10 класс XXXI Межрегиональная олимпиада школьников им. И.Я. Верченко по математике и криптографии

1 вариант

1. Решите уравнение $p^4 + q^2 = n^2$, где p и q – простые числа, а n –натуральное число.

Решение: Перепишем исходное равенство: $p^4 = (n-q)(n+q)$.

Учитывая, что $(n-q) < (n+q)$ и что p – простое число, возможны следующие случаи:

1) $\begin{cases} n-q=1 \\ n+q=p^4 \end{cases}$

2) $\begin{cases} n-q=p \\ n+q=p^3 \end{cases}$

В случае 1): вычтем из второго уравнения первое. Получим равенство

$$2q = p^4 - 1$$

Это равносильно

$$2q = (p-1)(p+1)(p^2+1)$$

Так как q простое число, то это возможно только при $p-1=1$. Непосредственной проверкой убеждаемся, что $p=2$ не подходит.

В случае 2): вычтем из второго уравнения первое. Получим равенство

$$2q = p^3 - p$$

Это равносильно

$$2q = (p-1)p(p+1)$$

Так как q простое число, то это возможно только при $p-1=1$.

Отсюда найдём $p=2, q=3, n=5$.

Ответ: $p=2, q=3, n=5$.

2. Дана последовательность $a_1, b_1, a_2, b_2, \dots, a_k, b_k$, состоящая из 0 и 1. Пусть N – количество чисел i от 1 до k таких, что $a_i = 0$ и $b_i = 1$. Докажите, что число последовательностей указанного вида, для которых N нечетно, находится по формуле $2^{2k-1} - 2^{k-1}$.

Решение: Применим метод математической индукции по параметру k. При $k=1$ формула очевидна. Допустим формула верна для значения $k-1$. Искомое число равно числу последовательностей $a_1, b_1, a_2, b_2, \dots, a_{k-1}, b_{k-1}$, в которых количество $i = 1,2,\dots,k-1$ таких, что $a_i = 0$ и $b_i = 0$ четно (в этом случае пара (a_k, b_k) может быть только $(0,1)$) плюс количество последовательностей $a_1, b_1, a_2, b_2, \dots, a_{k-1}, b_{k-1}$, в которых количество чисел $i = 1,2,\dots,k-1$ таких, что $a_i = 0$ и $b_i = 1$ нечетно, умноженному на 3 (так как пара (a_k, b_k) может быть любой из пар $(0,0), (1,0), (1,1)$). В итоге по предположению индукции нужное число последовательностей будет удовлетворять равенству

$$\left(2^{2(k-1)} - \left(2^{2(k-1)-1} - 2^{k-2}\right)\right) + 3\left(2^{2(k-1)-1} - 2^{k-2}\right) = 2^{2k-1} - 2^{k-1}.$$

Комментарий

Во многих криптографических приложений в качестве функций усложнений или функций гаммирования используются двоичные булевы функции. В то же время важно, чтобы

используемая функция принимала значение 0 и 1 на равном количестве наборов, т. е. была сбалансированной. Помимо таких функций, особое место в криптографии занимают так называемые бент-функции, которые более всех остальных «не похожи» на линейные функции. Это обусловлено тем, что близость к линейной функции упрощает задачу нахождения решения или других ключевых элементов схемы. Без доказательства отметим, что любая бент-функция не является сбалансированной, что затрудняет их непосредственное использование в криптографических приложениях. Однако они широко используются как первоначальные конструкции с целью построения сбалансированных функций достаточно «удаленных» от класса всех линейных функций. В данной задаче искалось количество наборов, на которых бент-функция $\overline{a_1}b_1 \oplus \overline{a_2}b_2 \oplus \ldots \oplus \overline{a_k}b_k$, где $\oplus$ – стандартная операция сложения битов, принимает значение 1. Из решения задачи следует, что такая фукнкция действительно не является сбалансированной.

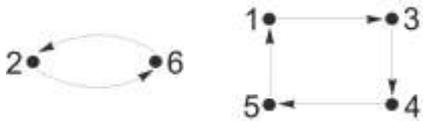
3. Петя использует для работы в интернете пароли из шести символов. Опасаясь злоумышленников, он решил в каждом пароле изменить порядок следования символов, используя для этого одно и то же *правило*, которое записал в книжечку. Правило могло выглядеть, например, так: $\begin{pmatrix}1&2&3&4&5&6\\3&6&4&5&1&2\end{pmatrix}$. То есть первый символ ставится на третье место, второй – на шестое и так далее. В своем пароле для почты **qwerty** Петя переставил буквы по правилу из книжечки, а затем, для большей надежности переставил буквы по этому же правилу еще раз. (Если использовать правило как в примере, то из **qwerty** после первой перестановки получится **tyqerw**, а после второй – **rwtqey**). Какие из нижеследующих комбинаций могли быть получены двойной перестановкой букв в пароле **qwerty** (используя, возможно, другие правила указанного вида):

а)

yetrqw eyrtqw yrwteq rewqyt qwtyre tywreq

б) Петя потерял книжечку! Он помнит, что первоначально пароль был **qwerty**, но правило, по которому были в нем дважды переставлены буквы, не помнит. За какое наименьшее число попыток можно с гарантией подобрать утерянный пароль?

Решение: Приведенное в условии правило перестановки букв, или *перестановку*, будем обозначать греческой буквой σ. Перестановку σ можно интерпретировать как отображение множества цифр {1, 2, 3, 4, 5, 6} в себя. Например, тот факт, что первая буква перешла на третье место, можно записать как $\sigma(1) = 3$, а также изобразить стрелочкой из 1 в 3:

$\sigma = \begin{pmatrix}1&2&3&4&5&6\\3&6&4&5&1&2\end{pmatrix}$	

Видно, что если бы мы перестановку σ применяли многократно, то буквы на 2-й и 6-й позициях постоянно менялись бы местами, а буквы на позициях 1, 3, 4, 5 переставлялись бы по циклу. Поэтому перестановка σ может символически быть записана в виде *произведения циклов*:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 5 & 1 & 2 \end{pmatrix} = (1345)(26) = 4 * 2.$$

Запись $4 * 2$ отражает *цикловую структуру* перестановки σ, показывая, что в ней один цикл длины 4 и один цикл длины 2.

Посмотрим теперь более детально на то, что произойдет, если по правилу σ переставить буквы еще раз. Так 1 при первом применении правила σ перешла в 3: $\sigma(1) = 3$, а при повторном применении 3 перешла в 4: $\sigma(3) = 4$. Значит, в результате двойной перестановки 1 переходит в 4. Будем это записывать как $\sigma(\sigma(1)) = 4$ или же $\sigma^2(1) = 4$. Поэтому правило двойной перестановки букв, представляющее собой *квадрат перестановки* σ, выглядит так:

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 3 & 6 \end{pmatrix}$ $= (14)(13)(2)(6)$ $= 2 * 2 * 1 * 1$	

Заметим, что после повторной перестановки 2 и 6 вернутся на свои места, то есть цикл (2, 6) распадется на два тривиальных цикла (2) и (6), а цикл (1345) превратится в два цикла (1,4) и (3, 5). Таким образом, при повторном применении перестановки циклы четной длины $2n$ распадаются на два цикла, длины n каждый. Несложно проверить, что при этом циклы нечетной длины сохраняются. Справедливо утверждение.

Утверждение. *Перестановка представляет собой полный квадрат в том и только том случае, когда в ее представлении в виде произведения непересекающихся циклов имеется сколько и каких угодно циклов нечетной длины, в то время как циклов одной и той же четной длины должно быть четное число.*

Рассмотрим первую комбинацию yeqwrt из пункта а). Она получена из qwerty цикл длины 6. перестановкой (123456) = (1324561), которая представляет собой 342561

Поскольку циклов четной длины здесь нечетное количество (всего один), то, согласно утверждению, такая комбинация двойной перестановкой букв получиться не могла. Аналогично исследуются и остальные комбинации в пункте а).

Проведем подсчет общего числа перестановок, являющихся полными квадратами. Их цикловые структуры могут быть следующие:

- $1 * 1 * 1 * 1 * 1 * 1$. Это перестановка, оставляющая все на своих местах (тождественная перестановка). Она единственна.
- $1 * 5$. Мы должны выбрать 5 элементов из шести, чтобы составить цикл дины 5. Это можно сделать 6-ю способами. Из пяти элементов цикл длины 5 можно организовать $(5 - 1)!$ способами (действительно, организуем цикл из пяти элементов a_1, a_2, a_3, a_4, a_5; элемент a_1 может перейти в любой из четырех (т.к. в себя нельзя), элемент a_2 переходит в один из оставшихся трех и т.д. В итоге получаем $4 \cdot 3 \cdot 2 \cdot 1$ способов). Таким образом, здесь $6 \cdot 4! = 144$ перестановок.
- $2 * 2 * 1 * 1$. Выбрать два элемента из шести для первого цикла длины 2 можно C_6^2 способами. Для второго цикла длины 2 есть C_4^2 способа. Итого $C_6^2 \cdot C_4^2 = 90$. От порядка

следования циклов результат не зависит, поэтому 90 еще следует разделить на два. Всего 45 перестановок с такой структурой.

• $3 * 3$. Здесь мы 6 элементов десятью способами ($\frac{1}{2}C_6^3 = 10$) разбиваем на две тройки и из каждой тройки получаем по 2 цикла. Всего 40 перестановок.

• $3 * 1 * 1 * 1$. Здесь мы двадцатью способами ($C_6^3 = 20$) выбираем тройку и из каждой тройки получаем по 2 цикла. Всего 40 перестановок.

В итоге, имеется $1 + 144 + 45 + 40 + 40 = 270$ перестановок длины 6, представляющих собой полный квадрат.

Ответ: а) Полученные двойной перестановкой комбинации выделены цветом.

	y e t r q w	e y r t q w	y r w t e q	r e w q y t	q w t y r e	t y w r e q

б) 270.

4. На вход устройства подается лента с записанными на ней нулями и единицами:

Лента	**0** 0 0 **0** 1 1 0 0 **1** 0 1 0 1 1 1 1 0 1 0 0 1 1 0 1 0 1 1 0 0… ⇨
Позиции	μ_1 μ_2 μ_3

За один такт устройство считывает с ленты с позиций μ_1, μ_2, μ_3 (на первом такте $\mu_1 = 1$) три значения x, y, z. Если $x + y - z \geq 1$, то устройство на новой ленте печатает 1, иначе – 0. Затем устройство сдвигается на одну позицию вправо, и процедура повторяется. Найдите разности $d_1 = \mu_2 - \mu_1$ и $d_2 = \mu_3 - \mu_2$, если известно, что $d_1 + d_2 \leq 11$, а на новой ленте было напечатано следующее: 0 0 0 1 0 0 0 0 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1 0 1 1 1 0 1 1 0 1 0 1 0 1 0 0 1 … (для примера на рисунке изображен случай $d_1 = 3, d_2 = 5$).

Решение: Число возможных вариантов d_1 и d_2 : $10 + 9 + \cdots + 1 = 55$, можно для каждого варианта проверять, что соответствие входных и выходных символов, а можно предложить более быстрый способ, заключающийся в нахождении сначала d_1 (максимум 10 вариантов), а затем d_2. Для этого достаточно заметить следующее.

Если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии d_1 вида 1 ... 1 в произвольном такте работы μ_1:

$$x_{\mu_1} + x_{\mu_1+d_1} - x_{\mu_1+d_1+d_2} \geq 1,$$
$$x_{\mu_1+d_1} + x_{\mu_1+2d_1} - x_{\mu_1+2d_1+d_2} \geq 1,$$

то если $x_{\mu_1+d_1} = 0$, то $x_{\mu_1} = 1, x_{\mu_1+2d_1} = 1$.

Это позволяет отбраковать опробуемый вариант d_1. Устанавливаем, что $d_1 = 2$.

Аналогично, если рассмотреть систему уравнений, соответствующую выходным знакам на расстоянии d_2 вида 0 ... 1 в произвольном такте работы μ_1 :

$$x_{\mu_1} + x_{\mu_1+d_1} - x_{\mu_1+d_1+d_2} \leq 0,$$
$$x_{\mu_1+d_2} + x_{\mu_1+d_1+d_2} - x_{\mu_1+d_1+2d_2} \geq 1,$$

тогда если $x_{\mu_1+d_1+d_2} = 0$, то $x_{\mu_1+d_1} = 0, x_{\mu_1+d_1+2d_2} = 0$.

Это позволяет отбраковать опробуемый вариант d_2 (с учётом найденного ранее $d_1 = 2$). Находим $d_2 = 6$..

Ответ: $d_1 = 2, d_2 = 6$.

Комментарий

В данной задаче в качестве объекта исследования рассматривался так называемый *фильтрующий генератор*. Фильтрующий генератор представляет из себя бесконечную последовательность символов исходного алфавита, подчиняющуюся некоторому рекуррентному закону, а также функцию усложнения, принимающую значения этой последовательности на некоторых позициях, сдвигающихся совместно с тактами работы генератора. Полученная в результате работы такого генератора последовательность будет близка к случайной, то есть являться псевдослучайной, именно поэтому фильтрующий генератор – это один из типовых примеров генераторов псевдослучайных последовательностей.

Функция усложнения данной задачи является пороговой функцией, то есть двоичной функцией, заданной неравенством. Известно, что такая функция представляет приближенную модель работы логики нейронов живых организмов.

Позиции, с которых поступают значения на функцию выхода, называются точками съема. Вопросом же данной задачи на самом деле является определение расстояния между точками съема по известному входу (изначальной бесконечной последовательности) и выходу (полученной псевдослучайной последовательности).

5. Знаками открытого и шифрованного текстов являются пары целых от 0 до 31. Для зашифрования используется секретный ключ k (целое число от 0 до 31), заданная таблично функция h, а также функция $g(c, d)$, которая паре целых чисел (c, d) ставит в соответствие пару

$(d, c + h(d + k))$ (причем если число $d + k$ или $d + h(d + k)$ превышает 31, то их заменяют остатком от деления на 32). Знак шифрованного текста $(b1, b2)$ получается из знака открытого текста $(a1, a2)$ путем 128-кратного применения функции g:

$(b_1, b_2) = g^{128}(a_1, a_2) = g\,(\ldots\, g(g(a_1, a_2)))$.

Известно, что знак открытого текста (21,0) преобразовался в знак зашифрованного текста (15,25), знак (7,3) преобразовался в (29,5), (0,17) – в (25,4) и, наконец, (5,21) – в (22,9). Найдите ключ k.

i	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
$h(i)$	9	1	30	4	24	12	8	23	18	7	16	15	21	26	10	17	19	22	13	28	14	11	2	29	3	6	27	0	5	25	31	20

Решение: Для решения задачи необходимо заметить, что из равенств

$$(b_1, b_2) = g^{128}(a_1, a_2),$$
$$(b_1', b_2') = g^{128}(a_1', a_2'),$$
$$(a_1', a_2') = g(a_1, a_2)$$

следует равенство

$$(b_1', b_2') = g(b_1, b_2).$$

Необходимым условием выполнения равенств $(a_1', a_2') = g(a_1, a_2)$, $(b_1', b_2') = g(b_1, b_2)$ являются равенства $a_1' = a_2$, $b_1' = b_2$. Среди приведенных в задаче пар знаков открытого и

шифрованного текстов есть знаки, удовлетворяющие этому условию: одна пара $(21,0)$, $(0,17)$ и вторая пара $(29,5), (5,21)$. То есть

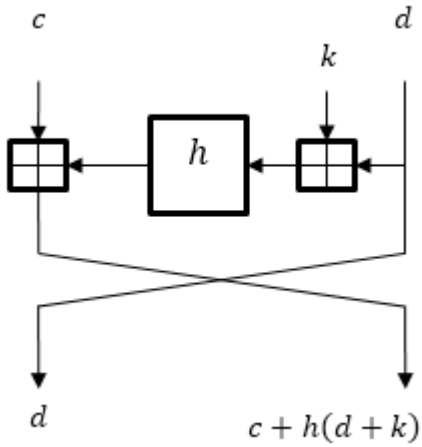
$$(15,25) = g^{128}(21,0),$$
$$(25,4) = g^{128}(0,17).$$

Из условия задачи возможность найти ключ – воспользоваться равенствами

$$(0,17) = g(21,0), (25,4) = g(15,25).$$

Остается убедиться, что при этих условиях оба равенства дают одинаковое значение ключа k

Работу функции g можно схематично изобразить следующим образом:



Ответ: 19.

Комментарий

Описанный в решении метод получения ключа в литературе носит название сдвиговой атаки или slide attack. В простейшем случае данная атака применяется к алгоритмам шифрования, представляющим собой многократное повторение функции шифрования на некотором фиксированном ключе. Интересной особенностью сдвиговой атаки заключается в том, что его эффективность не зависит от числа итераций, используемых в алгоритме шифрования.

6. Подписью битового сообщения $(a_1, \dots, a_5)$ является любой битовый набор $(x_1, \dots, x_{10})$, который удовлетворяет соотношениям

$a_1 = b_3 \oplus b_4 \oplus b_5$, $\quad b_1 = x_1x_9 \oplus x_2x_{10} \oplus x_3x_8 \oplus x_4x_9 \oplus x_5x_9 \oplus x_6x_8 \oplus x_7x_8 \oplus x_9x_{10}$,

$a_2 = b_2 \oplus b_4 \oplus b_5$, $\quad b_2$
$= x_1x_8 \oplus x_2x_9 \oplus x_3x_{10} \oplus x_4x_8 \oplus x_5x_{10} \oplus x_6x_{10} \oplus x_7x_8 \oplus x_8x_9$,

$a_3 = b_2 \oplus b_3 \oplus b_5$, $\quad b_3$
$= x_1x_9 \oplus x_2x_{10} \oplus x_3x_8 \oplus x_4x_7 \oplus x_5x_8 \oplus x_6x_8 \oplus x_7x_8 \oplus x_8x_9 \oplus x_{10}$,

$a_4 = b_1 \oplus b_2 \oplus b_3$, $\quad b_4$
$= x_1x_7 \oplus x_2x_{10} \oplus x_3x_{10} \oplus x_4x_7 \oplus x_5x_7 \oplus x_6x_{10} \oplus x_7x_{10} \oplus x_9x_{10}$,

$$a_5 = b_1 \oplus b_3 \oplus b_5, \quad b_5 = x_1x_8 \oplus x_2x_7 \oplus x_3x_7 \oplus x_4x_9 \oplus x_5x_9 \oplus x_6x_8 \oplus x_7x_8 \oplus x_8x_{10} \oplus x_9.$$

Здесь $\oplus$ – стандартная операция сложения битов: $0 \oplus 0 = 1 \oplus 1 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1$. Найдите какую-нибудь подпись для сообщения (0,1,0,0,0).

Решение: Сначала надо решить систему линейных уравнений и определить значения $(b_1, \dots, b_5)$. После в квадратичной системе от переменных $x_1, \dots, x_{10}$ зафиксируем значения переменных x_7, x_8, x_9, x_{10} произвольным образом и решим полученную систему линейных уравнений относительно оставшихся переменных. В случае, если получится несовместная СЛУ как, например, при $x_6 = 1, x_7 = 0, x_8 = 1$ то необходимо зафиксировать значения переменных x_6, x_7, x_8 другим образом. Например, при фиксации $x_6 = 1, x_7 = 0, x_8 = 0$ имеем два решения $x_1 = 0, x_2 = 0, x_4 = 1, x_3 = x_5$

Комментарий

В данной задаче предлагается осуществить подделку цифровой подписи. Примечательно, что рассматриваемая в задача криптографическая модель электронной цифровой подписи является упрощенным вариантом реальной электронной цифровой подписи Rainbow, которая выиграла международный конкурс стандартизации постквантовых криптографических схем подписи. Практическая стойкость электронной цифровой подписи Rainbow гарантируется математически доказанной сложностью вычисления декомпозиции квадратичного отображения, которая остается достаточно высокой даже с учетом возможности использования квантовых вычислителей.