ISSN 2542-1468, Лесной вестник / Forestry Bulletin, 2019. Т. 23. № 3. С. 114–120. © МГТУ им. Н.Э. Баумана, 2019

УДК 510.58 DOI: 10.18698/2542-1468-2019-3-114-120

О НЕКОТОРЫХ ВОЗМОЖНОСТЯХ СОПРОВОЖДЕНИЯ ЧТЕНИЯ КЛАССИЧЕСКОГО КУРСА АЛГЕБРЫ РЕАЛЬНЫМИ ПРИЛОЖЕНИЯМИ ИЗ ОБЛАСТИ КРИПТОГРАФИИ (ДЛЯ СТУДЕНТОВ МЛАДШИХ КУРСОВ ТЕХНИЧЕСКИХ УНИВЕРСИТЕТОВ)

Т.А. Ласковая[1], К.К. Рыбников[2], О.К. Чернобровина[3]

[1]МГТУ им. Н.Э. Баумана, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1
[2]ООО «Полиэдр» 107143, Москва, шоссе Открытое, д. 20, стр. 1
[3]МГТУ им. Н.Э. Баумана (Мытищинский филиал), 141005, Московская обл., г. Мытищи, ул. 1-я Институтская, д. 1

talaskovy@mail.ru

Одним из важных аспектов построения программы преподавания традиционных базовых курсов высшей математики для студентов технических университетов является задача сопровождения этих курсов реальными практическими приложениями. Только в этом случае будущие инженеры ощутят прикладную перспективу применения математического аппарата, которым они овладевают в процессе обучения. Эта задача представляется достаточно сложной, так как теоретический багаж студентов младших курсов невелик: основы дифференциального и интегрального исчисления и основные положения линейной алгебры. Авторы предлагают использовать при преподавании курса высшей алгебры в первую очередь примеры из области криптографии, для решения которых, как правило, достаточно материала первого курса (даже первого семестра). Это, например, шифр Лестера Хилла, подстановки и подходы к анализу структуры формальных нейронов.
Ключевые слова: шифр Хилла, подстановка, задача о назначениях

Ссылка для цитирования: Ласковая Т.А., Рыбников К.К., Чернобровина О.К. О некоторых возможностях сопровождения чтения классического курса алгебры реальными приложениями из области криптографии (для студентов младших курсов технических университетов) // Лесной вестник / Forestry Bulletin, 2019. Т. 23. № 3. С. 114–120. DOI: 10.18698/2542-1468-2019-3-114-120

Применение науки составляет особое умение,
гораздо более высокое, чем сама наука.

Фрэнсис Бэкон

Восприятие курсов высшей математики для студентов младших курсов технических университетов иногда оказывается достаточно сложным. И дело не только в трудности изучаемого материала, но и в психологических особенностях студентов. Будущий инженер интуитивно хотел бы с первых месяцев обучения оценить возможности прикладных исследований на основе изучаемого математического аппарата. Если преподаватель строит свой курс на изложении формального математического курса, то это может негативно сказаться на качестве обучения, не говоря уже об интересе обучающихся к дисциплине. Эта объективная опасность подстерегает даже опытного лектора [19, 20], и надо сказать, что проблема, которая в связи с этим встает перед преподавателем, достаточно сложна.

Цель работы

Авторы ставят целью с первых месяцев изучения курса высшей математики предоставить возможность будущим инженерам приступить к анализу реальных прикладных моделей.

Материалы и методы

Используемыми методами являются основные алгоритмы линейной алгебры, методы анализа выпуклых многогранников и исследования некоторых объектов симметрической группы. Весь этот материал доступен для первокурсника.

Среди таких приложений достаточно перспективным направлением является классическая криптография [6–10] в сочетании с самыми простыми сведениями из курса алгебры. Приведем несколько конкретных примеров.

Решение систем линейных уравнений и шифр Хилла. На самом раннем этапе изучения курса линейной алгебры студенты знакомятся с понятием определителя квадратной матрицы, способами построения обратной матрицы, а также с матричным методом решения невырожденной квадратной системы линейных уравнений. Как ни странно, даже эти начальные знания могут быть использованы при математическом анализе одного из шифров.

В 1929 году американский математик Лестер Сандерс Хилл (1890–1961) предложил достаточно простой способ шифрования [1, 2].

Пусть каждой букве латинского алфавита A, B, C, …, Z поставлено в соответствие некоторое целое положительное число 0, 1, 2, …, 25 так, что отображение {A, B, C, …, Z} → {0, 1, 2, …, 25} биективно.

Наиболее простой случай, разумеется, имеет вид (1)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

(1)

Процесс шифрования заключается в следующем. Предположим, что у нас есть n-мерный вектор $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, определяющий шифруемый, или открытый, текст, и квадратная матрица A размером $n \times n$, $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$, которая называется ключом шифрования.

Зашифрованный текст (шифртекст), соответствующий открытому тексту x, определяется как n-мерный вектор b:

$$Ax = b \pmod{26},$$

где

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, \; b_i = \sum_{j=1}^{n} a_{ij} x_j \pmod{26}, i = 1, 2, ..., n.$$

Операции по mod 26 таковы, что вместо чисел берутся их остатки при делении на 26.

Расшифрование, т. е. нахождение x по известному вектору b, определяется соотношением

$$x = A^{-1} b \pmod{26}. \qquad (2)$$

Разумеется, этот процесс возможен только при условии, что у матрицы A существует обратная матрица A^{-1}. В нашем случае это осуществляется при условиях:

1) $det\, A \neq 0$;

2) $det\, A$ не имеет общих делителей с основой модуля (в данном случае это число 26).

Последнее условие соблюдается автоматически, если основа модуля — простое число (например, 29). Это легко может быть достигнуто, если в биективное отображение вида (1) (нумерация букв алфавита может быть выбрана другой) добавить в качестве прообразов некоторые вспомогательные символы (например, пробел, точка, знак вопроса).

Пример по Хиллу

Пусть сообщение (открытый текст) имеет вид

x = ACT (0 2 19).

При выбранном ключе

$$A = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} = \begin{pmatrix} G & Y & B \\ N & Q & K \\ U & R & P \end{pmatrix}$$

шифртекст b определяется так:

$$b = Ax = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26} = \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix}$$

$$\text{или} \quad b = \begin{pmatrix} P \\ O \\ H \end{pmatrix}.$$

Восстановим теперь открытый текст x по шифртексту b, воспользовавшись соотношением (2):

$$x = A^{-1} b = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26} =$$

$$= \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} A \\ C \\ T \end{pmatrix}. \blacksquare$$

Криптоаналитические слабости шифра Хилла достаточно очевидны. Во-первых, это возможность определить матричный ключ A при большом наборе известных пар открытого текста и соответствующего ему шифртекста. Во-вторых, весьма трудно предположить эффективный алгоритм построения прямых и обратных матриц A и A^{-1}, что должно было бы обеспечить построение процедуры выбора и смены ключа.

Можно предположить, что сам автор осознавал слабости своей схемы шифрования. В своих работах он упоминал о возможности многократного применения этой схемы, т. е. построения схемы шифрования с набором ключей A, B_1, B_2, …, B_k:

$$Ax = b, \; B_1 b = \beta^{(1)}, \; B_2 \beta^{(1)} = \beta^{(2)}, \; ..., \; B_k \beta^{(k-1)} = \beta^{(k)}.$$

В то же время известный историк криптографии Дэвид Кан в своей книге «Взломщики кодов» [3] отметил некоторые перспективы развития этого подхода к шифрованию, а также его достоинства. Прежде всего, это был первый опыт так называемого блочного шифрования, т. е. шифрования не позначного, а оперирующего с векторами (словами из букв алфавита).

Хотя сам Хилл ограничился преобразованием трехмерных векторов X, очевидно, что размерность их может быть увеличена. Аппарат же процедуры шифрования полностью соответствует теоретическим сведениям из начального курса классической алгебры.

Именно это вызвало большой интерес у математиков-криптографов, когда в августе 1929 года Лестер Хилл представил свой доклад на съезде Американского математического общества в городе Боулдер (штат Колорадо).

Следует заметить, что все это много позже оценил Дэвид Кан, определив метод шифрования Хилла как «общий и мощный» [3].

Что же требуется студенту для анализа схемы шифрования Хилла? Не так уж много. Достаточно знать теорию решения квадратных систем линейных уравнений над полем действительных чисел и ее модификацию над кольцами вычетов по модулям 26 и 29 [4]. Впрочем, возможен выбор и других оснований модуля.

Решение системы линейных неравенств и анализ структуры соответствующего полиэдра как основа для изучения ряда технических приложений. При изучении теории решения систем линейных уравнений в стороне, как правило, оказывается смежный, естественно возникающий вопрос: как решать систему линейных неравенств?

На самом деле решение систем линейных неравенств может быть сведено к решению систем линейных уравнений путем простого введения дополнительных переменных [15, 17].

Для системы линейных неравенств

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n \le b_i,$$
$$b_i \ge 0 \ \left(i = 1,2,\ldots,m\right), \qquad (3)$$

вводим дополнительные переменные и переходим к рассмотрению системы линейных уравнений

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n + x_{n+i} = b_i$$
$$\left(i = 1,2,\ldots,m\right). \qquad (4)$$

Для полученной системы (4) можно применять методы нахождения ее общего решения, что входит в программу алгебры на первом курсе. Такой подход достаточно хорошо известен [5, с. 139–141].

Целесообразность изучения на первом курсе методов решения систем линейных неравенств обосновывается двумя факторами.

Во-первых, в том случае, если полученная система неравенств задает ограниченный полиэдр, то в дальнейшем для соответствующего выпуклого многогранника можно легко ввести понятие его вершины, что пригодится при обучении, когда студенты будут осваивать симплекс-метод решения задач линейного программирования.

Во-вторых, что касается явных простых технических приложений математических полиэдральных моделей, то это в первую очередь рассмотрение задач анализа структуры комплекса формальных нейронов с линейной функцией активации [12–14], в том числе задач синтеза формальных нейронов (так называемые задачи настройки нейронов [13]).

Кроме того, при минимальных затратах времени можно продемонстрировать студентам, что системы линейных неравенств можно трактовать как математические модели распределения ресурсов [5].

Подстановки как базовый элемент построения узлов криптосхем. Математическая модель выбора подстановки. Подстановкой из n элементов конечного множества $X = \{x_1, x_2, \ldots, x_n\}$ называется биективное отображение этого множества на себя $f : X \to X$.

Общепринятая в математической литературе символическая запись подстановки имеет вид

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ x_1 & x_2 & \ldots & x_i & \ldots & x_n \end{pmatrix}.$$

Каждому из элементов множества X присваивается номер от 1 до n (разумеется, все номера различны), а их образами $x_1, x_2, \ldots, x_n$ являются те же числа, записанные в другом порядке. Случай, когда $i = x_i$ ($i = 1, 2, \ldots, n$), также возможен:

$$1 \to x_1,$$
$$2 \to x_2,$$
$$\ldots\ldots\ldots$$
$$i \to x_i,$$
$$\ldots\ldots\ldots$$
$$n \to x_n,$$

и называется тождественной подстановкой.

Тождественная подстановка имеет вид

$$\begin{pmatrix} 1 & 2 \ldots & i & \ldots & n \\ 1 & 2 \ldots & i \ldots & & n \end{pmatrix}.$$

На множестве подстановок из n элементов можно определить бинарную операцию умножения:

$$A = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ x_1 & x_2 & \ldots & x_i & \ldots & x_n \end{pmatrix}, \ B = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \end{pmatrix};$$

$A \times B$ определяется как отображение $i \to x_i \to y_i$ ($i = 1, 2, \ldots, n$).

Пример

Пусть

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Тогда

$$P \cdot Q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \; Q \cdot P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}. \; \blacksquare$$

Операция умножения является не коммутативной, но ассоциативной. Множество подстановок, очевидно, образует группу. Для каждого элемента существует обратный, а в качестве единицы принимается тождественная подстановка.

Именно подстановки являются наиболее старым и известным способом шифрования. Еще в I веке до нашей эры Гай Юлий Цезарь применял подобный шифр. Схема такого шифрования описывается как подстановка

$$\begin{pmatrix} 1 & 2 & 3 & ... & 33 \\ 4 & 5 & 6 & ... & 3 \end{pmatrix}$$

применительно к русскому алфавиту. Это отображение

$$i \to (x + 3) \pmod{33}, \; i = 1, 2, \ldots, 33.$$

Юлий Цезарь использовал подстановку, использующую сдвиг букв алфавита на 3 позиции. Разумеется, сдвиг может быть осуществлен на любое число позиций в пределах мощности алфавита [9]. Сдвиг может быть переменным и использоваться как ключевая система [10].

В работе [5] приводятся примеры из литературы, оживляющие изложение этого раздела для студентов: В.А. Каверин «Исполнение желаний» — студент Николай Трубачевский расшифровывает десятую главу «Евгения Онегина» А.С. Пушкина; А.Н. Толстой «Петр Первый» — разбойники общаются на секретном языке «Тарабарщина»; А.Н. Рыбаков «Кортик» — директор школы Алексей Иванович расшифровывает мудрую литорею (древнерусский шифр), с помощью которой в ножнах и кортике записывается фраза «Сим гадом завести часы»; упоминаются также рассказы Эдгара По «Золотой жук» и А. Конан Дойля «Пляшущие человечки». В последних двух рассказах герои, занимающиеся расшифровкой тайнописи, учитывают статистические характеристики открытых текстов и соответствующих им шифртекстов.

Подстановки часто используются в качестве узлов современных криптосхем. При этом основное требование к подстановке — «хорошее перемешивание» знаков входа (первой строки подстановки) при отображении. Это позволяет защитить криптосхему от попыток использовать статистические (частотные) характеристики открытого текста. Одно из таких требований для подстановки

$$X = \begin{pmatrix} 1 & 2 & ... & i & ... & j & ... & n \\ x_1 & x_2 & ... & x_i & ... & x_j & ... & x_n \end{pmatrix}$$ —

добиться возможно меньшего числа пар (прообраз — образ)

$$\begin{pmatrix} i \\ x_i \end{pmatrix}, \begin{pmatrix} j \\ x_j \end{pmatrix} \quad (i \to x_i, \; j \to x_j),$$

удовлетворяющих условию

$$(x_i - i) \pmod{n} = (x_j - j) \pmod{n}.$$

Кстати, с точки зрения этого требования подстановка шифра Гай Юлия Цезаря является очень слабой.

В работе [11] предлагается математическая модель выбора подстановки, удовлетворяющей вышеуказанному требованию.

Для этой модели предлагается построить матрицу $C = \left\| c_{ijkl} \right\|$ размером $n^2 \times n^2$, где

$$c_{ijkl} = \begin{cases} 1, \text{ если выполняется условие} \\ \quad (i \to j), (k \to l), (j - i) \pmod{n} = \\ \quad = (l - k) \pmod{n}, \\ 0, \text{ в противном случае.} \end{cases}$$

Требуется решить квадратичную задачу о назначениях

$$\sum_{i,j,k,l=1}^{n} c_{ijkl} x_{ij} x_{kl} \to \min \qquad (5)$$

при условиях:

$$\sum_{i=1}^{n} x_{ij} = 1, \quad j = 1, 2, ..., n; \qquad (6)$$

$$\sum_{j=1}^{n} x_{ij} = 1, \quad i = 1, 2, ..., n; \qquad (7)$$

$$x_{ij} = 0 \text{ или } 1, \; i = 1, 2, \ldots, n; \; j = 1, 2, \ldots, n. \qquad (8)$$

Решение задачи (5)–(8) достаточно трудоемко при относительно больших значениях n. Однако возможно решать задачу приближенно, применяя схему метода ветвей и границ, где нижние оценки для ветвей могут быть получены с помощью решения линейных задач о назначениях при выборе для ветви фиксированного набора назначений вида $i \to j$ [11, 16]. Для линейных задач условие (8) может быть заменено на $x_{ij} \geq 0$.

Остается заметить, что подстановка определяется при решении задачи (5)–(8) как подстановочная матрица

$$X = \begin{pmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ . & . & . & . \\ x_{n1} & x_{n2} & ... & x_{nn} \end{pmatrix},$$

элементы которой принимают значения 0 и 1 при условиях (6), (7), т. е. в каждой строке и в каждом столбце такой матрицы находится только одна единица (остальные элементы нулевые).

При изучении множества подстановок студенту не требуется дополнительных специальных

знаний. Понятие подстановки, операция умножения — этого достаточно, чтобы решать подстановочные уравнения и проводить первичный анализ подстановочных узлов криптосхем. Все это доступно первокурснику. Впоследствии на старших курсах по алгебраическим дисциплинам студентам предстоит познакомиться с симметрической группой (группой подстановок), изучить линейное программирование и дискретную математику.

Выводы

Рассмотренные авторами модели являются полезными приложениями прикладной части курса высшей математики и обеспечены необходимым математическим аппаратом. Этот материал расширяет представление о перспективах работы выпускника высшего учебного заведения.

Список литературы

[1] Lester Hill. Cryptography in an Algebraic Alphabet // The American Mathematical Monthly, v. 36, June-July, 1929, pp. 306–312.

[2] Lester Hill. Concerning Certain Linear Transformation Apparatus of Cryptography // The American Mathematical Monthly, 1931, v. 37, March, pp. 135–154.

[3] David Kahn. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York: Scribner, 1966, pp. 405–723.

[4] Ласковая Т.А., Рыбников К.К., Чернобровина О.К., Чернышова А.Г. Об истории развития основных математических принципов криптографии и их иллюстративном значении при преподавании математических дисциплин // Труды XII Международных Колмагоровских чтений. Ярославль: РИО ЯГПУ, 2015. С. 296–400. 459 с.

[5] Рыбников К.К. Введение в дискретную математику и теорию решения экстремальных задач на конечных множествах. М.: Гелиос АРВ, 2010, 320 с.

[6] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. С. 115–119. 481 с.

[7] Гомес Ж. Математики, шпионы и хакеры. Кодирование и криптография. М.: Де Агостини,2014. 144 с.

[8] Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002. 512 с.

[9] Черчхауз Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. М.: Весь мир, 2007. 263 с.

[10] Земор Ж. Курс криптографии. Ижевск: НИЦ «Регулярная и хаотическая динамика», ИКИ, 2006. 256 с.

[11] Рыбников К.К. Прикладные аспекты использования одного приближенного метода решения квадратичной задачи о назначениях // Обозрение прикладной и промышленной математики, 2004. Т. 11. Вып. 3. С. 582–583.

[12] Никонов В.Г., Рыбников К.К. Применение полиэдральных методов в прикладных математических задачах, сводящихся к анализу и решению систем линейных неравенств // Вестник МГУЛ–Лесной Вестник, 2003. № 1(26). С. 81–85.

[13] Рыбников К.К. Приближенные методы настройки формального нейрона для решения задачи распознавания двух векторных массивов // Обозрение прикладной и промышленной математики, 2009. Т. 16. Вып. 2. С. 380–382.

[14] Ласковая Т.А., Рыбников К.К., Чернобровина О.К. О реализации универсальных двоичных узлов преобразования в электронных схемах комплексом формальных нейронов // Обозрение прикладной и промышленной математики, 2011. Т. 18. Вып. 2. С. 295–297.

[15] Ласковая Т.А., Рыбников К.К., Чернобровина О.К. История развития методов анализа полиэдральных математических моделей // Труды X Международных Колмогоровских чтений. Ярославль: ЯГПУ, 2012. С. 188–191.

[16] Кирилина Т.Ю., Рыбников К.К., Чернышова А.Г. Задачи о назначениях как математические модели принятия управленческих решений и определения оценок рейтинга в социологических исследованиях рабочих коллективов // X Ковалевские чтения «Россия в современном мире: взгляд социолога»: материалы научно-практической конференции. Санкт-Петербург, Санкт-Петербургский государственный университет, 13–15 ноября 2015 г. / Отв. ред. Ю.В. Асочаков. СПб.: Скифия-принт, 2015. С. 42–48.

[17] Рыбников К.К., Ласковая Т.А. К истории развития теории решения систем линейных неравенств в XIX веке // Современная математика и математическое образование, проблемы истории и философии математики: материалы Межд. научная конференции, Тамбов, ТГУ им. Г.Р.Державина, 22.04–25.04 2008 г. Тамбов: ТГУ. С. 155–157.

[18] Рыбников К.К., Чернобровина О.К. Математическая подготовка инженеров космической отрасли на базе Московского лесотехнического института. Страницы истории (к 50-летию отечественной пилотируемой космонавтики) // Труды IX Международных Колмогоровских чтений. Ярославль: ЯГПУ, 2011. С. 309–311.

[19] Рыбников К.К., Чернобровина О.К. О некоторых принципах построения учебного курса «Дискретная математика» для студентов инженерных специальностей // Труды IX Международных Колмогоровских чтений. Ярославль: ЯГПУ, 2011. С. 311–313.

[20] Рыбников К.К. Элементы численного дискретного анализа в подготовке преподавателей математики. Связь непрерывного и дискретного // Гуманитаризация среднего и высшего математического образования: методология, теории и практика: материалы Всероссийской научной конференции. Ч. 2. Саранск: МГПИ, 2002. С. 132–135.

Сведения об авторах

Ласковая Татьяна Алексеевна — старший преподаватель кафедры математического моделирования МГТУ им. Н.Э. Баумана, talaskovy@mail.ru

Рыбников Константин Константинович — канд. физ.-мат. наук, доцент, директор ООО «Полиэдр», kkrybnikov@mail.ru

Чернобровина Ольга Константиновна — старший преподаватель кафедры информационно-измерительных систем и технологии приборостроения МГТУ им. Н.Э. Баумана (Мытищинский филиал), olga@mgul.ac.ru

Поступила в редакцию 21.12.2018.
Принята к публикации 25.04.2019.

ON SOME POSSIBILITIES OF SUPPORTING THE READING OF THE CLASSICAL COURSE OF ALGEBRA WITH REAL APPLICATIONS IN THE FIELD OF CRYPTOGRAPHY FOR STUDENTS OF JUNIOR COURSES OF TECHNICAL UNIVERSITIES

T.A. Laskovaya[1], K.K. Rybnikov[2], O.K. Chernobrovina[3]

[1]BMSTU, 5, Block 1, 2nd Baumanskaya st., 105005, Moscow, Russia
[2]«POLYEDR», Open Highway, 20, Moscow, 107143, Russia
[3]BMSTU (Mytishchi branch), 1, 1st Institutskaya st., 141005, Mytishchi, Moscow reg., Russia

talaskovy@mail.ru

One of the important aspects of the program of teaching traditional basic courses of higher mathematics for students of technical universities is the task of supporting these courses with real practical applications. Only in this case, future engineers will feel the applied perspective of the mathematical apparatus, which they master in the learning process. This task is quite difficult as the theoretical background of junior students is very poor. The authors propose to use in teaching the course of higher algebra in the first place examples from the field of cryptography, for which, as a rule, enough material of the first course (and even the first semester!). These are, for example, Leicester hill cipher, substitutions and approaches to the analysis of the structure of formal neurons.
Keywords: the hill cipher, substitution, assignment problem

Suggested citation: Laskovaya T.A., Rybnikov K.K., Chernobrovina O.K. *O nekotorykh vozmozhnostyakh soprovozhdeniya chteniya klassicheskogo kursa algebry real'nymi prilozheniyami iz oblasti kriptografii dlya studentov mladshikh kursov tekhnicheskikh universitetov* [On some possibilities of supporting the reading of the classical course of algebra with real applications in the field of cryptography for students of junior courses of technical universities]. Lesnoy vestnik / Forestry Bulletin, 2019, vol. 23, no. 3, pp. 114–120. DOI: 10.18698/2542-1468-2019-3-114-120

References

[1] Lester Hill. Cryptography in an Algebraic Alphabet // The American Mathematical Monthly, v. 36, June-July, 1929, pp. 306–312.
[2] Lester Hill. Concerning Certain Linear Transformation Apparatus of Cryptography // The American Mathematical Monthly, 1931, v. 37, March, pp. 135–154.
[3] David Kahn. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York: Scribner, 1966, pp. 405–723.
[4] Laskovaya T.A., Rybnikov K.K., Chernobrovina O.K., Chernyshova A.G. *Ob istorii razvitiya osnovnykh matematicheskikh printsipov kriptografii i ikh illyustrativnom znachenii pri prepodavanii matematicheskikh distsiplin* [The story of the development of the basic mathematical principles of cryptography and their illustrative value in teaching mathematical disciplines]. Trudy XII Mezhdunarodnykh Kolmagorovskikh chteniy [Proceedings of the XII International Kolmogorovsky readings]. Yaroslavl: RIO YGPU, 2015, pp. 296–400. 459 p.
[5] Rybnikov K.K. *Vvedenie v diskretnuyu matematiku i teoriyu resheniya ekstremal'nykh zadach na konechnykh mnozhestvakh* [Introduction to discrete mathematics and theory for solving extremal problems on finite sets]. Moscow: Gelios ARV, 2010, 320 p.
[6] Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V. *Osnovy kriptografii* [Fundamentals of cryptography], 2nd ed. Moscow: Gelios ARV, 2002, pp. 115–119, 481 p.
[7] Gomes Zh. *Matematiki, shpiony i khakery. Kodirovanie i kriptografiya* [Maths, spies and hackers. Encryption and cryptography]. Moscow: De Agostini, 144 p.
[8] Babash A.V., Shankin G.P. *Kriptografiya* [Cryptography]. Moscow: SOLON-R, 2002, 512 p.
[9] Cherchkhauz R. *Kody i shifry. Yuliy Tsezar', «Enigma» i Internet* [Codes and ciphers. Julius Caesar, Enigma and the Internet]. M .: Ves' mir, 2005, 263 p.
[10] Zemor Zh. *Kurs kriptografii* [Cryptography course]. Izhevsk: NITs «Regulyarnaya i khaoticheskaya dinamika», IKI, 2006, 256 p.
[11] Rybnikov K.K. *Prikladnye aspekty ispol'zovaniya odnogo priblizhennogo metoda resheniya kvadratichnoy zadachi o naznacheniyakh* [Applied aspects of using one approximate method for solving a quadratic assignment problem] Obozrenie prikladnoy i promyshlennoy matematiki [Review of applied and industrial mathematics], 2004, t. 11, v. 3, pp. 582–583.
[12] Nikonov V.G., Rybnikov K.K. *Primenenie poliedral'nykh metodov v prikladnykh matematicheskikh zadachakh, svodyashchikhsya k analizu i resheniyu sistem lineynykh neravenstv* [Application of polyhedral methods in applied mathematical problems, which are reduced to the analysis and solution of systems of linear inequalities]. Moscow state forest university bulletin – Lesnoy vestnik, 2003, no. 1 (26), pp. 81–85.
[13] Rybnikov K.K. *Priblizhennye metody nastroyki formal'nogo neyrona dlya resheniya zadachi raspoznavaniya dvukh vektornykh massivov* [Approximate methods for setting up a formal neuron for solving the problem of recognizing two vector arrays]. Obozrenie prikladnoy i promyshlennoy matematiki [Review of applied and industrial mathematics], 2009, t. 16, v. 2, pp. 380–382.
[14] Laskovaya T.A., Rybnikov K.K., Chernobrovina O.K. *O realizatsii universal'nykh dvoichnykh uzlov preobrazovaniya v elektronnykh skhemakh kompleksom formal'nykh neyronov* [On the implementation of universal binary transformation nodes in electronic circuits by a complex of formal neurons]. Obozrenie prikladnoy i promyshlennoy matematiki [Review of applied and industrial mathematics], 2011, t. 18, v. 2, pp. 295–297.
[15] Laskovaya T.A., Rybnikov K.K., Chernobrovina O.K. *Istoriya razvitiya metodov analiza poliedral'nykh matematicheskikh modeley* [History of development of methods of analysis of polyhedral mathematical models] [Proceedings of the X International Kolmogorov readings: Collection of articles]. Yaroslavl: YAGPU, 2012, p. 188–191.

[16] Kirilina T.Yu., Rybnikov K.K., Chernyshova A.G. *Zadachi o naznacheniyakh kak matematicheskie modeli prinyatiya upravlencheskikh resheniy i opredeleniya otsenok reytinga v sotsiologicheskikh issledovaniyakh rabochikh kollektivov* [The problem of assignments as a mathematical model in managerial decisions and determine ranking in sociological studies of work teams]. X Kovalevskie chteniya «Rossiya v sovremennom mire: vzglyad sotsiologa»: materialy nauchno-prakticheskoy konferentsii [The Tenth Kovalevskie reading. Materials of scientific-practical conference]. Sankt-Peterburg, Sankt-Peterburgskiy gosudarstvennyy universitet, November 13–15, 2015. Ed. Yu.V. Asochakov. Sankt-Peterburg: Skifiya-print, 2015, 248 p.

[17] Rybnikov K.K., Laskovaya T.A. *K istorii razvitiya teorii resheniya sistem lineynykh neravenstv v XIX veke* [The history of the theory of solving systems of linear inequalities in the XIX century]. Sovremennaya matematika i matematicheskoe obrazovanie, problemy istorii i filosofii matematiki [Modern mathematics and mathematical education, problems of history and philosophy of mathematics] Inter. scientific conference, Tambov, TSU them. G. R. Derzhavina, 22.04–25.04 2008), p. 155–157.

[18] Rybnikov K.K., Chernobrovina O.K. *Matematicheskaya podgotovka inzhenerov kosmicheskoy otrasli na baze Moskovskogo lesotekhnicheskogo instituta. Stranitsy istorii (k 50-letiyu otechestvennoy pilotiruemoy kosmonavtiki)* [Mathematical training of engineers of space branch on the basis of the Moscow forest engineering Institute. Pages of history (to the 50th anniversary of the national manned cosmonautics)]. Trudy IX Mezhdunarodnykh Kolmogorovskikh chteniy [Proceedings of IX International Kolmogorov readings: Collection of articles]. Yaroslavl: YAGPU, 2011, pp. 309–311.

[19] Rybnikov K.K., Chernobrovina O.K. *O nekotorykh printsipakh postroeniya uchebnogo kursa «Diskretnaya matematika» dlya studentov inzhenernykh spetsial'nostey* [About some principles of construction of a training course «Discrete mathematics» for students of engineering specialties]. Trudy IX Mezhdunarodnykh Kolmogorovskikh chteniy [Proceedings of IX International Kolmogorov readings: Collection of articles]. Yaroslavl: AGPU, 2011, pp. 311–313.

[20] Rybnikov K.K. *Elementy chislennogo diskretnogo analiza v podgotovke prepodavateley matematiki. Svyaz' nepreryvnogo i diskretnogo* [Elements of numerical discrete analysis in the training of teachers of mathematics. Communication of continuous and discrete] Gumanitarizatsiya srednego i vysshego matematicheskogo obrazovaniya: metodologiya, teorii i praktika: materialy Vserossiyskoy nauchnoy konferentsii [Proceedings of the all-Russian scientific conference «Humanitarization of secondary and higher mathematical education: methodology, theory and practice»], P. 2. Saransk: MGPI, 2002, pp. 132–135.

Authors' information

Laskovaya Tat'yana Alekseevna — Senior Lecturer at the Department of Mathematical Modeling of the BMSTU, talaskovy@mail.ru

Rybnikov Konstantin Konstantinovich — Cand. Sci. (Phys.-Mat.), Associate Professor, Director of Polyedr, kkrybnikov@mail.ru

Chernobrovina Ol'ga Konstantinovna — Senior Lecturer at the Department of Information Measuring Systems and Instrument Engineering Technologies of the BMSTU (Mytishchi branch), olga@mgul.ac.ru

Received 21.12.2018.
Accepted for publication 25.04.2019.