Государственное бюджетное общеобразовательное учреждение гимназия №498

Невского района Санкт-Петербурга

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

Математика

ЭЛЕМЕНТЫ КРИПТОГРАФИИ ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ

Автор: Ефремова Анастасия Александровна,

обучающаяся 10А класса,

ГБОУ Гимназия № 498, Россия, г. Санкт-Петербург

Научный руководитель: Качалова Ирина Викторовна,

учитель математики,

ГБОУ Гимназия № 498, Россия, г. Санкт-Петербург

г. Санкт-Петербург

2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Математика была и остается одним из моих самых любимых предметов. Участие в различных конкурсах и олимпиадах всегда давало стимул к саморазвитию и познанию нового. Я заинтересовалась криптографией после того, как мне предложили принять участие в Межрегиональной олимпиаде школьников им. И. Я. Верченко по математике и криптографии.

Оказывается, распространение доступного интернета по всему миру невозможно представить без криптографии. С появлением мессенджеров, социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональной информации в сети происходит без остановки и в огромных количествах. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почты, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка.

Шифрование информации применяется в различных науках. В биологии вся информация содержится в генетическом коде. В географии координаты объекта – своеобразный шифр его местоположения. Ноты тоже можно рассматривать как шифр, владея которым несложно исполнить чудесную мелодию. Даже в художественной литературе, особенно в приключенческом и детективном жанрах есть описание использования различных шифров. Например, в рассказе «Пляшущие человечки» Артур Конан Дойл описывает подстановочный шифр из рисунков пляшущих человечков.

Актуальность проекта заключается в том, что в настоящее время в связи с совершенствованием информационных технологий и технических средств обработки и передачи информации, существование без такой науки как криптография почти невозможно.

На данный момент существуют работы по изучению истории криптографии, по исследованию методов шифрования и дешифрования. Однако,

наша работа *уникальна* новым подходом к изучению криптографии - внедрению изучения ее элементов начиная с 5 класса.

Цель проекта: заинтересовать учащихся 5 и 6 классов изучением основ криптографии и разработать серию задач по криптографии для этой возрастной категории.

Гипотеза: изучение элементов криптографии в рамках урока математики или внеурочной деятельности вызывает у учащихся интерес и обеспечивает преемственность и перспективность математического образования.

Для достижения поставленной цели нам необходимо решить следующие задачи:

1. Изучить историю криптографии.
2. Познакомиться с различными способами шифрования информации.
3. Рассмотреть применение криптографии в различных науках.
4. Подготовить и провести занятие для обучающихся 5-х и 6-х классов.
5. Разработать серию задач по криптографии.
6. Сделать выводы об успешности проведенного мероприятия.

Объект изучения: основы криптографии.

Предмет: задачи по криптографии, которые можно использовать при изучении математики.

Для решения поставленных задач были использованы следующие *методы:*

- теоретические (анализ и синтез информации из литературных источников по теме исследования);

- эмпирические (наблюдение, сравнение);

- математические (статистические методы, метод визуализации данных с помощью круговых диаграмм).

Глава 1. Теоретические основы криптографии

1.1 Первые шифры

Древнесемитский атбаш, приблизительно 600 г. до н. э, является одним из первых шифров. Здесь информацию запутывали самым простым способом – с помощью подмены букв алфавита. Криптограммы на атбаше встречаются в Библии. Одним из первых документально зафиксированных шифров является шифр Цезаря (около 100 г. до н. э.). Его принцип был очень прост: каждая буква исходного текста заменялась на другую, отстоящую от нее по алфавиту на определенное число позиций.

1.2 Успехи арабских ученых

Шифрованием пользовались многие древние народы, но особенного успеха в криптографии уже в нашу эру достигли арабские ученые. Высокий уровень развития математики и лингвистики позволил арабам не только создавать свои шифры, но и заниматься расшифровкой чужих. Это привело к появлению первых научных работ по криптоанализу – дешифровке сообщений без знания ключа. Работы арабских ученых способствовали появлению полиалфавитных шифров, более стойких к расшифровке, в которых использовались сразу несколько алфавитов.

1.3 Тайнопись в Древней Руси

Интересно, что в Древней Руси тоже были свои способы тайнописи, например литорея, которая делилась на простую и мудрую. В мудрой версии шифра некоторые буквы заменялись точками, палками или кругами. В простой литорее, которая еще называлась тарабарской грамотой, все согласные буквы кириллицы располагались в два ряда. Зашифровывали письмо, заменяя буквы одного ряда буквами другого. Еще одним известным шифром Древней Руси была цифирь, когда буквы, слоги и слова заменялись цифрами.

1.4 Криптография в эпоху Возрождения, изобретения Леона Альберти

В эпоху Возрождения криптография переживает подъем. Около 1466 года итальянский ученый Леон Альберти изобретает шифровальный диск. На неподвижном внешнем диске был написан алфавит и цифры. Внутренний подвижный диск также содержал буквы и цифры в другом порядке и являлся ключом к шифру. Таким образом, шифр Альберти стал одним из первых шифров многоалфавитной замены, основанных на принципе комбинаторики. Здесь также стоит упомянуть такое явление, как стеганография, которому в работе Альберти тоже было уделено внимание. Если с помощью шифра пытаются утаить смысл информации, то стеганография позволяет скрыть сам факт передачи или хранения данных. То есть текст, спрятанный с помощью этого метода, вы примите за обычную картинку. Часто методы стеганографии и криптографии объединялись.[2]

1.5 Шифр Виженера, «цилиндр Джефферсона»

Самым известным шифровальщиком XVI века считается дипломат и алхимик из Франции Блез де Виженер, придумавший шифр, в котором использовалось 26 алфавитов, а порядок использования шифра определялся знанием пароля. Можно сказать, что шифр Виженера представлял собой комбинацию нескольких шифров Цезаря.

Промышленная революция не обошла вниманием и криптографию. Около 1790 года Томас Джефферсон создал дисковый шифр, прозванный позже цилиндром Джефферсона. Этот прибор, основанный на роторной системе, позволил автоматизировать процесс шифрования и стал первым криптоустройством Нового времени. Большое влияние на шифровальное дело оказало изобретение телеграфа. Прежние шифры вмиг перестали работать, при этом потребность в качественном шифровании только возрастала в связи с чередой крупных военных конфликтов.

1.6 Криптография в военной сфере XIX–XX веков

В XIX–XX веках основные импульсы для развития криптографии давала именно военная сфера. Во Второй мировой войне противники уже использовали шифры которые считались не раскрываемыми. К таким относилась знаменитая

машина «Энигма», которой пользовались нацисты, а также – американская машина М-209. Шифры «Энигмы» считались самыми стойкими для взлома, так как количество ее комбинаций достигало 15 квадриллионов. Однако код «Энигмы» все же был расшифрован, сперва польскими криптографами в 1932 году, а затем английским ученым Аланом Тьюрингом, создавшим машину для расшифровки сообщений «Энигмы» под названием «Бомба». Комплекс из 210 таких машин позволял англичанам расшифровывать до 3 тыс. военных сообщений нацистов в сутки и внес большой вклад в победу союзников.

1.7 Советские шифровальные машины

О советских шифровальных машинах известно мало, так как до последнего времени информация о них была засекречена. Например, до 1990-х годов в СССР и союзных странах использовалась роторная шифровальная машина М-125 «Фиалка». Также достаточную популярность получили машины М-100 «Спектр», К-37 «Кристалл», М-101 «Изумруд» и М-105 «Агат». Все они кроме последней использовались советскими войсками во время Второй мировой войны на оперативно-тактическом уровне. М-105 «Агат» — это одна из последних шифровальных машин, созданная в СССР.

Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Будущее этой науки творится на наших глазах – очередная революция в шифровании произойдет с появлением квантовых суперкомпьютеров, разработка которых уже ведется. [3]

1.8 Сферы применения криптографии

Элементы криптографии используются для решения конкурсных и олимпиадных задач. Например, в России уже много лет проходит

Межрегиональная олимпиада школьников имени И.Я. Верченко по математике и криптографии с 8 по 11 класс. Вот пример задачи отборочного этапа 2021 года:

Задача 3. Магический квадрат

На рисунке представлено сообщение, зашифрованное с помощью магического квадрата 3x3, состоящего из неповторяющихся цифр от 1 до 9. Магический квадрат – квадратная таблица из целых чисел, в которой суммы чисел вдоль любой строки, любого столбца и любой из двух главных диагоналей равны одному и тому же числу.

Р	Й	Е
К	Е	Н
Ы	С	Т

Расшифруйте сообщение, если известна часть квадрата.

		2
3	5	

Ответ запишите ЗАГЛАВНЫМИ буквами!

Ответ: СЕКРЕТНЫЙ

Решение задач по шифрованию и дешифровке способствует развитию логического мышления, что является залогом успеха в дальнейшем обучении.

Более того, в банке заданий ОГЭ по информатике для 9 класса есть ряд заданий на дешифровку информации, как пример:

Валя шифрует русские слова, записывая вместо каждой буквы её код.

А	В	Д	О	Р	У
01	011	100	111	010	001

Некоторые цепочки можно расшифровать не одним способом. Например, 00101001 может означать не только УРА, но и УАУ.

Даны три кодовые цепочки:

01001001
100011111010
10011101001

Найдите среди них ту, которая имеет только одну расшифровку и запишите в ответе расшифрованное слово.

Спрятать решение

Решение.

Проанализируем каждый вариант ответа:

1) «01001001» может означать как «РАУ», так и «АУУ».
2) «100011111010» может означать только «ДВОР».
3) «10011101001» может означать как «ДОАУ», так и «ДОРА».

Ответ: ДВОР.

Все вышесказанное дает нам возможность сделать следующие выводы.

Криптография стремительно развивается, а ее значимость и важность в современном мире набирает обороты. Способы шифрования информации основываются на алгоритмах, используемых в комбинаторике – разделе математики, а криптография как наука невозможна без сравнительного анализа, синтеза, аналогии, поэтому «знакомство» с криптографией можно начинать на уроках или внеурочных занятиях по математике. Метапредметные связи криптографии с другими науками указывает на целесообразность изучения ее основ уже с 5 класса.

Глава 2. Практическое применение криптографии

Проанализировав разные источники, было принято решение разработать и провести занятие для ребят 5-х классов, на котором у них была бы возможность познакомиться с основами криптографии и попробовать свои силы при решении задач на дешифровку информации. В рамках внеурочной деятельности было проведено три занятия в пятых классах, по 30 минут каждое (Приложение 4). На занятиях были предложены историческая справка, теоретическая информация, а также представлены задачи 4 уровней сложностей (Приложение 1), ребус для разминки и задача «Пляшущие человечки», разработанная по аналогии с задачей, описанной в одном из произведений Артура Конана Дойла (Приложение 2).

Решение нескольких задач было выполнено совместно, чтобы ребята поняли алгоритм и активнее включились в дальнейшую работу. Далее было предложено самостоятельно решить задачи, выбирая уровень сложности на свое усмотрение. Поэтапная проверка в течении занятия (совместная и индивидуальная) показала, что учащиеся более чем успешно справились с задачами.

В начале и конце урока был проведен опрос, в котором приняли участие 79 человек. Ребятам были заданы следующие вопросы:

- Знаете ли вы, что такое криптография?
- Хотели бы изучать основы криптографии в школе?
- Как вы оцениваете свою работу на занятии?

В ходе рефлексии было отмечено, что пятиклассники высоко оценили продуктивность своей деятельности. Ребята отметили, что им не знакомо такое понятие как криптография, а также 99% из них ответили, что с удовольствием продолжат изучение элементов криптографии.

Уже в 5 классе ребята проявили особый интерес к криптографии, довольно успешно с явным удовольствием, решали предложенные задачи и придумывали свой шифр.

Спустя год я решила повторить занятие для этих же классов (уже 6-х) и подготовила для них ряд новых задач (приложение 3) и пару задач на повторение изученного в прошлом году материала. Ребята, как и в прошлый показали свою заинтересованность и с удовольствием решали предложенные задачи. Это позволяет констатировать о целесообразности использования элементов криптографии уже с 5 класса на занятиях внеурочной деятельности или в контексте одной из тем на уроках математики. Таким образом, гипотеза была подтверждена, а цель достигнута.

Изучение основ криптографии и решение задач, из этой области — это большой потенциал для углубления знаний обучающихся. Знания, полученные при изучении элементов криптографии, могут обеспечивать преемственность и перспективность математического образования.

ЗАКЛЮЧЕНИЕ

В математике постоянно решаются разнообразные, сложные, порой нестандартные задачи, а каждый шифр – это логическая задача. Решение задач по криптографии может способствовать:

- развитию мыслительных операций,
- умению структурировать информацию,
- общему интеллектуальному развитию ребенка.

Практической значимостью работы является привлечение внимания к необходимости и перспективности изучения основ криптографии уже с 5 класса и возможности использования разработанных и подобранных задач для данной

возрастной группы детей. Эти знания дадут основу для дальнейшего изучения информатики.

В будущем планируется разместить серию криптографических задач на просторах сети Интернет в общем доступе, чтобы желающие могли получить новые или усовершенствовать имеющиеся знания в области криптографии.

ЛИТЕРАТУРА

1. Бабаш А. В. История криптографии. Часть I / А.В. Бабаш, Г.П. Шанкин. - М.: Гелиос АРВ, 2002
2. Душкин Р. Шифры и квесты: таинственные истории в логических загадках. – М., 2017, 288 с.
3. Русецкая И. А. История криптографии в Западной Европе в раннее новое время. – СПб.: Центр гуманитарных инициатив, 2014, 144с
4. Сингх Саймон “Книга шифров. Тайная история шифров и их расшифровки”, Р.: Аванта+, 2009, 462 с.
5. Интернет-портал «Что такое криптография? Где она применяется?»: https://aws.amazon.com/ru/what-is/cryptography/
6. Интернет-портал «Что такое криптография и как она стала частью нашей жизни»: https://trends.rbc.ru/trends/innovation/63120ea49a7947ccdd023670
7. Интернет-портал «Криптоком. Системы защиты информации»: https://www.cryptocom.ru/articles/crypto.html
8. Интернет-портал «Основы криптографии: от математики до физики»: https://tproger.ru/translations/understanding-cryptography/

ПРИЛОЖЕНИЕ

Приложение 1

1) Вася и Петя играли в шпионов и кодировали сообщения собственным шифром. Фрагмент кодовой таблицы приведён ниже:

Н	М	Л	И	Т	О
~	*	*@	@~*	@*	~*

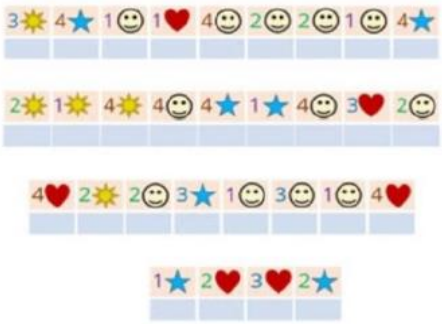
Расшифруйте сообщение, если известно, что буквы в нём не повторяются:

*@@~**~*~

Запишите в ответе расшифрованное сообщение.

2)

	1	2	3	4
❤	Ц	А	Й	Д
☀	Н	И	П	Т
☺	О	С	В	Е
★	Ф	Л	К	Р



3)

4*) Валя шифрует русские слова (последовательности букв), записывая вместо каждой буквы её код:

А	Д	К	Н	О	С
01	100	101	10	111	000

Некоторые цепочки можно расшифровать не одним способом. Например, 00010101 может означать не только СКА, но и СНК. Даны три кодовые цепочки:

1010110
100000101
00011110001

Найдите среди них ту, которая имеет только одну расшифровку, и запишите в ответе расшифрованное слово.

Приложение 2

Расшифруйте послание _____

Приложение 3

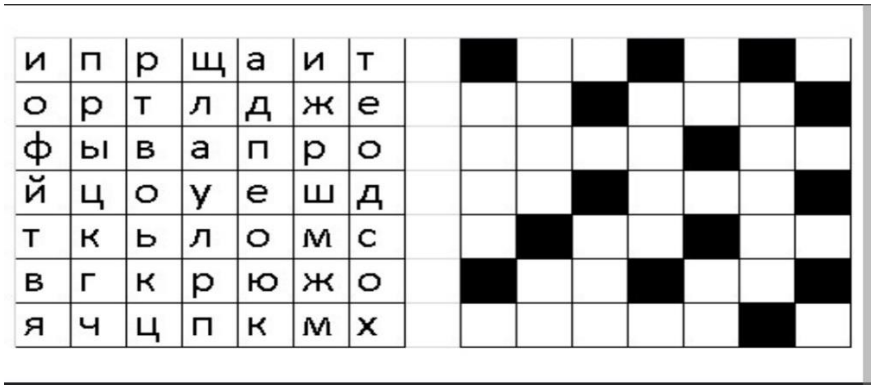
Кирилл шифрует английские слова, записывая вместо каждой буквы её номер в алфавите (без пробелов). Номера букв даны в таблице:

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

Некоторые шифровки можно расшифровать не одним способом. Например, 16118 может означать «AFAR», может — «PAR», а может — «AFAAH». Даны четыре шифровки:

1234
2013
3120
4321

Только одна из них расшифровывается единственным способом. Найдите её и расшифруйте. То, что получилось, запишите в качестве ответа.



нарово → ворона

кабасо → собака

гайпупо →?

Рогсоно →?

Мотгебе →?

a ألف	? - فاء ألف راء و ز
в في	? - سين في كاف واو فا
ж ز	? - سين واو كاف واو كاف
и و	
у في	
р راء	
п ـپـ	
ф فا	
о واو	
к كاف	
с سين	

Приложение 4