УДК 003.26

# КРИПТОГРАФИЯ В СРЕДНЕЙ ШКОЛЕ

CRYPTOGRAPHY IN SECONDARY SCHOOLS

***С.А. Богданович, А.А. Черняк, С.И. Василец, Ж.А. Черняк, А.А. Ермолицкий,***
*S.A. Bogdanovich, A.A. Charniak, S.I. Vasilets, Zh.A. Charniak, A.A. Ermolitski,*
*Белорусский государственный педагогический университет им. М. Танка,*
*г. Минск, Республика Беларусь*
bosead@mail.ru

***Аннотация***. Мы анонсируем учебное пособие по криптографии для средней школы. Его девиз: приложения мотивируют математику. Другими словами, математический инструментарий привлекается по мере необходимости и диктуется идеями шифрования и дешифрования, с изложения которых и начинается каждый раздел пособия.

***Summary***. The motto of this textbook is applications motivate the mathematics. The mathematics is developed only as it is needed.

***Ключевые слова***: криптография, школьнаяматематика.
***Keywords***: cryptography, mathematics in secondary schools.

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. В настоящее время перед системой образования встает новая проблема – подготовить подрастающее поколение к жизни и профессиональной деятельности в новой, высокоразвитой информационной среде, эффективному использованию ее 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.

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

Основные цели, которые ставили перед собой авторы:

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 представлен фрагмент из пособия в сокращенной форме (убраны пояснения и комментарии).

**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 $p:A\to Z_n$, которое алфавит из букв превращает в алфавит открытого текста из чисел. Система шифрования задается подстановкой $f$: $Z_n\to Z_n$, 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 $p:A\to Z_{26}$ задано таблицей

| $x$ | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| $x$ | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 |

Используя отображение $f:Z_{26}\to Z_{26}$, 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 $Z_{26}$ $7^{-1}=15$, $res_{26}(-15\cdot4)=18$, 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** |

**2.1**. Используйте аффинный шифр $f:Z_{26}\to Z_{26}$, при котором $f(x)=3x+14$, для: (а) шифрования открытого текста REPUBLICAN; (б) дешифрования шифртекста ZCAGWPQV.

**Ответ**: (а) PCJYTXOWQD; (б) DEMOCRAT.

**2.2**. Пусть Σ включает 26-буквенный английский алфавит, запятую, точку и пробел. Отображение $p:\Sigma\to Z_{29}$ задано таблицей

| $x$ | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| $x$ | Q | R | S | T | U | V | W | X | Y | Z | , | . | | | | |
| $p$ | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 0 | | | |

Используйте аффинный шифр $f:Z_{29}\to Z_{29}$, при котором $f(x)=5x+11$, для: (а) шифрования открытого текста ALBERTEINSTEIN; (б) дешифрования шифртекста XVG.NTK.LKNGMPX,E,XT

Используйте аффинный шифр $f:Z_{29}\rightarrow Z_{29}$, при котором $f(x)=4x+10$, для: (в) шифрования открытого текста WARANDPEACE; (г) дешифрования шифртекста CL .CLW

**Ответ**: (а) PMUGNXKG, WSXG,W; (б) THEORY OF RELATIVITY; (в) ONXJNHZJPANVA; (г) TOLSTOY.