предыдущей секунде. Если посмотреть на таблицу то видно, что количество перестановок фрагментов в этом случае совпадает с $T(n-1)$, то есть количеством способов переставить звук длины $n-1$.

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
3	2	1	3, 2 или 1
4	3	2	4, 3 или 2
…	…	…	
$n-1$	$n-2$	$n-3$	
n	$n-1$	$n-2$	$n-1$ или $n-2$
–	n	$n-1$	n

2. Пусть на $n+1$ секунде в линию был передан $(n-1)$-ый фрагмент (см. таблицу). Тогда $(n-1)$-ый фрагмент не мог быть передан на предыдущих секундах. Так как n-ый фрагмент должен уйти в линию, то он должен быть передан

Читающая головка			В линию
(2)	(3)	(4)	
2	1	–	2 или 1
3	2	1	3, 2 или 1
4	3	2	4, 3 или 2
…	…	…	
$n-1$	$n-2$	$n-3$	$n-2$ или $n-3$
n	$n-1$	$n-2$	n
–	n	$n-1$	$n-1$

в момент времени n. Тогда до $(n-1)$-ой должно быть

передано $(n-2)$ последовательных фрагментов, что может быть сделано $T(n-2)$ способами.

Таким образом $T(n) = T(n-1) + T(n-2)$. Тогда для нахождения количества перестановок $T(n)$ для любого n, достаточно найти $T(1)$, $T(2)$.

Читающая головка			В линию
2)	3)	4)	
–	1	–	1

$$T(1) = 1$$

Читающая головка			В линию
2)	3)	4)	
2	1	–	2 или 1
	2	1	2 или 1

$$T(2) = 2$$

Остается с использованием формулы $T(n) = T(n-1) + T(n-2)$ вычислить нужное значение.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Ответ: 10946

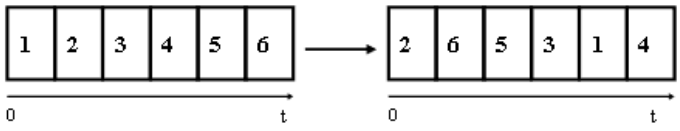
Комментарий

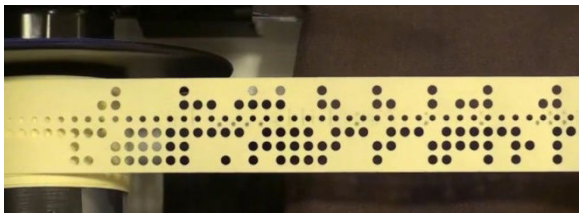
Развитие средств связи к началу Великой Отечественной войны обусловило необходимость перехода от медленных систем предварительного шифрования текстовой информации к синхронному линейному засекречиванию телефонных переговоров непосредственно в процессе связи. В этих условиях стало актуальным создание особой секретной телефонии, которая обеспечила бы надёжную защиту содержания перехваченного противником телефонного разговора.

Задача была решена коллективом специалистов под руководством начальника лаборатории и главного инженера по радио в Центральном научно-исследовательском институте связи Народного комиссариата почт и телеграфов (НИИС НКПиТ) **Владимира Александровича Котельникова**. В сложнейших условиях военного времени в лаборатории был разработан и построен принципиально новый телефонный шифратор «мозаичного» типа «Соболь-П», не имевший аналогов в мире.

Шифратор осуществлял частотно-временные («мозаичные») преобразования речевого сигнала с последующей перестановкой отрезков полученного сигнала по времени. Частотные преобразования заключались в делении сигнала на три-четыре частотных поддиапазона посредством системы полосовых фильтров. К некоторым из частотных поддиапазонов применялись частотные инверсии. Далее поддиапазоны случайным образом перемешивались.

Сигнал, полученный после частотных преобразований, делился на отрезки по 100 миллисекунд и задерживался для осуществления перемешивания отрезков во времени посредством записи на магнитный барабан. Перемешивание частотно-временных отрезков осуществлялось с помощью специального узла, управлявшегося посредством перфоленты, отверстия в которой проделывались случайным (непредсказуемым) образом.





Описанные преобразования надёжно защищали содержание подлежащего засекречиванию речевого сообщения не только от непосредственного подслушивания сигнала в канале связи, но и от попыток восстановить исходную речь доступными на тот момент техническими средствами и методами.

Уровень безопасности телефонных переговоров, обеспечиваемый аппаратурой «Соболь-П», для своего времени являлся беспрецедентным. По каналам связи, оборудованным аппаратурой «Соболь-П», разрешалась передача совершенно секретных донесений и приказов.

Задача 9 (11 класс)

Рассмотрим девять чисел $k_1, \dots, k_9$, где $k_i \in \{0,1,2\}$. При этом хотя бы одно число k_i отлично от нуля. С помощью этих чисел вырабатывают последовательность $u_1, u_2, \dots, u_{2019}$ по формулам: $u_1 = k_1,\ u_2 = k_2, \dots,\ u_9 = k_9$, $u_{i+9} = r_3(u_i + u_{i+1}),\ i = 1,2, \dots, 2010$, где $r_3(a)$ – остаток от деления числа a на 3. Найдите такое наименьшее натуральное число l, что какие бы исходные числа $k_1, \dots, k_9$ мы ни взяли, в последовательности $u_1, u_2, \dots, u_l$ каждое из чисел 0, 1 и 2 гарантированно встретится хотя бы один раз.

Решение

Для каждого набора $\boldsymbol{k} = (k_1, \dots, k_9)$ укажем такое минимальное l, что в соответствующей последовательности $u_1, u_2, \dots, u_l$ присутствует каждое из чисел 0, 1 и 2. Затем среди всех таких l останется выбрать наибольшее – это и будет ответом в задаче.

1. В наборе $\boldsymbol{k}$ встречается каждое из чисел 0, 1 и 2. Тогда искомое l не превосходит 9;

2. Набор $\boldsymbol{k}$ состоит только из 1. Тогда $u_{10} = \dots = u_{17} = 2$ и $u_{18} = 0$. Значит $l = 18$;

3. В наборе $\boldsymbol{k}$ присутствуют и 1, и 2, но нет 0. Значит среди чисел $u_1, u_2, \dots, u_9$ есть два соседних (u_s и u_{s+1}), одно из которых равно 1, а другое 2. Тогда $u_{s+9} = 0$ и $l \leq 17$;

4. Набор $\boldsymbol{k}$ состоит из 0 и 1. Число 2 впоследствии дадут только две рядом стоящие 1. Поэтому рассмотрим варианты:

a) в $\boldsymbol{k}$ есть рядом стоящие 1. Тогда $l < 19$;

b) в $\boldsymbol{k}$ нет рядом стоящих 1. Здесь возможны следующие случаи:

- Есть хоть одна 1 «не с краю». То есть найдется номер s такой, что $2 \leq s \leq 8$ и $k_s = 1$. Рядом стоящих 1 нет, поэтому $k_{s-1} = k_{s+1} = 0$. Тогда $u_{s+8} = u_{s+9} = 1$. Следовательно, $u_{s+17} = 2$ и $l \leq 25$;
- 1 есть только «с краю». Пусть $\boldsymbol{k} = (1,0, \dots, 0)$. В этом случае начало последовательности $u_1, u_2, \dots$ можно вычислить непосредственно: $\{u_n\} = \{1,$ 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0,

0, 0, 0, 1, 2, 1, 0,…} и убедиться, что $l = 27$. Пусть $\boldsymbol{k} = (1,0,\dots 0,1)$. Тогда $\{u_n\}$ ={1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0…} и $l = 18$. И, наконец, для $\boldsymbol{k} = (0,\dots 0,1)$ находим $\{u_n\}$ ={0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0, …}, $l = 26$.

Отметим, что случаи, «$\boldsymbol{k}$ состоит только из 2» и «$\boldsymbol{k}$ состоит только из 0 и 2» эквивалентны случаям 2 и 4 соответственно. Действительно, если в последовательности $\{u_n\}$, отвечающей набору $2 \cdot \boldsymbol{k}$**,** заменить все 2 на 1, а 1 на 2, то получится последовательность, соответствующая набору $\boldsymbol{k}$.

Ответ: $l = 27$.

Комментарий

Последовательность чисел $\{u_n\}$, удовлетворяющая при некоторых числах $m \in \mathbb{N}, a_0, \dots, a_{m-1} \in \mathbb{R}$ рекуррентному соотношению при всех $n \in \mathbb{N}_0$

$$u_{n+m} = a_{m-1}u_{n+m-1} + \cdots + a_1u_{n+1} + a_0u_0,$$

называется линейной рекуррентной последовательностью (ЛРП) порядка m, а многочлен

$$f(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0$$

– ее характеристическим многочленом. ЛРП – это такая рекуррентная последовательность, в которой очередной член есть фиксированная линейная комбинация ее предыдущих членов. Примерами ЛРП служат *последовательности Фибоначчи, арифметические и геометрические прогрессии.*

ЛРП применяются для построения генераторов псевдослучайных последовательностей, которые в свою

очередь используются в *шифрах гаммирования* в качестве источника случайной и равновероятной *гаммы*. Стоит отметить, что для того, чтобы ЛРП могла быть использована в таких генераторах, она должна удовлетворять достаточно большому набору криптографических характеристик, в противном случае гамма может оказаться «плохой» и соответствующая шифрсистема окажется нестойкой. Параметр l можно рассматривать как одну из таких характеристик. Он показывает наименьшую длину отрезка последовательности, на которой каждое из чисел 0, 1, 2 встретиться хотя бы один раз. Отсутствие хотя бы одного из этих чисел в отрезке последовательности заведомо означало бы неравновероятность рассматриваемой ЛРП $\{u_n\}$.

ПРИЛОЖЕНИЕ
(основные обозначения и свойства остатков)

Обозначения:

- запись $A \Leftrightarrow B$ означает, что утверждение A выполняется тогда и только тогда, когда выполняется утверждение B, а $A \Rightarrow B$ означает, что из A следует B;
- запись $a \in M$ означает принадлежность элемента a множеству M;
- НОД(a, b) – наибольший общий делитель чисел a и b;
- $k = 1,2,3 \ldots$ – индекс k пробегает (принимает последовательно) значения $1,2,3 \ldots$;
- $\mathbb{N}$ – множество натуральных чисел;
- $r_n(x)$ – остаток от деления натурального числа x на ненулевое целое число n.

Определение. *Разделить целое число a на ненулевое целое число n с остатком означает найти такие целые числа q, r такие, что выполнено равенство $a = q \cdot n + r$, и при этом $0 \le r < |n|$ – остаток от деления числа a на n, который обозначают как $r_n(a)$, а число q называют неполным частным.*

Пример. Остаток от деления 7 на 3 равен 1 (то есть $r_3(7) = 1$), поскольку $7 = 3 \cdot 2 + 1$. В то же время остаток от деления -2 на 3 так же равен 1 ($r_3(-2) = 1$): $-2 = 3 \cdot (-1) + 1$.

Теорема. *Любое целое число a можно разделить с остатком на ненулевое целое число n, при этом остаток и неполное частное определены однозначно.*

Утверждение. *Справедливы следующие свойства:*

1. $r_n(a + c) = r_n(r_n(a) + r_n(c))$;

2. $r_n(a \cdot c) = r_n(r_n(a) \cdot r_n(c))$;
3. $r_n(a) = r_n(c) \Leftrightarrow a - c$ *делится на* n.

Проверка работ проводилась централизовано по единым критериям. Всего дипломами I, II, III степени награждены более 150 участников. Задания олимпиады были подготовлены для каждой возрастной категории (8-9, 10 и 11 классы) в нескольких равноценных вариантах. В сборнике приводились условия и решения одной из задач каждого типа.

С задачами прошедших олимпиад по математике и криптографии и их решениями можно ознакомиться:

- на сайте www.cryptolymp.ru в разделе «Подготовка к олимпиаде» и «Архив задач»;
- на сайте Академии ФСБ России по адресу www.academy.fsb.ru (раздел для абитуриентов);
- в учебно-методическом журнале «Математика», Издательский дом «Первое сентября» (ежегодно в одном из апрельских выпусков, www.1september.ru);
- в книге «Введение в криптографию» (М.:МЦНМО, 2012);
- в книге «Олимпиады по криптографии и математике для школьников» (М.: МЦНМО, 2013);
- также можно получить доступ к системе дистанционного обучения для подготовки к олимпиаде на сайте: http://www.v-olymp.ru.