УДК 003.26

**А. А. Черняк,** *профессор кафедры математики и методики преподавания математики Белорусского государственного педагогического университета имени Максима Танка, доктор физико-математических наук;*
**Ж. А. Черняк,** *доцент кафедры математики и физики Белорусской государственной академии связи, кандидат физико-математических наук;*
**С. А. Богданович,** *доцент кафедры математики и методики преподавания математики Белорусского государственного педагогического университета имени Максима Танка, кандидат физико-математических наук*

# КРИПТОГРАФИЯ В СРЕДНЕЙ ШКОЛЕ

mailto:bosead@mail.ru

**Аннотация.** Описывается учебное пособие по криптографии для средней школы. Отличительные особенности данного пособия: каждый раздел начинается с изложения собственно идей криптографии, которые затем подкрепляются соответствующим математическим инструментарием, адаптированным для восприятия школьниками старших классов.

**Ключевые слова:** криптография, высшая алгебра в средней школе.

**Abstract.** It is described the new textbook on cryptography for secondary schools. Its features are: each chapter starts with explanations and description of cryptographical ideas and methods which are followed by necessary mathematical tools adapted to the level of secondary school students.

**Keywords:** cryptography, higher algebra in secondary school.

В последние десятилетия во всем мире криптография получила интенсивное развитие не только как прикладная, но и как фундаментальная наука, лежащая в основе научно-технических методов обеспечения безопасности государственных, экономических и военных информационных ресурсов [1–3]. В настоящее время перед системой образования встаёт новая проблема — подготовить подрастающее поколение к жизни и профессиональной деятельности в новой, высокоразвитой информационной среде, эффективному использованию её возможностей и защите электронных информационных ресурсов от негативных воздействий сторонних пользователей. В связи с этим наряду с изучением аппаратных основ защиты информации необходимым условием формирования у учащихся компетентности в области защиты информации является изучение методов и алгоритмов криптографии на всех этапах школьного образования [4].

Нами разработано оригинальное учебное пособие для обучения основам криптографии на факультативных занятиях в средней школе.

Основные цели, которые ставили перед собой авторы, следующие:

1. Изложить идеи шифрования, доступные школьникам старших классов: от шифров Юлия Цезаря до современной системы RSA, применяемой в интернете.

2. Погрузить школьника в удивительный мир модульной арифметики — раздела теории чисел, используемого в классической и современной криптографии.

3. Попутно привить навыки доказывать математические утверждения, необходимые для понимания излагаемых идей криптографии.

4. Облегчить работу учителя при организации самостоятельной контролируемой работы и проверки домашних заданий, сопроводив каждый раздел компьютерной программой для шифрования и дешифрования примеров. Программы имеют очень простой дизайн, могут запускаться с любого компьютера и требуют минимум памяти на внешнем носителе.

Отличительные особенности пособия:

1. Изложение непосредственно начинается с идей шифрования (дешифрования) и постепенно втягивает в орбиту обсуждения математические аспекты по мере необходимости. Это позволяет избежать перегруженности математическими выкладками и затуманивания прикладных идей.

2. Все математические аспекты обосновываются и строго доказываются в максимально доступной форме.

3. Наличие сопутствующих компьютерных программ не только интенсифицирует процесс обучения, но и делает его более привлекательным для современного школьника, привыкшего повсеместно использовать компьютер в своей повседневной жизни.

Ниже представлены два фрагмента пособия в сокращённой форме.

## Фрагмент 1. Аффинный шифр

Пусть $A$ — алфавит для открытого текста и шифртекста, $Z_n$ — конечное кольцо целых чисел по модулю $n$, $|A| = n$. Выбираем произвольное биективное отображение $p\colon A \to Z_n$, которое алфавит из букв превращает в алфавит открытого текста из чисел. Система шифрования задаётся подстановкой $f\colon Z_n \to Z_n$, при которой

$$f(x) = ax + b,$$

где $a$, $b \in Z_n$ и $a$ взаимно просто с $n$. Ключом шифрования является пара чисел $(a, b)$ кольца $Z_n$. Поэтому пространство ключей в этом случае состоит всего из $\varphi(n)$ $n$ ключей, которое можно найти исчерпывающим перебором. Так как

$$f^{-1}(y) = a^{-1}y - a^{-1}b = x,$$

то пару $a^{-1}$, $-a^{-1}b$ можно считать ключом дешифрования.

**Пример.** Пусть $A$ — 26-буквенный английский алфавит, и отображение $p\colon A \to Z_{26}$ задано таблицей

| $x$ | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| $p$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| $x$ | J | K | L | M | N | O | P | Q | R |
| $p$ | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| $x$ | S | T | U | V | W | X | Y | Z | |
| $p$ | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | |

Используя отображение $f\colon Z_{26} \to Z_{26}$, при котором

$$f(x) = 7x + 4,$$

зашифруем открытый текст ALGEBRA:

| Открытый текст | A | L | G | E | B | R | A |
|---|---|---|---|---|---|---|---|
| $x$ | 1 | 12 | 7 | 5 | 2 | 18 | 1 |
| $res_{26}(7x+4)$ | 11 | 10 | 1 | 13 | 18 | 0 | 11 |
| Шифртекст | K | J | A | M | R | Z | K |

Расшифруем шифртекст AMEQMNZW с помощью обратного отображения $f^{-1}$. Так как в кольце

$$Z_{26}\ 7^{-1} = 15,$$

$$res_{26}(-15 \cdot 4) = 18,$$

то

| Шифртекст | A | M | E | Q | M | N | Z | W |
|---|---|---|---|---|---|---|---|---|
| $y$ | 1 | 13 | 5 | 17 | 13 | 14 | 0 | 23 |
| $res_{26}(15y+18)$ | 7 | 5 | 15 | 13 | 5 | 20 | 18 | 25 |
| Открытый текст | G | E | O | M | E | T | R | Y |

## Фрагмент 2. Криптосистемы с открытым ключом

Во всех рассмотренных ранее криптосистемах знание ключа шифрования

$$K_E = (k_1, \ldots, k_s),$$

задающего алгоритм шифрования $f_{k_1 \ldots k_s}$ на множестве $A$ (т. е. инъективное отображение $f_{k_1 \ldots k_s} : A \to B$), позволяло для каждого $x \in A$ не только алгоритмически эффективно определять шифртекст

$$y = f_{k_1 \ldots k_s}(x),$$

но и алгоритмически эффективно осуществлять обратную процедуру дешифрования — превращение шифртекста $y \in B$ в оригинальный открытый текст

$$x = f^{-1}_{k_1 \ldots k_s}(y).$$

Все подобные криптосистемы называются криптосистемами с открытым ключом.

В 1976 г. был открыт принципиально новый тип криптосистем «с открытым ключом». В таких системах знание ключа шифрования $K_E$ недостаточно для нахождения эффективной процедуры дешифрования, которая становится доступной только при наличии дополнительной информации, называемой ключом дешифрования $K_D$.

**Определение.** Пусть ключ шифрования $K_E$ задаёт алгоритм шифрования $f_{K_E} : A \to B$. Тогда $f_{K_E}$ называется функцией с замком, если:

а) для каждого $x \in A$ значение

$$y = f_{K_E}(x)$$

вычисляется за время, ограниченное многочленом от длины $x$;

б) вычисление значений обратной функции $f^{-1}_{K_E}$ является алгоритмически трудноразрешимой задачей;

в) существует ключ дешифрования $K_D$, с помощью которого для каждого $y \in B$ можно найти

$$x = f^{-1}_{K_E}(y)$$

за время, ограниченное многочленом от длины $y$.

Таким образом, функция с замком $f_{K_E}$ — это легковычислимая функция, для которой обратную функцию $f^{-1}_{K_E}$ вычислить чрезвычайно трудно, если не иметь некоторой дополнительной информации сверх той, что используется при вычислении $f_{K_E}$. Однако обратная функция $f^{-1}_{K_E}$ становится легко вычислимой, если доступна дополнительная информация — ключ дешифрования $K_D$.

Определение функции с замком использует эмпирическое понятие «алгоритмической трудноразрешимости», правомерность которого определяется сегодняшним развитием теории алгоритмов и быстродействием вычислительной техники. (Насколько это справедливо — мы увидим ниже на примере рюкзачной криптосистемы.) Даже обосновав алгоритмическую трудноразрешимость задачи вычисления $f^{-1}_{K_E}$, нельзя гарантировать, что функция $f_{K_E}$ со временем не утратит этот статус. Строгое доказательство алгоритмической трудноразрешимости означало бы наличие теоремы, гарантирующей отсутствие эффективного алгоритма дешифрования без ключа $K_D$. При этом следовало бы допускать возможность

использования большого числа соответствующих друг другу элементов открытого и шифрованного текстов (как это делалось при частотном анализе), поскольку по определению системы с открытым ключом кто угодно может вырабатывать произвольно большое число таких пар. К сожалению, подобной теоремы не было доказано ни для одной из криптосистем, заслуживающих сегодня звания «системы с открытым ключом».

Рассмотрим общие принципы применения систем с открытым ключом. Пусть имеется группа пользователей, каждый из которых хочет иметь возможность принимать и дешифровать конфиденциальные сообщения от любого другого пользователя без участия третьих лиц. Некий центральный узел может собрать ключи шифрования всех пользователей и опубликовать их в справочнике. Пользователь Боб, желающий послать сообщение пользователю Анфисе, шифрует своё послание с помощью ключа шифрования $K_{E\,A}$ Анфисы. И только Анфиса имеет в своём распоряжении ключ дешифрования $K_{D.A}$, с помощью которого она дешифрует посланный ей шифртекст.

Заметим, что криптосистемы с открытым ключом, в отличие от классических криптосистем, позволяют большой группе пользователей начать секретный обмен данными без предварительного контакта, взаимной проверки и постоянного обновления ключей.

Криптосистема с открытым ключом используется при идентификации цифровой подписи. Пусть Анфиса и Боб используют функции с замком $f_A$ и $f_B$. Когда Анфиса посылает сообщение Бобу, она шифрует его с помощью алгоритма $f_B$. При получении этого сообщения Боб дешифрует его с помощью известного только ему алгоритма $f_B^{-1}$. Но как Боб может быть уверен, что это послание действительно от Алисы или Анфисы? Ведь ввиду открытости ключа к алгоритму $f_B$ любой злоумышленник может сымитировать послание от Анфисы.

Решение этой проблемы кроется в цифровой подписи. Пусть $m$ — открытый текст, используемый Анфисой в качестве подписи. Она использует свой секретный ключ к алгоритму $f_A^{-1}$ для получения цифровой подписи

$$s = f_A^{-1}(m).$$

При отправлении послания Бобу, Анфиса присоединяет свою цифровую подпись к основному открытому тексту и шифрует весь текст, включая $s$, с помощью алгоритма $f_B^{-1}$. Боб, получив шифртекст, дешифрует его с помощью алгоритма $f_B^{-1}$ и находит в нём цифровую подпись Анфисы

$$s = f_A^{-1}(m).$$

Используя затем открытый ключ к алгоритму $f_A$, Боб находит

$$f_A(s) = f_A(f_A^{-1}(m)) = m$$

и удостоверяется, что послание действительно пришло от Анфисы, поскольку секретный ключ к алгоритму $f_A^{-1}$ известен только ей, и никто другой не может подделать цифровую подпись

$$s = f_A^{-1}(m).$$

Криптосистемы с открытым ключом работают медленнее классических. Однако если группа пользователей предпочитает традиционные криптосистемы, то она может воспользоваться криптосистемой с открытым ключом для рассылки секретных ключей. Таким образом, работая в классических криптосистемах, можно периодически обновлять ключи при помощи более медленной системы с открытым ключом.

Теперь опишем так называемую рюкзачную криптосистему с открытым ключом. Пусть имеется рюкзак объёмом $V$, с которым надо идти в поход. Имеется также $m$ предметов объёмами

$$b_i \in \mathbf{N}\ (1 \le i \le m),$$

которые можно положить в рюкзак. Предположим, что опытный упаковщик рюкзаков

может заполнить его, не оставляя свободного места. Чтобы максимально использовать объём рюкзака, необходимо определить совокупность предметов, которая полностью бы его заполнила. Другими словами, если обозначить

$$K = \{b_1, \ldots, b_m\},$$

то требуется найти такое подмножество $S \subset K$ (если оно существует), чтобы сумма всех элементов из $S$ равнялась $V$. Отметим, что $S$ — элемент степенного множества $\mathbf{P}(K)$ ($\mathbf{P}(K)$ — множество всех подмножеств), порядок которого равен $2^m$. Поэтому исчерпывающий перебор всех подмножеств множества $K$ приводит к экспоненциальному алгоритму. Более того, эта задача, хотя и является частным случаем оптимизационной задачи о рюкзаке, однако остаётся алгоритмически трудноразрешимой. Но при некоторых дополнительных ограничениях на множество $K$ эту задачу можно решить за полиномиальное время.

Множество натуральных чисел

$$K = \{b_1, \ldots, b_m\}$$

называется быстрорастущим, если

$$b_{i+1} > b_1 + \ldots + b_i$$

для всех $i = 1, \ldots, m-1$.

Заметим, что любое подмножество быстрорастущего множества также является быстрорастущим.

**Теорема 1 [5]** (*о быстрорастущих наборах чисел*). Пусть множество натуральных чисел

$$K = \{b_1, \ldots, b_m\}$$

является быстрорастущим. Тогда для любого натурального числа $V$ за время $O(m \log_2 V)$ можно либо найти подмножество $S \subset K$, сумма всех элементов которого равна $V$ (и такое подмножество единственное), либо установить отсутствие таких подмножеств.

**Доказательство.**

Если $V < b_1$ или

$$V > b_1 + \ldots + b_m,$$

то очевидно, что в $K$ нет подмножеств, сумма всех элементов которых была бы равна $V$. Предположим, что

$$b_1 < V < b_1 + \ldots + b_m.$$

Среди чисел множества $K$ выберем наибольшее такое $b_s$, которое не превосходит $V$.

Предположим теперь, что существует такое подмножество $S \subset K$, сумма всех элементов которого равна $V$. Тогда, во-первых, $S$ не содержит

$$b_{s+1}, \ldots, b_m,$$

поскольку каждое из этих чисел превосходит $S$. Во-вторых, множество $S$ обязано содержать $b_s$, поскольку даже сумма

$$b_1 + \ldots + b_{s-1}$$

меньше $V$.

Положим

$$V' = V - b_s, \quad K' = \{b_1, \ldots, b_{s-1}\}.$$

Задача, таким образом, однозначно сводится к поиску такого подмножества $S' \subset K'$, сумма всех элементов которого равна $V'$.

Продолжая этот процесс, менее чем за $m$ шагов либо найдём искомое множество $S$, либо установим его отсутствие. При этом временная сложность алгоритма равна $O(m \log_2 V)$, поскольку на каждом шаге требуется выполнить всего $O(\log_2 V)$ битовых операций.

Построим теперь с помощью быстрорастущего множества функцию с замком $f_{K_E}$.

Какой-нибудь случайной процедурой генерируем натуральные числа $r_1, \ldots, r_{m+1}$ и полагаем

$$b_1 = r_1, \; b_2 = b_1 + r_2, \; \ldots, \; b_m = b_1 + \ldots + b_{m-1} + r_m.$$

Получаем быстрорастущее множество

$$\{b_1, \dots, b_m\}.$$

Затем полагаем

$$q = b_1 + \dots + b_{m-1} + b_m + r_{m+1}$$

и случайной процедурой выбираем число $k$, не превосходящее $q$ и взаимно простое с ним. В кольце $\mathbf{Z}_q$ находим элементы $a_i = kb_i$, $i = 1, \dots, m$.

Обозначим множество всех упорядоченных наборов из $m$ чисел кольца $Z_2$ через $Z_2^m$ (напомним, что $Z_2 = \{0; 1\}$ и сложение и умножение в $Z_2$ осуществляется по модулю 2). Зададим функцию $f_{K_E}$: $(Z_2)^m \to \mathbf{Z}_q$ следующим образом:

$$f_{K_E}(x_1, \dots, x_m) = x_1a_1 + \dots + x_ma_m$$

для любого $(x_1, \dots, x_m) \in (Z_2)^m$.

**Теорема 2.** Если объявить множество

$$K_E = (a_1, \dots, a_m;\ q)$$

открытым ключом шифрования, а $K_D = k$ — секретным ключом дешифрования, то получим функцию с замком $f_{K_E}$.

**Доказательство.** Элемент

$$x_1a_1 + \dots + x_ma_m$$

кольца $\mathbf{Z}_q$ вычисляется за полиномиальное время.

Если элемент

$$y = x_1a_1 + \dots + x_ma_m \in \mathbf{Z}_q$$

известен, то нахождение набора $(x_1, \dots, x_m)$ равносильно поиску такого подмножества

$$E \in \{a_1, \dots, a_m\},$$

сумма всех элементов которого равна $y$. А это алгоритмически трудноразрешимая задача, поскольку множество $\{a_1, \dots, a_m\}$ не является быстрорастущим: умножения на $k$ элементов быстрорастущего множества $\{b_1, \dots, b_m\}$ разрушило это свойство.

В то же время, знание ключа дешифрования $K_D = k$ позволяет найти набор $(x_1, \dots, x_m)$ за полиномиальное время. Действительно, за полиномиальное время в кольце $\mathbf{Z}_q$ находим

$$k^{-1}y = k^{-1}(x_1a_1 + \dots + x_ma_m) = x_1b_1 + \dots + x_mb_m.$$

При этом отметим, что ввиду

$$x_1b_1 + \dots + x_mb_m \le b_1 + \dots + b_m < q$$

уравнение

$$y' = x_1b_1 + \dots + x_mb_m,$$

где $y' = k^{-1}y$, имеет в кольце $\mathbf{Z}_q$ единственное решение на множестве $(Z_2)^m$, и, значит, это решение должно совпадать с тем набором

$$(x_1, \dots, x_m) \in (Z_2)^m,$$

который использовался при шифровании открытого текста.

Поскольку множество $\{b_1, \dots, b_m\}$ быстрорастущее, то по теореме 1 за полиномиальное время можно найти единственное подмножество

$$\{b_{i_1}, \dots, b_{i_s}\} \subset \{b_1, \dots, b_m\}$$

такое, что

$$b_{i_1} + \dots + b_{i_s} = y'.$$

Но тогда, положив

$$x_{i_1} = 1, \dots, x_{i_s} = 1,$$

а все остальные $x_i$ — равными нулю, получим искомый набор $(x_1, \dots, x_m)$ такой, что

$$x_1b_1 + \dots + x_mb_m = y'.$$

Рюкзачная криптосистема не кажется слишком надёжной, поскольку её ключ шифрования, хотя и не является быстрорастущим множеством, всё же получается простым умножением на $k$ элемента кольца $\mathbf{Z}_q$. Эта ненадёжность подтвердилась в середине 80-х годов XX века, когда был изобретён полиномиальный алгоритм дешифрования рюкзачной криптосистемы.

Одним из способов защиты от этого алгоритма может служить усложнение ключей рюкзачной криптосистемы следующим образом. Помимо множества $\{b_1,\dots,b_m\}$ и чисел $k$, $q$, описанных выше, выбираются числа $\bar{k},\bar{q}$, такие что

$$\bar{q} > mq,\ \bar{k} < \bar{q} \text{ и } \bar{k},\bar{q}$$

взаимно просты. После нахождения в кольце $\mathbf{Z}_q$ элементов

$$a_i = kb_i,\ i = 1,\dots,m$$

в кольце $\mathbf{Z}_{\bar{q}}$ находятся элементы

$$c_i = \bar{k}a_i,\ i = 1,\dots,m.$$

При этом открытым ключом шифрования объявляется набор

$$K_E = (c_1,\dots,c_m,q,\bar{q}),$$

а $K_D = (k,\bar{k})$ — секретным ключом дешифрования. Дешифрования производится следующим образом. Если известен шифртекст $z$, где

$$z = x_1c_1 + \dots + x_mc_m \in \mathbf{Z}_{\bar{q}},$$

то в кольце $\mathbf{Z}_{\bar{q}}$ находим

$$\bar{k}^{-1}z = \bar{k}^{-1}(x_1c_1 + \dots + x_mc_m) = x_1a_1 + \dots + x_ma_m.$$

Поскольку $qm < \bar{q}$, то уравнение

$$y = x_1a_1 + \dots + x_ma_m,$$

где $y = \bar{k}^{-1}\bar{z}$, должно иметь в кольце $\mathbf{Z}_{\bar{q}}$ не более одного решения и, значит, это решение должно совпадать с тем набором

$$(x_1, \dots, x_m) \in (\mathbf{Z}_2)^m,$$

который использовался при шифровании открытого текста.

Затем в кольце $\mathbf{Z}_q$ находим

$$k^{-1}y = k^{-1}(x_1a_1 + \dots + x_ma_m) = x_1b_1 + \dots + x_mb_m$$

и дальше определяем искомый набор $(x_1,\dots,x_m)$ с помощью теоремы 1.

Имеются и другие версии усложнения рюкзачной криптосистемы, для которых пока ещё не найдены эффективные алгоритмы.

**Пример.** Вначале условимся о способе трансформации $A^r \xrightarrow{p} (\mathbf{Z}_2)^m$ открытого текста $(\mathbf{Z}_2)^m$ в строку битов $(\mathbf{Z}_2)^m$, причём если каждый элемент алфавита $A$ преобразуется в строку из $t$ битов, то

$$m = tr \text{ и } 2^t > |A|.$$

Пусть $A$ — 26-буквенный английский алфавит, $r = 2, t = 5, m = 10$ и отображение $p\colon A^r \to (\mathbf{Z}_2)^m$ задано таблицей

| A | B | C | D | E |
|---|---|---|---|---|
| 00001 | 00010 | 00011 | 00100 | 00101 |
| F | G | H | I | J |
| 00110 | 00111 | 01000 | 01001 | 01010 |
| K | L | M | N | O |
| 01011 | 01100 | 01101 | 01110 | 01111 |
| P | Q | R | S | T |
| 10000 | 10001 | 10010 | 10011 | 10100 |
| U | V | W | X | Y |
| 10101 | 10110 | 10111 | 11000 | 11001 |
| Z | | | | |
| 11010 | | | | |

Зашифруем открытый текст REST с помощью рюкзачной криптосистемы с открытым ключом

$K_E = (302, 453, 906, 1812, 784, 1417, 145, 290, 580, 1305; 2991)$ (здесь $q = 2991$):

| Открытый текст | RE | ST |
|---|---|---|
| $x \in (\mathbf{Z}_2)^{10}$ | 1001000101 | 1001110100 |
| $x_1a_1 + \dots + x_{10}a_{10}$ в кольце $\mathbf{Z}_{2991}$ | 302 + 1812 + + 290 + + 1305 = 718 | 302 + 1812 + + 784 + 1417 + + 290 = 1614 |
| Шифртекст | 718 | 1614 |

Дешифруем шифртекст 2773 747 с помощью секретного ключа $K_D = 151$. В кольце $\mathbf{Z}_{2991}$ $k^{-1} = 2476$, откуда находим $\{b_1, \ldots, b_{10}\}$:

$$k^{-1}\{a_1, \ldots, a_{10}\} =$$

$$= 2476 \cdot \{302, 453, 906, 1812, 784, 1417, 145,$$

$$290, 580, 1305\} =$$

$$= \{2, 3, 6, 12, 25, 49, 100, 200, 400, 900\}.$$

| Шифртекст $y$ | 2773 | 747 |
|---|---|---|
| $k^{-1}y$ | 1603 | 1134 |
| $x_1a_1 + \ldots + x_{10}a_{10}$ в кольце $\mathbf{Z}_{2991}$ | 3 + 100 + + 200 + 400 + + 900 | 3 + 6 + 25 + + 200 + 900 |
| $x \in (\mathbf{Z}_2)^{10}$ | 0100001111 | 0110100101 |
| Открытый текст | НО | МЕ |

## Заключение

Высказывание «*приложения мотивируют математику*» может служить девизом данного пособия.

В пособии мы попытались передать идеи криптографии, которые опираются на аппарат высшей алгебры, с доступных для старшеклассников позиций, не пренебрегая при этом строгостью математического изложения. Для этого мы отказались от популяризированных подходов, которыми перенасыщены интернет-ресурсы, с одной стороны, и от перенасыщения текста излишним математическим аппаратом, предваряющим многие современные учебники по приложениям, — с другой. Каждая глава начинается с изложения собственно идей криптографии, которые затем подкрепляются соответствующим математическим инструментарием, адаптированным для восприятия школьниками старших классов.

**Список использованных источников**

1. *Бауэр, Ф.* Расшифрованные секреты. Методы и принципы криптологии / Ф. Бауэр. — М. : Мир, 2007. — 550 с.

2. *Сингх, С.* Книга шифров. Тайная история шифров и их расшифровки / С. Сингх. — М. : Аст; Астрель, 2006. — 447 с.

3. *Мао, В.* Современная криптография. Теория и практика / В. Мао. — М. : Вильямс, 2005. — 763 с.

4. *Ященко, В. В.* Введение в криптографию / В. В. Ященко [и др.] : под общ. ред. В. В. Ященко. — 4-е изд., доп. — М. : МЦНМО, 2012. — 348 с.

5. *Саломаа, А.* Криптография с открытым ключом / А. Саломаа. — М. : Мир, 1995. — 318 с.

*Дата поступления в редакцию 19.05.2020*