педагогические науки (теория и методика профессионального образования). Калининград: Изд-во БГАРФ. – 2018. – № 3 (45). – С. 89–96.

16. Тесленко А. Н., Тамарская Н. В. Социализация молодежи в условиях постиндустриального урбанизированного общества // ИЗВЕСТИЯ Балтийской государственной академии рыбопромыслового флота: психолого-педагогические науки (теория и методика профессионального образования). – Калининград: Изд-во БГАРФ. – 2018. – № 3 (45). – С. 31–35.

17. Шамис Е., Никонов Е. Теория поколений. Необыкновенный Икс. – Саратов: Synergy Book, 2020. –192 с.

С. И. Иванова, М. Н. Иванова, И. А. Иванов, С. П. Грушевский

УДК 378.147:511

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ТЕОРИИ ЧИСЕЛ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время вопросы шифрования-дешифрования информации приобрели особое значение, хотя возникли достаточно давно [2; 9]. Различные аспекты методов шифрования информации представлены в достаточно большом количестве исследований в области криптографии [1; 2; 6]. В последнее время появились новые направления в криптографии, например, сложностная криптография [3], инкрементальная криптография [9] и т. д.

Специалист в области криптографии должен обладать высоким уровнем математической культуры в области теории чисел [5; 7] – это, как правило, основа систематических курсов по криптографии [4; 8] для студентов вузов.

Очевидно, что качество подготовки специалистов по информационной безопасности связано с умением решать задачи по криптографии, при этом формировать это умение надо как можно раньше и лучше со школьной скамьи. Это направление реализуется в России с 1991 г. в форме межрегиональной олимпиады школьников (9–11 классы) по математике и криптографии [10; 11; 12; 13; 14]. «Основными целями и задачами Олимпиады являются выявление и развитие творческих способностей, интереса к научной деятельности, создание условий для интеллектуального развития, поддержки одаренных детей, в том числе содействие им в профессиональной ориентации и продолжении образования» [10]. Сайт олимпиады по математике и криптографии содержит материалы для подготовки к олимпиаде: приведен список литературы для подготовки к олимпиаде, предоставлена возможность дистанционной подготовки к различным этапам олимпиады, приведены методические материалы для подготовки к олимпиаде [12; 13].

При решении олимпиадных задач по криптографии используется математический аппарат (некоторые понятия объектов, их свойства), который, как правило, редко используется в основной школе. Примером такого понятия является понятие *сравнения по модулю* и его свойства.

Определение 1. Число $a \in Q$ сравнимо с числом $b \in Q$ (a, b – целые числа) по модулю $m \in N$ (т. е. $a \equiv b \,(mod\, m)$), если $(a - b) \vdots m$.

Из данного определения вытекает ряд свойств сравнений по модулю m, доказываемых по определению. Характер рассуждений при решении задач олимпиад часто соответствует характеру рассуждений, используемых при доказательстве свойств сравнений по модулю m. Примеры приведены ниже.

Свойства:

Если $a \equiv b \,(mod\, m)$ и $c \equiv d \,(mod\, m)$,

то $(a + c) \equiv (b + d) \pmod m$, (здесь и в дальнейшем *a, b, c, d* – целые числа, *m* – натуральное).

Доказательство. По определению $(a - b) \vdots m$, $(c - d) \vdots m$, значит, $((a - b) + (c - d)) \vdots m$, т. е. $(a + c) - (b + d) \vdots m$.

Тогда $(a + c) \equiv (b + d) \pmod m$.

2. Если $a \equiv b \pmod m$, то $ac \equiv bc \pmod m$.

Доказательство. По определению $(a - b) \vdots m$, значит $((a - b)c) \vdots m$, тогда $(ac - bc) \vdots m$, т. е. $ac \equiv bc \pmod m$.

3. Если $a \equiv b \pmod m$, то для $n \in N$ $a^n \equiv b^n \pmod m$.

Доказательство. По определению $(a - b) \vdots m$, $a^n - b^n \vdots (a - b$, тогда $a^n - b^n \vdots m$, т. е. $a^n \equiv b^n \pmod m$.

4. Если $a \equiv b \pmod m, b \equiv c \pmod m$, то $a \equiv c \pmod m$.

Доказательство. По определению $(a - b) \vdots m$, $(b - c) \vdots m$, Тогда $((a - b) + (b - c)) \vdots m$, т. е. $(a - c) \vdots m$, значит, $a \equiv c \pmod m$.

5. $(m - 1)a \equiv -a \pmod m$.

Доказательство., $(m - 1)a - (-a) = ma \vdots m$ т. е. $(m - 1)a \equiv -a \pmod m$.

При решении задач часто применяется следующая *лемма*.

Лемма 1. Для любого $x \in N$ верно: если $x \vdots 3$, то $x^2 \equiv 0 \pmod 3$, иначе $x^2 \equiv 1 \pmod 3$.

Доказательство. Верно, если $x \vdots 3$, то $x^2 \vdots 3$, т. е. $x^2 \equiv 0 \pmod 3$. Иначе применяем метод анализа остатков. Данный метод заключается в переборе остатков по заданному модулю и рассмотрении каждого из случаев. Если $x \equiv 1 \pmod 3$, то по свойству 3 $x^2 \equiv 1 \pmod 3$. Если, $x \equiv 2 \pmod 3$ то по свойству 3 $x^2 \equiv 2^2 \pmod 3$, т.е. $x^2 \equiv 4 \pmod 3$, а $4 \equiv 1 \pmod 3$, значит $x^2 \equiv 1 \pmod 3$ (по свойству 4).

Рассмотрим *примеры* решения избранных задач олимпиады по математике и криптографии для школьников 2018–2019 учебного года (автор решений – победитель олимпиады *Иванова С. И.* [14]).

1) *Задачи на сравнения.*

***Задача* 1**. Для шифрования слова из пяти букв каждая его буква заменяется на число согласно таблице. Полученный набор чисел $(x_0, x_1, x_2, x_3, x_4)$ затем преобразуется в набор $(y_0, y_1, y_2, y_3, y_4)$ по следующему правилу. Сначала вычисляем вспомогательные числа $\bar{y_0}, \bar{y_1}, \bar{y_2}, \bar{y_3}, \bar{y_4}$ о формулам

$\bar{y_0} = 2^0 \cdot x_0 + 2^4 \cdot x_1 + 2^3 \cdot x_2 + 2^2 \cdot x_3 + 2^1 \cdot x_4$,

$\bar{y_k} = (2^k \cdot x_0 + 2^{k-1} \cdot x_1 + \dots + 2^0 \cdot x_k)$

$+ (2^4 \cdot x_{k+1} + 2^3 \cdot x_{k+2} + \dots + + 2^{k+1} \cdot x_4), k = 1, 2, 3.$

$\bar{y_4} = 2^4 \cdot x_0 + 2^3 \cdot x_1 + 2^2 \cdot x_2 + 2^1 \cdot x_3 + 2^0 \cdot x_4$.

Далее полагаем равным остатку от деления числа $\bar{y_k}$ на 32. Расшифруйте исходное слово, если $(y_0, y_1, y_2, y_3, y_4) = (11, 27, 2, 16, 0)$.

0	А	16	Р
1	Б	17	С
2	В	18	Т
3	Г	19	У
4	Д	20	Ф
5	Е Ё	21	Х
6	Ж	22	Ц
7	З	23	Ч
8	И	24	Ш
9	Й	25	Щ
10	К	26	Ъ
11	Л	27	Ы
12	М	28	Ь
13	Н	29	Э
14	О	30	Ю
15	П	31	Я

Решение. Для решения данной задачи необходимо *найти закономерность*. Выпишем $\bar{y_0}, \bar{y_1}, \bar{y_2}, \bar{y_3}, \bar{y_4}$ в явном виде.

$\bar{y_0} = x_0 + 16x_1 + 8x_2 + 4x_3 + 2x_4$

$\bar{y_1} = 2x_0 + x_1 + 16x_2 + 8x_3 + 4x_4$ $\bar{y_3} = 8x_0 + 4x_1 + 2x_2 + x_3 + 16x_4$

$\bar{y_4} = 16x_0 + 8x_1 + 4x_2 + 2x_3 + x_4$

Заменим уравнения на сравнения (ведь $y_k \equiv \bar{y_k} \pmod{32}$). Получаем:

$y_0 \equiv x_0 + 16x_1 + 8x_2 + 4x_3 + 2x_4 \pmod{32}$

$y_1 \equiv 2x_0 + x_1 + 16x_2 + 8x_3 + 4x_4 \pmod{32}$

$y_2 \equiv 4x_0 + 2x_1 + x_2 + 16x_3 + x_4 \pmod{32}$

$y_3 \equiv 8x_0 + 4x_1 + 2x_2 + x_3 + 16x_4 \pmod{32}$

$y_4 \equiv 16x_0 + 8x_1 + 4x_2 + 2x_3 + x_4 \pmod{32}$.

Получаем систему из пяти сравнений по модулю 32 с пятью неизвестными. Решениями данной системы будут числа, с которыми сравнимы x_0, x_1, x_2, x_3, x_4 по модулю 32. По свойству 1 сравнений данную систему можно решать методом сложения сравнений и домножения сравнений на целое число (свойство).

2). Заметим, что если умножить первое сравнение в системе на 2 и вычесть второе, получим:

$2y_0 - y_1 \equiv 31x_1 \ (mod 32)$.

Аналогично:

$2y_1 - y_2 \equiv 31x_2 \ (mod\ 32)$

$2y_2 - y_3 \equiv 31x_3 \ (\text{mod } 32)$

$2y_3 - y_4 \equiv 31x_4 \ (mod\ 32)$

$2y_4 - y_0 \equiv 31x_0 \ (mod\ 32)$.

По свойству 5 сравнений $31x_1 \equiv -x_1$ (*mod* 32).

Подставляя y_0, y_1, y_2, y_3, y_4 из условия задачи:

$-5 \equiv -x_1 \ (mod\ 32)$

$52 \equiv -x_2 \ (mod\ 32)$

$-12 \equiv -x_3 \ (mod\ 32)$

$32 \equiv -x_4 \ (mod\ 32)$

$-11 \equiv -x_0 \ (mod\ 32)$.

Т. к. $\{x_0, x_1, x_2, x_3, x_4\} \in [0; 31]$ и являются целыми неотрицательными числами, то система сравнений принимает вид:

$x_1 = 5$

$20 \equiv -x_2 \ (mod\ 32)$

$x_3 = 12$

$x_4 = 0$

$x_0 = 11$.

Осталось решить сравнение $20 \equiv -x_2$ (*mod* 32). Домножим обе части на -1 (по свойству 2), получим $-20 \equiv x_2$ (*mod* 32), тогда по свойству 5 $-20 \equiv 12$ (*mod* 32), т.е. $x_2 = 12$. Тогда $x_0 = 11$, $x_1 = 5$, $x_2 = 12$, $x_3 = 12$, $x_4 = 0$.

Восстанавливаем искомое слово по таблице: ЛЕММА. *Ответ*: ЛЕММА.

Аналогичным методом (методом сравнений по модулю) решается следующая задача.

***Задача* 2.** В Крипто-Вегасе на табло игрового автомата отображаются два натуральных числа $x_0 = 5$ и $y_0 = 201$. При нажатии кнопки первое из этих чисел заменяется на $x_1 = r_{11}(a \cdot x_0 + b)$, где a и b некоторые неизвестные натуральные числа, а второе число заменяется на $y_1 = r_{2017}(y_0 + 523)$.

Здесь $r_k(m)$ – остаток от деления натурального числа m на k. Нажав кнопку еще раз, получим (по таким же формулам) числа $x_2 = r_{11}(a \cdot x_1 + b)$ и $y_2 = r_{2017}(y_1 + 523)$ и так далее. Игрок получает приз, если при очередном нажатии на табло загорятся числа $x_n = 4$ и $y_n = 1993$. Определите:

а) какие из следующих четырех последовательностей

(1): (2, 5, 4, 7, 1), (2): (6, 9, 7, 1, 3),

(3): (7, 10, 9, 2, 8), (4): (1, 0, 8, 8, 7)

при надлежащем выборе a и b в вышеуказанных фиксированных x_0, y_0 могли бы совпасть с последовательностью $(x_1, \ldots, x_5)$ полученной на этом игровом автомате?

б) может ли игрок получить приз, если $(x_1, \ldots, x_5)$ – одна из (реализуемых) последовательностей из пункта а)?

Решение.

а) Формула для x_n имеет вид $x_n = r_{11}(a \cdot x_{n-1} + b)$, т. е. x_n однозначно определяется для любого $n = 1, 2, \ldots$ Т. е., если в какой-то момент $x_k = c$, а $x_{k+1} = d$, то, в дальнейшем, если $x_m = c$, то $x_{m+1} = d$. По этой причине последовательности № 1 и № 4 не подходят: для № 1: 5→2→5→4→7→1, для № 4: 5→1→0→8→8→7.

Рассмотрим, могла ли получиться последовательность № 2. Для этого запишем систему сравнений по модулю и попытаемся найти ее решение. Если решение есть (т. е. если можно найти какие-нибудь a, b, удовлетворяющие системе), то данная последовательность реализуется. Получаем:

$5a + b \equiv 6 \ (mod\ 11)$

$6a + b \equiv 9 \ (mod\ 11)$

$9a + b \equiv 7 \ (mod\ 11)$

$7a + b \equiv 1 \ (mod\ 11)$

$a + b \equiv 3 \ (mod\ 11)$.

Из сравнений 1 и 2 по свойству 1 получаем: $a \equiv 3$ (*mod* 11). Из сравнения 5: $3 + b \equiv 3$ (*mod* 11), тогда $b \equiv 0$ (*mod* 11). Подставим найденные a и b в систему. Получим, что первое сравнение неверно, значит, у данной системы нет решений, т. е. последовательность № 2 не реализуется. Напишем такую же систему для последовательности № 3.

$5a + b \equiv 7 \ (mod\ 11)$

$7a + b \equiv 10 \ (mod\ 11)$

$10a + b \equiv 9 \pmod{11}$

$9a + b \equiv 2 \pmod{11}$

$2a + b \equiv 8 \pmod{11}$.

Вычтем из третьего сравнения четвертое (по свойству 1), получим, что $a \equiv 7 \pmod{11}$. Подставим a в первое уравнение, получаем: $35+b \equiv 7 \pmod{11}$. Тогда $(2 + b7) \equiv (mod\ 11)$, т. е. $b \equiv 5 (\mathrm{mod}\ 11)$. Подставив найденные a и b в исходную систему убеждаемся, что они подходят, т. е., например, при $a = 7$ и $b = 5$ последовательность № 3 реализуется.

b) Рассмотрим последовательность № 3. С учетом найденных выше a и b (имеется в виду, определены остатки от деления чисел a и b на 11) продолжим последовательность x_n:

$x_6 = r_{11}(8a + b) = r_{11}(8 \cdot 7 + 5) = 6$

$x_7 = r_{11}(6a + b) = r_{11}(6 \cdot 7 + 5) = 3$

$x_8 = r_{11}(3a + b) = r_{11}(3 \cdot 7 + 5) = 4$

$x_{10} = r_{11}(0a + b) = r_{11}(0 \cdot 7 + 5) = 5 = x_0$.

Таким образом, у рассматриваемой последовательности x_n длина периода равна 10, то есть $x_n = x_{r_{10}(n)}$. Далее, рассмотрим период последовательности y_n: $y_n = r_{2017}(y_0 + 523n)$. Требуется, чтобы выполнялось $x_n = 4, y_n = 1993$. Далее $x_n = 4$ при $n = 10k + 8$, где k – целое неотрицательное число. Тогда

$y_0 + 523 \cdot (10k + 8) \equiv 1993 \pmod{2017}$

$201 + 5230k + 523 \cdot 8 \equiv 1993 \pmod{2017}$

У данного сравнения существует решение, а значит, игрок может получить приз.

2) *Задачи на* использование леммы 1.

***Задача* 3**. Известно, что оба числа p и $p^{2018}+800$ простые. Докажите, что число тоже $p^4 + 8$ простое.

Решение. Рассмотрим два случая: p делится на 3 и p не делится на 3.

1. p не делится на 3. Тогда в соответствии с леммой 1 $p^2 \equiv 1 \pmod{3}$. Значит, $p^{2018} + 800 = (p^2)^{1009} + 800 \equiv 1^{1009} + 800 \pmod{3}$, $p^{2018} + 800 \equiv 1 + 2 \pmod{3}$, т.е. $p^{2018} + 800$ делится на 3, при этом это так как число больше 800, значит, $p^{2018} + 800$ - простое число, большее 3, и делящееся на 3. Противоречие. Тогда этот вариант невозможен. Значит, p делится на 3. Так как p – простое, то $p = 3$. Тогда $p^4 + 8 = 3^4 + 8 = 89$ – простое, что и требовалось доказать.

***Задача* 4.** Для подтверждения переводимой в банк суммы братья A и B используют «кольцевую подпись», которая не позволяет определить, кто именно из них совершил перевод. Брат A имеет свой открытый ключ и $e_A = 5$ некий секрет, позволяющий для любого натурального $y\ (y \le 90)$ находить x_A такое, что $y = r_{91}(x_A^{e_A})$. Здесь $r_k(m)$ – остаток от деления натурального числа m на k. (У брата B есть свой секрет и свой ключ $e_B = 25$). Тогда брат A для подписи суммы M случайно выбирает натуральные числа x_B и v, не превосходящие 100, вычисляет $y_B = r_{91}(x_B^{e_B})$ находит y_A из уравнения:

$r_{101}(M(y_A + M(y_B + v)) - v^3) = 0$. (*)

Используя свой секрет, брат A находит величину x_A такой, что $y_A = r_{91}(x_A^{e_A})$. Тогда тройка чисел (x_A, x_B, v) будет подтверждением факта перевода данной суммы M. В банке корректность подтверждения проверяют подстановкой $y_A = r_{91}(x_A^{e_A})$, $y_B = r_{91}(x_B^{e_B})$ и v в уравнение(*). Например, (1, 90, 46) корректное подтверждение суммы 46. Постройте хотя бы одно корректное подтверждение суммы $M = 69$.

Решение. В условии задачи дано сравнение по модулю 101, для которого нужно найти хотя бы одно решение. $M(y_A + M(y_B + v)) - v^3 \equiv 0 \pmod{101}$.

Первая мысль, возникающая при решении данной задачи:

$y_B = r_{91}(x_B^{e_B})$, $e_B = 25$. Какое натуральное x_B можно возвести в 25-ую степень? Только $x_B = 1$. Тогда $y_B = 1$. Подставим его в уравнение:

$M(y_A + M(1 + v)) - v^3 \equiv 0 \pmod{101}$

Раскроем скобки: $My_A + M^2 + M^2v - v^3 \equiv 0 \pmod{101}$. Вынесем общие множители, сгруппируем: $M(y_A + M) + v(M^2 - v^2) \equiv 0 \pmod{101}$. Возьмем $v = M$, тогда: $M(y_A + M) \equiv 0 \pmod{101}$. Будем искать такое y_A, что $y_A + M \equiv 0 \pmod{101}$.

Подставим M: $y_A + 69 \equiv 101 \pmod{101}$, тогда $y_A \equiv 32 \pmod{101}$. $y_A = r_{91}(x_A^5)$, тогда возьмем $y_A = 32$, значит $x_A^5 \equiv 32 \pmod{91}$. Возьмем $x_A = 2$. Таким образом, искомое подтверждение (2, 1, 69). *Ответ*: (2, 1, 69).

3) *Задачи на* частотный анализ.

Часто задачи по криптографии (а именно, задачи на шифрование-дешифрование) решаются с помощью поиска символа с наибольшей частотой появления в тексте (метод частотного анализа). Рассмотрим пример.

***Задача* 5.** Для шифрования сообщения на русском языке, знаки препинания в котором опущены, а слова отделены друг от друга знаком «пробела» (-), используется двухблочный шифратор. Первый блок шифратора заменяет буквы сообщения и пробелы (-) на числа в соответствии с таблицей, построенной на основе ключевого слова. Сначала записывается ключевое слово, потом знак пробела (-), потом остальной алфавит в естественном порядке за исключением букв, входящих в ключевое слово (при этом считается, что Е=Ё). Второй блок получает на входе числа из первого блока и осуществляет усложнение шифрованного сообщения по следующему правилу. Первое число он оставляет без изменений, а к каждому следующему прибавляет число, равное произведению числа 33 и остатка от деления на три предыдущего числа. Прочитайте сообщение, зашифрованное этим шифратором на ключе, если известно, что в сообщении встречается слово «здесь»: 30 5 84 6 16 51 10 42 5 72 19 51 14 66 11 66 5 95 70 65 72 4 38 86 66 17 83 94 49 39 17 84 6 17 84 24 29 97 39 11 74 75 4 62 72 1 37 42 6 14 84 25 47 78 6 4 42 20 94.

Решение. Для начала следует разобраться в математической модели шифрования, предлагаемой в условии задачи. Пусть a_n – числа, полученные после применения первого блока шифратора, b_n – числа, полученные после применения второго блока шифратора (т. е. те, что даны в условии задачи). Тогда , $b_n = a_n + r_3(a_{n-1}) \cdot 33$ а $a_n <= 32$, и, далее, $a_n = r_{33}(b_n)$. Вычислим по данным b_n и a_n.

30 5 18 6 16 18 10 9 5 6 19 18 14 0 11 0 5 29 4 32 6 4 5 20 0 17 17 28 16 6 17 18 6 17 18 24 29 31 6 11 8 9 4 29 6 1 4 9 6 14 18 25 14 12 6 4 9 20 28.

Теперь применим указанный выше метод – по частоте встречаемости чисел определить какой-нибудь символ. По условию, в данном сообщении есть пробелы между словами. Если рассмотреть наиболее часто встречающиеся числа (это 5, 6, 18), то можно определить, какое из этих чисел обозначает пробел. 5 и 18 не подходят, т.к. тогда получаются слишком длинные слова. Значит 6 – это пробел. Теперь рассмотрим все слова длины 5 (по условию известно, что в сообщении есть слово “здесь”): “16 18 10 9 5”, “17 18 24 29 31”, “11 8 9 4 29”, “14 18 25 14 12”. Последний вариант не подходит, т.к. в этом слове есть 2 одинаковые буквы (дважды встречается 14), а в слове “здесь” все буквы различны. Буква “д” раньше, чем буква “з” по алфавиту (а если “з” входит в ключ, то код “з” меньше 6), следовательно, слова 1, 2 также не подходят. Таким образом, единственный вариант для слова “здесь” – 11 8 9 4 29.

Заменим то, что уже знаем: 30 5 18 - 16 18 10 Е 5 - 19 18 14 0 3 0 5 Ь С 32 - С 5 20 0 17 17 28 16 - 17 18 - 17 18 24 Ь 31 - ЗДЕСЬ - 1 С Е - 14 18 25 14 12 - С Е 20 28. По слову 1СЕ можно определить, что В - 1.

Так как. Ь – 29, то Э – 30, Ю – 31, Я – 32. Получаем:

Э 5 18 - 16 18 10 Е 5 - 19 18 14 0 3 0 5 Ь С Я - С 5 20 0 17 17 28 16 - 17 18 - 17 18 24 Ь Ю - ЗДЕСЬ - ВСЕ - 14 18 25 14 12 - С Е 20 28.

По слову Э 5 18 получаем, что Т – 5, О – 18. Заменяем:

ЭТО- 16 О 10 Е Т - 19 О 14 0 3 0 Т Ь С Я - С Т 20 0 17 17 28 16 - 17 О - 17 О 24 Ь Ю - ЗДЕСЬ - ВСЕ - 14 О 25 14 12 - С Е 20 28.

Слово 17 О – не ТО, не ПО, значит НО. Тогда Н – 17.

ЭТО- 16 О 10 Е Т - 19 О 14 0 3 0 Т Ь С Я - С Т 20 0 Н Н 28 16 - НО - Н О 24 Ь Ю - ЗДЕСЬ - ВСЕ - 14 О 25 14 12 - С Е 20 28.

По слову НО 24 ЬЮ получаем, что 24 – Ч.

ЭТО- 16 О 10 Е Т - 19 О 14 0 3 0 Т Ь С Я - С Т 20 0 Н Н 28 16 - НО - НОЧЬЮ - ЗДЕСЬ - ВСЕ - 14 О 25 14 12 - С Е 20 28.

0 также часто встречается, при этом это не О, значит, это – А.

ЭТО- 16 О 10 Е Т - 19 О 14 А З А Т Ь С Я - С Т 20 А Н Н 28 16 - НО - НОЧЬЮ - ЗДЕСЬ - ВСЕ - 14 О 25 14 12 - С Е 20 28

Слово 16 О 10 ЕТ – МОЖЕТ, т. е. М – 16, Ж – 10.

ЭТО- МОЖЕТ - 19 О 14 А З А Т Ь С Я - С Т 20 А Н Н 28 М - НО - НОЧЬЮ - ЗДЕСЬ - ВСЕ - 14 О 25 14 12 - С Е 20 28.

Далее, СТ 20 АНН 28 М – СТРАННЫМ, 19 О 14 А З А Т Ь С Я – ПОКАЗАТЬСЯ, т. е.

ЭТО - МОЖЕТ - ПОКАЗАТЬСЯ - СТРАННЫМ - НО - НОЧЬЮ - ЗДЕСЬ - ВСЕ - 14 О 25 14 12 - СЕРЫ.

Пользуясь тем, что шифрование букв происходит *почти* последовательно (исключение составляют буквы, входящие в ключ). Тогда 25 – Ш, 14 – К.

ЭТО - МОЖЕТ - ПОКАЗАТЬСЯ - СТРАННЫМ - НО - НОЧЬЮ - ЗДЕСЬ - ВСЕ - КОШК 12 - СЕРЫ, значит, 12 – И. Таким образом, искомая фраза:

ЭТО - МОЖЕТ - ПОКАЗАТЬСЯ - СТРАННЫМ - НО - НОЧЬЮ - ЗДЕСЬ - ВСЕ - КОШКИ - СЕРЫ.

Ответ: ЭТО МОЖЕТ ПОКАЗАТЬСЯ СТРАННЫМ НО НОЧЬЮ ЗДЕСЬ ВСЕ КОШКИ СЕРЫ.

Рассмотренные задачи дают, как показывает анализ методов решения задач по криптографии, вполне адекватное представление о методах решения задач по криптографии для школьников старшей школы с применением теории чисел.

АННОТАЦИЯ

В предлагаемой статье представлен обзор некоторых методов теории чисел, применяемых при решении задач олимпиад по математике и криптографии для старших школьников. На примере задач заключительного этапа олимпиады 2018-2019 учебного года, а также задач олимпиад за предыдущие годы (с 2002 г.) приведены варианты решений.

Ключевые слова: криптография, математика, методы чисел, информационная безопасность

SUMMARY

The article provides an overview of some methods of number theory used in solving tasks of Olympiads in mathematics and cryptography for senior students. On the example of the tasks of the final stage of the 2018–2019 academic year, as well as the tasks of the Olympiads for previous years (since 2002), solutions are given.

Key words: cryptography, mathematics, methods of numbers, information security

ЛИТЕРАТУРА

1. Goldreich O. Foundations of cryptography. Volume 1 (Basic tools). Volume 2 (Basic applications). – Cambridge, United Kingdom: Cambridge University Press, 2001. (V. 1); 2004 (V. 2).

2. S. Goldwasser M. Bellare. Lecture notes on cryptography [Электронный ресурс]. – Cambridge, Massachusetts, 2008 URL: http://cseweb.ucsd.edu/users/mihir/papers/gb.pdf.

3. Хирш Е. Курс лекций «Сложностная криптография» [Электронный ресурс]. – URL: https://logic.pdmi.ras.ru/seminars/logic-seminar/2019-05-31.

4. Ященко В. Введение в криптографию. – М.: МЦНМО, 2012. – 348 с.

5. Коблиц Н. Курс теории чисел и криптографии [Электронный ресурс]. – М.: Научное издательство ТВП, 2001. – URL: http://booksshare.net/index.php?id1=4&category=math&author=koblicn&book=2001&page=10.

6. Логачев О, Сальников А, Ященко В. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.

7. Shapiro H. Introduction to the Theory of Numbers. New York: John Wiley & Sons, 1983.

8. Тилборг ван Х. К. А. Основы криптологии: профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с.

9. Варновский Н. Математическая криптография. Несколько этюдов. Московский университет и развитие криптографии в России: материалы конференции в МГУ. Москва, 17–18 октября 2002 г. – М.: МЦНМО, 2003. – С. 98–121.

10. Зубов А. [и др.]. Олимпиады по криптографии и математике для школьников. – М.: МЦНМО, 2019. – 184 с.

11. Олимпиады для школьников [Электронный ресурс]. – URL: http://olympiads.mccme.ru/20072008.htm.

12. Олимпиады для школьников [Электронный ресурс]. – URL: https://v-olymp.ru/cryptolymp/index.php.

13. Олимпиады для школьников [Электронный ресурс]. – URL: https://v-olymp.ru/cryptolymp/preparing_olympics/.

14. Олимпиады для школьников [Электронный ресурс]. – URL: https://v-olymp.ru/cryptolymp/photo_gallery/3240/187455/.

А. С. Петелин, Ф. Чжун, О. Б. Мазкина

УДК 378.01

ДИАГНОСТИКА СФОРМИРОВАННОСТИ НРАВСТВЕННО-ЭСТЕТИЧЕСКОГО САМООПРЕДЕЛЕНИЯ КИТАЙСКИХ СТУДЕНТОВ В МУЗЫКАЛЬНО-ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ РОССИЙСКОГО ВУЗА

Современная востребованность компетентных специалистов в различных странах мира предъявляет особые требования к уровню подготовки обеспечивающей их готовность и способность к выполнению профессиональной деятельности. В российских вузах наравне с русскими студентами более 100 тысяч иностранных студентов ежегодно выбирают учебу в нашей стране, и еще около 50 тысяч – в российских вузах, находящихся за рубежом, и зарубежных филиалах российских вузов [9]. Исходя из этого, динамично развивающиеся контакты российских вузов с ведущими университетами мира, актуализировали перед образовательными организациями, да и всей образовательной системой России необходимость выявления и решения специфических сложностей, особенностей связанных с организацией учебного процесса для иностранных студентов.

Для придания обучению направления, учитывающего специфические особенности нравственного и эстетического самоопределения китайских студентов в культурно-образовательном процессе педагогического вуза, необходимо к образовательной, воспитывающей, развивающей и социализирующей функциям среды вводить культурологическую, эмоционально-эстетическую и нравственную, побуждающих к конструктивному взаимодействию с новой культурно-образовательной средой вуза и ее традициями, не всегда совпадающими с национальными традициями Китая.

Лян Шумин, определяющий современную культуру Китая как симбиоз древних традиций и современных нововведений, подчеркивал, что специфические достоинства китайцев – в их национальном духе. А национальный дух – это мораль и стремление к лучшему [12]. Система норм, канонов, правил поведения в Китае закреплена не в церковных писаниях и законах, она представлена в общепризнанных обрядах, традициях, ритуалах и обычаях, которые формировались на значимых во всем мире таких этических учениях, как конфуцианство и даосизм. Исходя из этого своеобразия, принципиальным, на наш взгляд, является учет самобытного национального менталитета китайских студентов в системе межличностных и межкультурных отношений и связей в культурно-образовательной среде вуза, влияющей на нравственное и эстетическое самоопределение личности.

Самоопределение рассматривается: Л.И. Божович, К. А. Абульханова-Славская, Н. М. Борытко, С. Л. Рубинштейн, Д. И. Фельдштейн, К. Роджерс и др. как процесс и результат сознательного, самостоятельного выбора лич-