МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФГАОУ ВО «Казанский (Приволжский) федеральный университет»

Научно-образовательный математический центр

Приволжского федерального округа

Институт математики и механики им. Н.И. Лобачевского

ЛОБАЧЕВСКИЙ И XXI ВЕК

Материалы XII научно-образовательной студенческой конференции, посвященной Дню рождения Николая Ивановича Лобачевского

Казань, КФУ, 1 декабря 2025 года

Казань

2025

УДК 51
ББК 22.1
Л68

Книга издана в рамках реализации программы развития Научно-образовательного математического центра Приволжского федерального округа, соглашение № 075-02-2025-1725/1

Составитель и ответственный редактор –
доктор педагогических наук, профессор **Л.Р. Шакирова**

Л68 Лобачевский и XXI век [Электронный ресурс]: материалы XII научно-образовательной студенческой конференции, посвященной Дню рождения Н.И. Лобачевского (Казань, 1 декабря 2025 г.) / под ред. Л.Р. Шакировой. – Электронные текстовые данные (1 файл: 6,55 Мб). – 346 с. – Системные требования: Adobe Acrobat Reader. – URL: https://kpfu.ru/portal/docs/F_55397432/Sbornik_L21_2025.pdf

В сборнике представлены материалы XII Конкурса-конференции на лучшую студенческую работу «Лобачевский и XXI век», посвященного Дню рождения Н.И. Лобачевского. В сборник вошли конкурсные работы студентов в следующих номинациях: «Лучшая научно-исследовательская работа», «Лучшая поисково-исследовательская разработка», «Лучшая прикладная работа», «Лучшее эссе», «Лучшая методическая разработка». В представленных проектах отражены результаты самостоятельной научной, поисковой, исследовательской деятельности студентов математических и педагогических направлений вузов. Материалы сборника будут интересны и полезны студентам, школьникам и учителям. Печатается в авторской редакции.

УДК 51
ББК 22.1

Оглавление

МЕТОДИКА ПРЕПОДАВАНИЯ ЭЛЕМЕНТОВ КРИПТОГРАФИИ ШКОЛЬНИКАМ В РАМКАХ МАТЕМАТИЧЕСКОГО КРУЖКА

Келехсаева Н.С

Россия, г. Ижевск

Удмуртский Государственный Университет, Институт математики информационных технологий и физики

Научный руководитель: к. ф.− м., доцент Латыпова Н.В.

Аннотация. В статье представлена авторская методика преподавания основ криптографии школьникам 5−7 классов в рамках математического кружка. Рассматривается сценарий урока по теме «Криптография в Средние века и эпоху Возрождения» с детальным разбором изучения шифра

Виженера, методами его взлома и использованием игры для закрепления изученного материала.

Ключевые слова: криптография, методика преподавания, математический кружок, шифр Виженера.

METHODS OF TEACHING CRYPTOGRAPHY ELEMENTS TO SCHOOLCHILDREN IN THE FRAMEWORK OF A MATHEMATICAL CIRCLE

Kelekhsaeva N.S.

Russia, Izhevsk

Udmurt State University

Scientific supervisor: Ph.D., Associate Professor Latypova N.V.

Abstract. The article presents the author's methodology for teaching the basics of cryptography to schoolchildren in grades 5−7 within the framework of a mathematical circle. The scenario of the lesson on the topic "Cryptography in the Middle Ages and the Renaissance" is considered with a detailed analysis of the study of the Vigener cipher , methods of cracking it and using the game to consolidate the studied material.

Keywords: cryptography, teaching methods, mathematical circle, Vigener cipher.

Современные технологии, включая искусственный интеллект и криптографию, стремительно развиваются, но уровень понимания этих основ среди школьников остается низким. Криптография играет ключевую роль в защите данных и функционировании ИИ-систем, а ее изучение в школе может стать мощным инструментом для развития логического мышления, математических навыков и цифровой грамотности.

Актуальность данной темы обусловлена потребностью в специалистах в области информационной безопасности. Внедрение в школьный курс

информатики и математики основ криптографии может значительно повлиять на выбор профессии и на качество специалистов в области защиты информации.

Рабочая программа рассчитана на 1 месяц обучения по одному часу в неделю.

План курса: Введение в криптографию с использованием простых алгоритмов шифрования.

Цели курса:

1. Познакомить с базовыми понятиями криптографии и её ролью в современном мире.
2. Научить применять математические методы (арифметика, алгебра) для шифрования данных.
3. Развить логическое мышление через решение криптографических задач.

Занятие 1: Введение в криптографию. Исторические шифры. Учащиеся знакомятся с базовыми понятиями (шифрование, дешифрование, ключ) на примере шифров Цезаря и Атабаш ([2; с. 12-16]). Практическая часть включает кодирование собственных сообщений и попытку взлома простых шифров с помощью частотного анализа. Занятие проходит в интерактивной форме, включая игру «Шифровальщики».

Занятие 2: Криптография в Средние века и эпоху Возрождения.

Цель занятия: Познакомить учащихся с более сложными методами шифрования, которые использовались в Средние века и эпоху Возрождения. Научить применять шифр Виженера и понимать его уязвимости.

Подготовка и материалы: Для проведения занятия потребуется проектор для демонстрации таблицы Виженера (рис. 1), раздаточные материалы с алфавитными таблицами и числовыми обозначениями букв, а также карточки с зашифрованными текстами. Дополнительно можно

подготовить исторические примеры использования шифров в дипломатической переписке.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рисунок 1. Таблица Виженера

Ход занятия:

1. **Шифр Виженера**

Учитель рассказывает об истории шифра Виженера, который долгое время считался неразрушимым. Объясняется принцип его работы: использование ключевого слова для сдвига букв исходного текста.

Шифр Виженера, разработанный в XVI веке на основе более ранних криптографических идей, долгое время считался абсолютно надежным и использовался для защиты важнейшей дипломатической и военной переписки ([2; с. 45]). Его уникальность заключалась в полиалфавитном принципе: в отличие от простого шифра Цезаря, где все буквы сдвигаются на фиксированное число, здесь каждая буква исходного текста сдвигалась на разное количество позиций согласно буквам ключевого слова. Например,

для шифрования слова "МАТЕМАТИКА" с ключом "ЗАДАЧА" сначала повторяли ключ до длины сообщения ("ЗАДАЧАЗАД"), затем каждая буква текста сдвигалась на соответствующее количество позиций алфавита (М+З=Й, А+А=А и т.д.), получая зашифрованное сообщение "ЙАХЕЪЧДЙА". Именно эта изменчивость правил замены делала шифр устойчивым к частотному анализу, пока в XIX веке не были разработаны методы Казиски и Бэббиджа, обнаружившие уязвимости в повторяющихся паттернах зашифрованного текста ([6; с. 67]). Хотя сегодня этот шифр устарел, он стал важной вехой в развитии криптографии, демонстрируя как силу полиалфавитных систем, так и важность тщательного выбора криптографических ключей.

Затем ученики выполняют практическое задание: зашифровывают слово "ЗАДАЧА" с ключом "РУЧКА".

А=0, Б=1, В=2, Г=3, Д=4, Е=5, Ё=6, Ж=7, З=8, И=9, Й=10, К=11, Л=12, М=13, Н=14, О=15, П=16, Р=17, С=18, Т=19, У=20, Ф=21, Х=22, Ц=23, Ч=24, Ш=25, Щ=26, Ъ=27, Ы=28, Ь=29, Э=30, Ю=31, Я=32.

Стандартный алфавит с использованием букв ъ, ё:

2. **Взлом шифра Виженера**

Учащиеся знакомятся с методом Казиски, который позволяет определить длину ключа по повторяющимся фрагментам в зашифрованном тексте ([2; с. 69]).

Представь, что в зашифрованном сообщении несколько раз встречается одно и то же сочетание букв (например, "ХЩЧ"). Если эти повторы находятся на расстоянии, кратном длине ключа (скажем, через 6 символов), то, скорее всего, ключ состоит из 2 или 3 букв (потому что 6 делится на 2 и 3). После этого текст разбивают на группы по угаданной длине ключа и применяют частотный анализ к каждой группе отдельно, чтобы найти сам ключ.

На практике пробуют применить этот метод к тексту "ХЩЧЗТХЩЧ". В завершение проводится игра "Криптоаналитики", где команды соревнуются в расшифровке сообщений.

Методическое обоснование игрового этапа «Криптоаналитики: Тайна шифра Виженера».

Место в структуре занятия: Данная игра является хорошим закреплением материала о шифре Виженера и его уязвимостях.

Роль в достижении цели занятия: Игра напрямую учит применять шифр Виженера и понимать его суть через погружение учащихся в роль криптоаналитиков, решающих реальные задачи.

Синтез теории и практики: Учащиеся переходят от слушания истории шифра к активному использованию двух изученных методов (щифр Виженера и метод Казиски).

Сложность задач снижена для 5− 7 классов за счет ключевых подсказок (известная длина ключа, первая буква).

Этап 1: «Разведка» (5 минут)

Первое, что делают ученики, это изучают текст «ЪЯММУЦ ЧЧФ» и ищут повторения («ММ», «ЧЧ»), отмечают пробел.

На данном этапе у учеников формируется навык наблюдения. Это первый и ключевой шаг в любом аналитическом процессе. Ученики учатся не просто «смотреть», а «видеть» паттерны и аномалии в данных. Они на практике видят, что повторяющиеся последовательности («ММ» и «ЧЧ») − это главная «зацепка», о которой говорилось в теории метода Казиски. Расстояние между ними (3 символа) подтверждает известную длину ключа, что дает им уверенность в правильности выбранного пути. Пробел, который не шифровался, является важным тактическим данным − он сразу указывает на границу между словами, сужая поле для гипотез.

Этап 2: «Атака Виженера» (10 минут)

Используя простое правило: «Вычти номер ключа из номера шифра, и если результат отрицательный − прибавь 33», ученики пробуют подобрать осмысленный вариант.

На втором этапе ученики не просто запоминают формулу, а многократно применяют ее, видя мгновенный результат в виде букв расшифрованного текста. Это превращает абстрактную математику в конкретный, осязаемый процесс. Перебор вариантов («КОД», «КЛЮЧ», «КОТ») − это не хаотичное угадывание, а выдвижение и проверка гипотез. Если при ключе «КОТ» получается бессмысленный набор букв, гипотеза отвергается. Это основа научного метода.

Этап 3: «Метод Казиски» (10 минут)

Ученики разбивают текст на группы по номеру символа ключа и проводят частотный анализ для каждой группы.

Третий − это самый сложный и самый ценный этап. Ученики понимают, что взлом основан не на удаче, а на системном анализе. Они видят, как огромная задача (подобрать ключ) разбивается на три маленькие и решаемые (подобрать каждую букву ключа). Получив возможные буквы ключа («Ж» и «Д»), команды должны сделать логический вывод: какой ключ − «КОЖ» или «КОД» − является осмысленным словом? Это учит их проверять и интерпретировать полученные результаты.

Этап 4: «Проверка» (5 минут)

Ученики применяют найденный ключ «КОД» для полной расшифровки сообщения «ПРИВЕТ МИР».

Этот этап учит обязательной проверке решения. Важно не только найти ответ, но и убедиться, что он работает для всей системы. Превращение из бессмысленного набора букв «ЪЯММУЦ ЧЧФ» в понятное «ПРИВЕТ МИР» в конце занятия вызывает восторг и чувство глубокого удовлетворения у учащихся. Положительные эмоции создают устойчивый интерес к предмету и лучшему закреплению изученного материала.

Заключительная часть (10 минут)

Подводятся итоги занятия. Ученики отвечают на вопросы: почему шифр Виженера считался надёжным и как его можно взломать. Даётся домашнее задание: зашифровать свою фамилию с ключом "ВОЗРОЖДЕНИЕ" и попробовать взломать текст "ЦЫВМРЫВМПТ".

Методические рекомендации: Для лучшего усвоения материала можно использовать визуализацию (цветные маркеры для выделения повторений) и дифференцировать задания по сложности.

Ожидаемые результаты: К концу занятия ученики понимают принцип полиалфавитного шифрования, умеют применять шифр Виженера и знают основы его взлома. Это создаёт базу для изучения более сложных криптографических методов в будущем.

Занятие 3: Криптография в XX веке. Энигма и симметричное шифрование.

Это занятие посвящено переходу от ручных шифров к машинным. Учащиеся узнают о принципах работы легендарной шифровальной машины «Энигма» и основах симметричного шифрования (на примере операции XOR) ([5; с. 203]). Особое внимание уделяется проблеме безопасной передачи ключа, для понимания которой моделируется алгоритм Диффи−Хеллмана ([2; с. 72]).

Занятие 4: Итоговый проект. Криптографический квест.

Заключительное занятие − командное соревнование, где учащиеся применяют все изученные методы на практике. Команды расшифровывают сообщения, определяют тип шифра, проводят криптоанализ и восстанавливают ключи. Такая форма позволяет закрепить материал, развить навыки логики и коммуникации командной работы.

Ожидаемые результаты и образовательный потенциал

Участие в кружке по криптографии дает школьникам комплекс преимуществ:

- *Развитие компетенций:* курс эффективно развивает логическое, алгоритмическое и критическое мышление, креативность через создание и анализ шифров.
- *Профориентация:* знакомство с востребованными профессиями в области кибербезопасности и криптографии.
- *Популяризация* математики.
- *Подготовка к олимпиадам:* решение криптографических задач тренирует нестандартное мышление, необходимое для успеха на олимпиадах по математике и информатике.
- *Формирование цифровой культуры:* школьники осознают важность защиты персональных данных и принципов информационной безопасности в интернете и повседневной жизни.

Игровая форма занятий, включающая квесты и соревнования, поддерживает высокую мотивацию, превращая изучение сложных математических концепций в увлекательное интеллектуальное приключение.

Заключение

Внедрение основ криптографии в школьное образование через систему математических кружков представляет собой идеальный синтез фундаментального математического знания и практико−ориентированного подхода. Такой курс не только расширяет кругозор учащихся, но и готовит их к жизни в цифровом будущем, формируя ответственное и грамотное поведение в информационной среде. Разработанная методика демонстрирует, что криптография − не просто набор алгоритмов, а живая и развивающаяся наука, тесно связанная с историей, математикой и технологиями.

Список литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С. Основы криптографии. − М.: Гелиос АРВ, 2005.

2. Бабаш А.В., Шанкин Г.П. История криптографии. − М.: Гелиос, 2002.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. − М.: МЦНМО, 2003.
4. Гарднер, М. Математические головоломки и развлечения / М. Гарднер; пер. с англ. − Москва: Мир, 2017.
5. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. − СПб.: Лань, 2011.
6. Кан Д. Взломщики кодов. − М.: Центрполиграф, 2000.
Нечаев В.И. Элементы криптографии. − М.: Высшая школа, 1999.

Электронное издание

ЛОБАЧЕВСКИЙ И XXI ВЕК

Материалы XII научно-образовательной студенческой конференции, посвященной Дню рождения Н.И. Лобачевского

Компьютерная верстка
А.А. Нурмухаметовой

Гарнитура «Times New Roman, Calibri».