Краевая научно-практическая конференция
учебно-исследовательских работ учащихся 6-11 классов
«Прикладные и фундаментальные вопросы математики и физики»

Прикладные вопросы математики

Криптография в математике

Русских Злата Юрьевна,
7 кл., Зюкайская СОШ, Верещагинского р-а
Чудинова Любовь Сергеевна,
учитель математики

Пермь. 2017.

Оглавление

Паспорт проекта

1	**Название проекта**	«Криптография в математике»
2	**Руководитель проекта**	Чудинова Любовь Сергеевна
3	**Консультанты проекта**	Федорова Елена Александровна Русских Юлия Александровна
4	**Возраст учащихся, на которых рассчитан проект**	11-14 лет
5	**Состав проектной группы**	
6	**Описание основных этапов проекта**	1. Подготовительный: определение темы проекта, выбор материала для реализации проекта. 2. Этап планирования: планирование деятельности по созданию проекта, отбор методов работы 3. Этап реализации проекта: работа с литературой, применение на практике методов шифрования Создание сборника заданий по применению различных видов шифров для использования при углубленном изучении предмета математики

Введение

Наверно, каждый из нас в детстве играл в тайные записочки, содержание которых знали и понимали только единицы, так сказать, избранные. Создание своего особенного языка, своего, ни на что не похожего алфавита, чтобы никто-никто на всем белом свете не догадался о содержании нашей переписки. Это увлекательнейшее занятие! Ведь можно было писать о чем угодно, зная тайный шифр. Это было началом моего увлечения криптологией. Проблема защиты информации от прочтения посторонним лицом или противником волновала человеческие умы с незапамятных времен. В дальнейшем меня ждала встреча с таинственными «пляшущими человечками», загадку которых так блистательно разгадал великий сыщик Шерлок Холмс. Это только подогрело интерес. Именно поэтому я выбрал столь сложную, но очень интересную для меня тему.

Данный проект предназначен для знакомства и глубокого понимания криптографии и ее связи с математикой и другими науками.

Целью проекта является знакомство с криптографией и изучение применения в ней основ математики.

Итогом работы над проектом является сборник заданий, ориентированный на средний школьный возраст, презентация шифров для обучающихся, изучающих математику углубленно в рамках дополнительных факультативных занятий.

Задачи:

1. Изучить историю криптографии с помощью специальной литературы.
2. Познакомиться с различными видами и способами шифрования и проанализировать различные шифры с применением элементарных математических навыков и действий.
3. Составить презентацию различных методов и форм шифрования.
4. Осуществить шифровку и дешифровку текста с применением собственного шифра.
5. Создать сборник заданий для обучающихся.

Для реализации поставленных задач были использованы следующие методы исследования: теоретический (поисковый, описательный) и практический (метод анализа и обобщения, анкетирование).

Гипотеза: криптография не потеряла своей актуальности и полезности и в наше время, заниматься шифрованием и дешифрованием увлекательно и полезно, знание и использование шифра различной сложности помогает скрыть информацию, не предназначенную для посторонних.

Этапы работы над проектом

№	Этап проекта	Содержание
1.	Подготовительный	Определение темы проекта, выбор материала для реализации проекта.
2.	Этап планирования	Планирование деятельности по созданию проекта, отбор методов работы.
3.	Этап реализации проекта	Работа с литературой, поиск шрифтов, основанных на математических методах.
		Создание шрифта и сборника заданий

Объект: криптография и методы ее практического применения.

Предмет: математические и логические способы кодирования и шифрования.

Новизна: высокая значимость при недостаточности внимания к криптографии, как науке, в среднем звене общего образования.

Глава I. Что такое криптография

Криптография - наука о математических методах обеспечения конфиденциальности, т.е. невозможности прочтения информации посторонними. С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в источниках, датируемых временами до нашей эры. Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день, появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

1.1. История возникновения

История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была своеобразной криптографической системой, так как в древних обществах ею владели только избранные. Считается, что основы криптографии заложил Эней Тактик. Попытки зашифровать данные делали ещё в древней Индии и Месопотамии. Но они были не очень удачными. Первая надёжная система защиты была разработана в Древнем Китае. Широкое распространение криптография приобрела и в странах Античности. Тогда она использовалась в военных целях. Методы криптографии нашли своё применение и в Средние века, но их уже взяли на вооружение купцы и дипломаты. Золотым веком данной науки называют эпоху Возрождения. Тогда же был предложен двоичный способ шифрования, аналогичный которому используется в компьютерной технике в наши дни. Во время Первой мировой войны она была признана полноценным боевым инструментом. Стоило только разгадать сообщения противника – и можно было получить ошеломляющий результат. В качестве примера можно привести перехват телеграммы, посланной немецким послом Артуром Циммерманом американскими спецслужбами. Конечным результатом этого стало то, что США вступило в боевые действия на стороне Антанты.

Искусство шифрования и тайной передачи информации было присуще практически всем государствам. Криптография в прошлом использовалась, прежде всего, в военных целях. Однако сейчас, по мере образования информационного общества, криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, корпоративную безопасность.

Условно историю криптографии можно разделить на несколько периодов:

- первый период (приблизительно с 3-го тысячелетия до н.э.) характеризуется господством моноалфавитных шифров (основной принцип – замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).
- второй период (хронологические рамки – с IX века на Ближнем Востоке и с XV века в Европе – до начала XX века) ознаменовался введением в обиход полиалфавитных шифров.
- третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков, при этом продолжалось использование полиалфавитных шифров.
- четвёртый период – с середины до 70-х годов XX века – период перехода к математической криптографии.
- современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления – криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами (в предыдущие эпохи использование криптографии было исключительной прерогативой государства).

1.2. Каким должен быть шифр

Поскольку основной задачей криптографии является защита информации, то необходимо рассмотреть определенные требования к шифрам. Итак, каким же должен быть шифр?

Впервые несколько общих принципов сформулировал голландский лингвист 19 века Август Керкхоффс.

Во-первых, шифр должен обеспечивать достаточную стойкость к взлому. Несмотря на то, что одиночное шифрованное сообщение может быть в принципе невзламываемым, часто бывает необходимо переслать сотни сообщений, зашифрованных в одной и той же системе.

Во-вторых, шифр должен быть прост в использовании. Опыт показывает, что пользователи избегают пользоваться сложными и громоздкими шифросистемами либо пользуются ими с ошибками.

В-третьих, стойкость шифра к взлому должна полностью зависеть от обеспечения секретности ключа, а не алгоритма. Опять-таки из опыта известно, что алгоритм, которым пользуется много людей, не может долго оставаться в секрете.

«Невзламываемый» шифр – это целый класс систем, широко известных под названием «одноразовые вкладыши». Соответствующий принцип был впервые отчетливо сформулирован американским ученым Гилбертом Вернамом примерно в 1917. Вернам занимался разработкой криптографических методов для использования в телетайпных машинах. В этой связи он предложил комбинировать открытый текст, представленный в виде отверстий в бумажной перфоленте, с данными, нанесенными на другую перфоленту и являющимися ключом к шифру. Ключ должен был состоять из отверстий, перфорированных в ленте случайным образом. Комбинация этих двух лент и составляла шифротекст. Без знания ключа такое сообщение не поддается анализу.

1. 3. Виды шифрования

Сначала немного терминологии, чтобы разобраться с основными понятиями в криптографии.

Шифр – какая-либо система преобразования текста с секретом для обеспечения секретности передаваемой информации.

Открытый текст – сообщение, подлежащее передаче адресату.

Шифротекст – преобразованное с помощью шифра сообщение.

Шифрование – процесс преобразования открытого текста.

Ключ – параметр, определяющий правило и метод шифрования.

Все многообразие существующих криптографических методов можно свести к следующим классам преобразований.

Моно- и многоалфавитные подстановки или замена - наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Перестановки - также несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами.

Гаммирование - этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры - представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем “чистые”

преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

Известны случаи, когда криптография считалась даже черной магией. Этот период развития криптографии как искусства длился с незапамятных времен до начала XX века, когда появились первые шифровальные машины. Понимание математического характера решаемых криптографией задач пришло только в середине XX века — после работ выдающегося американского ученого К.Шеннона. В криптографии, всегда использовались всевозможные устройства, как для облегчения кодирования сообщения, так и повышения стойкости шифра. Одним из самых известных устройств являются роторные машины. Самым известным роторным устройством является «Энигма» (Enigma). Энигма использовалась немцами во Второй Мировой Войне. Сама идея пришла в голову Артуру Шербиусу (Arthur Scherbius) и Арвиду Даму (Arvid Gerhard Damm) в Европе. В настоящее время известно множество различных видов шифров. Вот примеры некоторых из них.

Книжный шифр

В таком шифре ключом является некая книга, имеющаяся и у отправителя и у получателя. В шифре обозначается страница книги и строка, первое слово которой и является разгадкой. Дешифровка невозможна, если книги у отправителя и корреспондента разных годов издания и выпуска. Книги обязательно должны быть идентичными.

Шифр Цезаря

Сутью данного шифра является замена одной буквы другой, находящейся на некоторое постоянное число позиций левее или правее от неё в алфавите. Гай Юлий Цезарь использовал этот способ шифрования при переписке со своими генералами для защиты военных сообщений. Этот шифр довольно легко взламывается, поэтому используется редко.

Шифр с кодовым словом

Еще один простой способ как в шифровании, так и в расшифровке. Используется кодовое слово (любое слово без повторяющихся букв). Данное слово вставляется впереди алфавита и остальные буквы по порядку дописываются, исключая те, которые уже есть в кодовом слове.

Шифр Атбаш

Один из наиболее простых способов шифрования. Первая буква алфавита заменяется на последнюю, вторая – на предпоследнюю и т.д.

Шифр Фрэнсиса Бэкона

Один из наиболее простых методов шифрования. Для шифрования используется алфавит шифра Бэкона: каждая буква слова заменяется группой из пяти букв «A» или «B» (двоичный код).

a AAAAA g AABBA m ABABB s BAAAB y BABBA

b AAAAB h AABBB n ABBAA t BAABA z BABBB

c AAABA i ABAAA o ABBAB u BAABB

d AAABB j BBBAA p ABBBA v BBBAB

e AABAA k ABAAB q ABBBB w BABAA

f AABAB l ABABA r BAAAA x BABAB

Сложность дешифрования заключается в определении шифра. Как только он определен, сообщение легко раскладывается по алфавиту.

Поросячья латынь

Чаще используется как детская забава, особой трудности в дешифровке не вызывает. Обязательно употребление английского языка, латынь здесь ни при чем. В словах, начинающихся с согласных букв, эти согласные перемещаются назад и добавляется “суффикс” ау. В русском языке такой метод тоже используется. Называют его по-разному: “синий язык”, “солёный язык”, “белый язык”, “фиолетовый язык”. Таким образом, в Синем языке после слога, содержащего гласную, добавляется слог с этой же гласной, но с добавлением согласной “с” (т.к. язык синий).

Решетка Кардано

Инструмент кодирования и декодирования, представляющий собой специальную прямоугольную (в частном случае — квадратную) таблицу-карточку, часть ячеек которой вырезана. Решетка не имеет жесткого шаблона, она сделана из листа картона или пергамента, или же из тонкого металла. Чтобы обозначить линии письма, бумагу разлиновывают, и между этими линиями вырезают прямоугольные области через

интервалы произвольной длины. Шифратор помещает решетку на лист бумаги и пишет сообщение в прямоугольных отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделенным на большое число маленьких фрагментов. Затем решетка убирается, и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью другого текста. Такое заполнение требует известного литературного таланта. Для расшифровки у получателя сообщения должна быть такая же решетка.

Цифровое (числовое) кодирование

Кодирование с помощью чисел. Появилось, наверное, вместе с первым алфавитом. Например, поскольку каждая буква знает свое место, то у нее есть номер, а значит букву можно заменить цифрами: а - I, к - 12, о - 16 и т.д. Для того, чтобы пользоваться цифровым кодом нужно выучить алфавит, но это как раз очень пригодится, особенно будущему переводчику, ученому и в любой профессии, связанной с информацией.

Азбука Морзе

«Морзянка» или код Морзе — способ знакового кодирования, представление букв алфавита, цифр, знаков препинания и других символов последовательностью сигналов: длинных (тире) и коротких (точка). За единицу времени принимается длительность одной точки. Длительность тире равна трём точкам. Пауза между элементами одного знака — одна точка, между знаками в слове — 3 точки, между словами — 7 точек. Назван в честь американского изобретателя и художника Сэмюэля Морзе.

Шрифт Брайля

Рельефно-точечный тактильный шрифт, или «ночной», предназначенный для письма и чтения незрячими и плохо видящими людьми. Шрифт активно используется слабовидящими и незрячими людьми. Для изображения букв в шрифте Брайля используются шесть точек. Точки расположены в два столбца. При письме точки прокалываются, и поскольку читать можно только по выпуклым точкам, «писать» текст приходится с обратной стороны листа. Текст пишется справа налево, затем страница переворачивается, и текст читается слева направо. Для читающего точки нумеруются по столбцам слева направо и по строкам сверху вниз. Для пишущего на перевёрнутой странице нумерация выглядит по иному: точка 1 находится в верхнем правом углу, под ней — точка 2, в нижнем левом углу — точка 6.

Шифр «Сцитала»

Этот шифр известен со времен войны Спарты против Афин в V веке до н.э. Для его реализации использовалась сцитала — жезл, имеющий форму цилиндра. На сциталу виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль оси сциталы записывался открытый текст. Лента разматывалась и получалось (для непосвященных), что на ленте в беспорядке написаны какие-то буквы (каждая из букв поперек ленты). Затем лента отправлялась адресату. Адресат брал такую же сциталу, таким же образом наматывал на нее полученную ленту и читал сообщение вдоль оси сциталы.

Древнерусская тайнопись

Наидревнейший метод тайнописания согласно имеющихся в руках учёных старых рукописей именовался «иными письменами». В них символы кириллицы менялись на символы глаголицы, латиницы, греческой или пермской азбуки. Немного в стороне от всех других азбук как тайнопись стоит пермская. Её придумал епископ Стефан из Перми, используя как базу кириллическую и греческую азбуку, но реально никто не применял. В 15-м веке, как мало кому известный, пермский алфавит стал методом тайнописания, но даже так он не был широко распространён. За «иными письменами» по распространению следует метод тайнописания, который можно найти в древнерусских письменных памятниках, - это метод «изменённых значков», появившаяся в 14-м столетии. Ещё один метод, бывший в ходу у писарей тех времён, именовался методом подстановки. Существовали две его разновидности: «простая литорея» (от лат. litera - буква) и «мудрая литорея», а также разновидность «мудрой» - «риторские письмена». В «простой литорее» каждая согласная буква из первых 10, написанных в одну строчку в порядке следования алфавита, изменялась на букву, находившуюся под ней в нижней строчке, которая содержала последние 10 согласных букв, записанных в порядке обратного следования:

Б	**В**	**Г**	**Д**	**Ж**	**З**	**К**	**Л**	**М**	**Н**
Щ	**Ш**	**Ч**	**Ц**	**Х**	**Ф**	**Т**	**С**	**Р**	**П**

Матричный способ

Для того чтобы воспользоваться способом шифровки с помощью матриц, достаточно уметь считать на уровне 6 класса, знать порядок букв в алфавите и помнить всего 8 чисел.

Расшифровать же его специалисты могут только с помощью компьютера. Матрица - это прямоугольная таблица, составленная из элементов, имеющих произвольную природу. Элементы матрицы расположены в строки и столбцы. Матрица, в которой одинаковое количество строк и столбцов, называется квадратной.

Ребусы

Ребус - это задача, в которой картинками зашифровано слово. Данное определение ребуса уже всем давно известно. Теперь же ребус можно не редко увидеть и в другом контексте, когда говорят о чем-нибудь загадочном и неизведанном. Ребус играл очень важную роль в образовании письменности всех веков и народов, ведь даже пещерные люди писали на древних скалах рисунками, которые понимали только они, позже эти рисунки переходили впервые буквы названий этих рисунков. В России ребусы появились лишь в 1845 году. В современном ребусном письме есть множество знаков и правок, которые называются ребусным кодом, а сами значки можно называть кодовыми знаками. Это загадка, в которой, с помощью картинок, букв, слов, символов зашифровано слово или целая фраза.

Числовым ребусам уже почти тысяча лет. Впервые они появились в Китае, затем в Индии. В европейских странах числовые ребусы поначалу называли крипт-арифметические задачи. Их появление в Европе впервые было отмечено только в двадцатом веке, несмотря на то, что развитие математики началось много столетий назад.

Встречается упоминание о шифрах: Розовых рыцарей, масонские «Крестики-нолики», «Змейка», «Зоопарк», «А сегодня…», Виженера или пятисотлетнем шифре, «Сложенный лист», «Грандиозный алфавит» Мэтью Уайтекера, шифр «Бусинка» десятиклассницы одной из московских школ, флажковая азбука и много-много других невообразимых шифровок.

1.4 Криптография в других науках.

Кодирование или шифрование информации применяется не только в математике или информатике, но и в других науках. В географии шифрование используются как координаты местонахождения объекта, в биологии вся информация о человеке зашифрована в генетическом коде, прекрасная музыка зашифрована в нотах, художники скрывают информацию в своих неотразимых полотнах. Некоторые сведения о свойствах шифров и их применении можно найти и в художественной литературе, особенно в приключенческой, детективной и военной. Хорошее подробное объяснение особенностей одного из простейших шифров — шифра замены и методов его вскрытия содержится в известных произведениях: «Золотой жук» Э. По и «Пляшущие человечки» А. Конан Дойла, Ж.Верна «Путешествие к центру Земли», В.Каверин «Исполнение желаний», А.С. Пушкин «Евгений Онегин». Например, в романе Ж. Верна «Путешествие к центру Земли» в руки профессора Лиденброка попадает пергамент с рукописью из знаков рунического письма. Каждое множество α состоит из одного элемента. Элемент каждого множества выбирается из набора символов. В рассказе А. Конан Дойла «Пляшущие человечки» каждый символ изображает пляшущего человечка в самых различных позах. В романе Ж. Верна «Путешествие к центру Земли» каждый рунический знак был заменен на соответствующую букву немецкого языка, что облегчило восстановление открытого сообщения. В заключение рассказа о шифрах перестановки можно вспомнить историю с зашифрованным автографом А. С. Пушкина, описанную в романе В. Каверина «Исполнение желаний», где главный герой романа нашел в одном из секретных ящиков пушкинского бюро фрагмент недописанной X главы «Евгения Онегина». Льюис Кэрролл, автор знаменитой на весь мир «Алисы в Стране чудес» и «Алисы в Зазеркалье», преподавал математику в Оксфордском университете и выдумывал не только сказки, но и головоломки, математические загадки и игры. Именно ему принадлежит идея сделать «из мухи слона», «волка» превратить в «козу» и т.д. Большим любителем математики был также великий русский поэт М.Ю.Лермонтов. Он является автором любимого салонного развлечения с угадыванием задуманного числа путем преобразования множества арифметических действий.

Глава II Криптография в математике

2.1 Математические основы криптографии.

Методы и результаты различных разделов математики (в частности, алгебры, комбинаторики, теории чисел, теории алгоритмов, теории вероятностей и математической статистики) используются как при разработке шифров, так и при их исследованиях, в частности, при поиске методов вскрытия шифров. Криптография является богатым источником трудных математических задач, а математика — одной из основ криптографии. История показывает, что рано или поздно развитие математических методов и техники приводит к тому, что задачи, казавшиеся неразрешимыми, находят решение. Отставание в творческом соревновании математиков разных стран может привести к поражениям в экономике, дипломатии и военных операциях.

Хотя сами методы криптографии и криптоанализа до недавнего времени были не очень тесно связаны с математикой, во все времена многие известные математики участвовали в расшифровке важных сообщений. И часто именно они добивались заметных успехов, ведь математики в своей работе постоянно имеют дело с разнообразными и сложными задачами, а каждый шифр — это серьезная логическая задача. Постепенно роль математических методов в криптографии стала возрастать, и за последнее столетие они существенно изменили эту древнюю науку.

Понимание математического характера криптографии началось с работ все того же К. Шеннона. Его труд «Математическая теория криптографии» в секретном варианте появился в 1945 году. А рассекречен и опубликован был в США в 1949 году. В 1963 году по инициативе А. Н. Колмогорова сборник работ К. Шеннона был издан и на русском языке. Криптографические методы и средства защиты информации, а также их математические основы являются фундаментальными исследованиями, связывающими воедино области математики, информатики и физики.

Одним из разделов математики, который используется в криптографии, является комбинаторика. Она занимается разного рода наборами, которые можно образовывать из элементов некоего конечного множества. Некоторые элементы комбинаторики были известны в Индии ещё во II в. до н. э. Индийцы умели вычислять числа, которые сейчас называют «сочетаниями». В XII в. Баскара вычислял некоторые виды сочетаний и перестановок. Как научная дисциплина комбинаторика сформировалась в XVII в. Термин «комбинаторика» стал употребляться после опубликования Лейбницем в 1665 г. работы

«Рассуждение о комбинаторном искусстве», в которой впервые дано научное обоснование теории сочетаний и перестановок. Изучением размещений впервые занимался Я. Бернулли во второй части своей книги «Ars conjectandi» («Искусство предугадывания») в 1713 г. Современная символика сочетаний была предложена разными авторами учебных руководств только в XIX в.

Для криптографии важными являются такие алгоритмы комбинаторики как правило умножения, выборки и перестановки. На этих алгоритмах основываются способы формирования секретных ключей для симметричных шифров.

Криптосистемы разделяются на симметричные и с открытым ключом (ассиметричные). В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Заключение.

Подводя итоги нашему исследованию, можно сказать, что цель работы достигнута и получены следующие результаты:

• систематизированы знания научных источников по истории криптографии;

• проанализированы математические основы симметричной криптографии;

• расширены знания о существующих способах защиты данных и о преимуществах криптографической защиты информации;

Практической значимостью данной работы является привлечение внимания к изучению проблем защиты информации в общеобразовательной школе. Часть вопросов защиты информации может быть изучена в рамках школьной программы по информатике и математике, ведь наука криптография в наши дни получила новое развитие Простые криптоалгоритмы можно использовать для составления различных ребусов, головоломок на уроках математики и кружках по информатике в начальной школе и среднем звене.

Ход работы над проектом

Подготовительным этапом моей работы было определение темы проекта, выбор материала для реализации проекта, проведен опрос обучающихся 5-7 классов.

Анкета состояла из нескольких вопросов:

1. Знаете ли вы, что такое криптография?
2. Знаете ли вы, что такое шифр?
3. Пробовали ли вы что – то зашифровать?
4. Знакомы ли тебе шифры в математике?
5. Встречались ли тебе шифры в повседневной жизни?

Результаты анкеты показали, что 89% одноклассников не знают что такое криптография.

Все учащиеся знают, что такое шифр и пробовали зашифровать какую либо информацию.

11 % учащихся сказали, что им знакомы шифры в математике, и назвали такие: ребусы, перестановки.

Только 15 % одноклассников сказали, что встречали шифры в повседневной жизни, а если и встречали, то не обращали внимания.

Первым этапом было планирование работы: после проведения и обработки данных диагностики спланирована деятельность по реализации проекта, который сможет помочь одноклассникам видеть шифры в математике и повседневной жизни, использовать их для скрытия информации, выполнять задания с шифрами.

Следующим этапом была реализация проекта: на этом этапе состоялось создание собственного шифра, который поможет зашифровать какую - либо личную информацию. Были созданы математические задания, которые заключаются в шифровании и дешифровании информации. На этапе реализации проекта появился собственный шифр и сборник заданий по криптографии.

Приложение

Сборник заданий с использованием криптографии

Числовой ребус (шифр замена)

В буквенных ребусах каждой буквой зашифрована одна определенная цифра: одинаковые цифры шифруются одной и той же буквой, а разным цифрам соответствуют различные буквы. В ребусах зашифрованных, например, звездочками, каждый символ может обозначать любую цифру от 0 до 9. Причём, некоторые цифры могут повторяться несколько раз, а другие не использоваться вовсе. Перед началом решения математического буквенного ребуса (например, крипторифма), убедитесь, что в нём использовано не более 10 различных букв. В противном случае, такой ребус не будет иметь решений. Начните решение ребуса с правила, согласно которому ноль не может быть крайней левой цифрой в числе. Таким образом, все буквы и знаки, с которых начинается число в ребусе, уже не могут обозначать ноль. Круг поиска нужных цифр сузится. В ходе решения отталкивайтесь от основных математических правил. Например, умножение на ноль всегда дает ноль, а при умножении любого числа на единицу, мы получим в результате исходное число.

1)КРОССх2=СПОРТ

2)ПОДАЙ –ВОДЫ= ПАША

3) ОКУНЬ х 8 = СУДАК

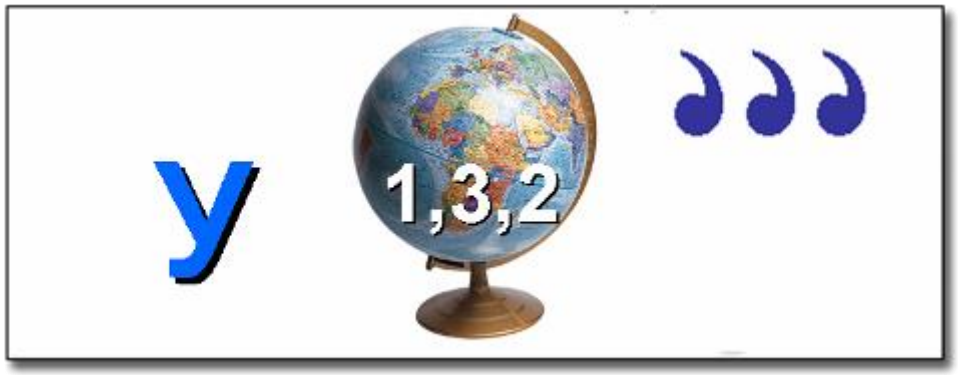
4) ДОМНА + ДОМНА + ДОМНА = ЗАВОД

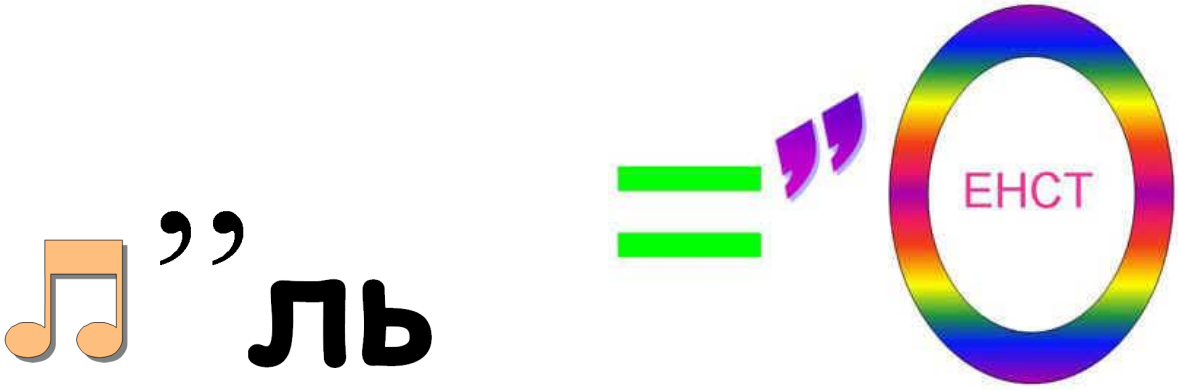
5) $(КИТ)^3 = МОНБЛАН$

6) ПОРТ х 3 = ТОРГ

7) СИНУС х 2 + КОСИНУС = ТАНГЕНС

8) (ЕМ)Д = ДОМ





- Найдите шифр, по которому текст «Красный арбуз» закодирован как «Нугфрюм гудцз» и закодируйте с помощью этого шифра текст «Информация». *(Лрчсупгщлв)*
- Догадайтесь, с помощью какого шифра слово «Остров» было закодировано как «Птуспг» и закодируйте с помощью этого шифра слово «Ключ». *(Лмяш)*
- Декодируйте слово «Еинаворидок». С помощью какого шифра оно было закодировано? *(«Кодирование», слово записано слева направо)*
- Расшифруйте послание. Какой шифр использовался для кодирования сообщения?

ВИПАСИ СВРВОФ ЕМЕЛБР ВИДЯО. ЕРСЮЙ ЩЕТТШ

(«Все вещи в мире представляют собой шифр.»)

М	о	м	з	о	л
б	а	р	ь	у	ф
з	я	о	к	у	к
р	у	ю	и	н	.
и	т		у	с	с
	ю	п	е		а

- Расшифруйте послание. Какой шифр использовался для кодирования сообщения?

(«Моряки используют семафорную азбуку», решетка Кардано)

- Расшифруйте послание. Какой шифр использовался для кодирования сообщения?

ВРЛСНР СОЯЕЫО ЯДЕКММ ПАТРШ. РЯСЕИ ИВЯТФ

(«Вся природа является секретным шифром»)

Л	а	д	г	е	В
р	е	о	и	а	л
н	н	к	ф	ч	а
р	и	и	р	и	е
д	в	й	п	о	л
!	т	д	а		о

- Расшифруйте послание. Какой шифр использовался для кодирования сообщения?

(«Леонардо да Винчи владел криптографией!», решетка Кардано)

- Расшифруйте послание. Какой шифр использовался для кодирования сообщения?

БУОКЮЧ УСЯОТЕ КСЗДРЛ ВКЫИЕО ЫОКРЧВ РГАУЬЕ

(«Буквы русского языка кодируют речь человека»)

Б	е	к	т	л	р
а	н	е	н	т	и
а	з	г	о	п	В
у	ш	и	и	Т	и

ж	с	ф	р	е	а
р	а	н	т	а	к

- Расшифруйте послание. Какой шифр использовался для кодирования сообщения?

(«Блез Виженер написал книгу трактат о шифрах, решетка Кардано)

- Робот придумал шифр для записи слов: заменил некоторые буквы алфавита однозначными или двузначными числами, используя только цифры 1, 2 и 3 (разные буквы он заменял разными числами). Сначала он записал шифром сам себя: РОБОТ = 3112131233. Зашифровав слова КРОКОДИЛ и БЕГЕМОТ, он с удивлением заметил, что числа вышли совершенно одинаковыми! Потом Робот записал слово МАТЕМАТИКА. Напишите число, которое у него получилось.

Решение

Рассмотрим слово РОБОТ = 3112131233. В нём 5 букв и 10 цифр, так что все коды двузначные и определяются без труда. Напишем все двенадцать возможных кодов и те буквы, которые мы точно знаем:

1 =	11 =	21 =	31 = Р
2 =	12 = О	22 =	32 =
3 =	13 = Б	23 =	33 = Т

Теперь подумаем, как запишется слово КРОКОДИЛ = БЕГЕМОТ. Начинается оно с Б = 13, то есть К = 1. Теперь мы можем записать начало слова: КРОКО... = 13112112...

Начинаем его читать как слово БЕГЕМОТ: Б = 13, Е ≠ 1, то есть Е = 11, а тогда Г = 2, иначе второе Е не получается. Ну а М начинается на 2, то есть М = 2*. Теперь посмотрим на конец слова, там ...ОТ, то есть ...1233. Это значит, что Л = 3 и И = 23, а Д заканчивается на 1, то есть Д = *1. Звёздочка – единственная оставшаяся неразгаданной цифра.

Разгадать её нетрудно: 31 = Р, 11 = Е, так что Д = *1 = 21. Тогда М = 22, и мы раскрыли почти весь шифр:

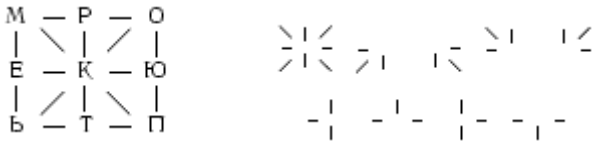
1 = К	11 = Е	21 = Д	31 = Р
2 = Г	12 = О	22 = М	32 =
3 = Л	13 = Б	23 = И	33 = Т

Теперь мы знаем всё, что нужно, чтобы записать шифром слово МАТЕМАТИКА, кроме одного – как шифруется буква А. Но раз Робот смог записать это слово, значит, для А должен найтись код. И этот код 32, ибо все остальные использованы.

Ответ

2232331122323323132.

- Попробуйте прочесть слово, изображённое на рис. 1, пользуясь ключом (см. рис. 2).



Подсказка

Не напоминают ли вам элементы ключа уменьшенные фрагменты основного рисунка?

Решение

Ключ показывает, какие именно стрелки отходят из того места, где стоит буква, которую мы должны выбрать. В результате прочитывается слово КОМПЬЮТЕР.

Ответ

КОМПЬЮТЕР.

- Найдите ключ к "тарабарской грамоте" — тайнописи, применявшейся ранее в России для дипломатической переписки: "Пайцике тсюг т "`камащамлтой чмароке"' — кайпонили, нмирепяшвейля мапее ш Моллии цся цинсоракигелтой неменилти".

Подсказка

Известный венгерский математик Д.Пойа в таких случаях предлагал смотреть на условие задачи до тех пор, пока решение само не придёт в голову. Найдите ключ к "тарабарской грамоте" - тайнописи, применявшейся ранее в России для дипломатической переписки:
Пайцике тсюг т "камащамлтой чмароке" - кайпонили, нмирепяшвейля мапее ш Моллии цся цинсоракигелтой неменилти.

Решение

Присмотревшись к напечатанному условию задачи, можно заметить, что в зашифрованной фразе и фразе, предшествовавшей ей, все гласные буквы совпадают, а согласные — распределены по парам и каждая буква из пары заменяет другую из той же пары. Это значит, что здесь зашифрована первая фраза условия задачи.

Ответ

Зашифрована первая фраза условия задачи.

- Как-то раз Таня ехала в поезде. Чтобы не скучать, она стала зашифровывать названия разных городов, заменяя буквы их порядковыми номерами в алфавите. Когда Таня зашифровала пункты прибытия и отправления поезда, то с удивлением обнаружила, что они записываются с помощью всего лишь двух цифр: 21221-211221. Откуда и куда шёл поезд?

Подсказка

Обратите внимание: название города, из которого шёл поезд, может состоять только из букв с номерами 1, 2, 11, 12, 21, 22.

Решение

На примере расшифровки названия первого города покажем способ рассуждений:

1. Первая буква либо *Б* (2), либо *У* (21).
2. Варианты для вторых букв: *БА* (21), *БК* (212), *УБ* (212), *УФА* (21221). Итак, возможный ответ — *УФА*, проверим, нет ли других.
3. Варианты для третьих букв: *БАБ* (212), *БАФА* (21221), *БКБА* (21221), *БКУ* (21221), *УБУ* (21221), *УББА* (21 221).
4. Следующие варианты: *БАББА, БАБУ*.

Таким образом, мы выяснили, что поезд идёт из Уфы, а куда — вы сможете определить сами, рассуждая аналогично. При этом должно получиться название города БАКУ.

Ответ

Уфа — Баку.

Заключение

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ. Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптографических преобразований информации.

Ситуация складывается так, что в недалёком будущем знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией. Поэтому вскоре криптография станет «третьей грамотностью» - по аналогии со «второй грамотностью», как называют владение компьютером и информационными технологиями. Проблема защиты информации очень актуальна в настоящее время и в России. У нас не хватает специалистов, которые занимались бы этой проблемой. Многие российские пользователи ПК имеют только поверхностное представление о проблемах защиты информации и поэтому относятся к защите информации попустительски, что часто приводит к серьезным проблемам.

Актуальность настоящей работы обуславливается возникшими противоречиями между возрастающими требованиями общества к уровню знаний молодого поколения в области защиты информации и современным состоянием процесса обучения в общеобразовательной школе по данному вопросу. Рассмотрение вопросов, связанных с данной тематикой носит как теоретическую, так и практическую значимость.
Высокая значимость и недостаточная практическая разработанность этой проблемы определяют несомненную новизну данного исследования.

Изучив материал по данной теме, я выяснила, что криптография – это наука, занимающаяся методами шифрования и дешифрования, она немыслима без анализа и синтеза, без сравнения и аналогии, а значит, математика больше всего подходит для этой науки. Подводя итоги, можно сказать, что цель работы достигнута и получены следующие результаты:

• получены и систематизированы знания по истории криптографии;

• проанализированы математические основы симметричной криптографии;

• расширены знания о существующих способах защиты данных и о преимуществах криптографической защиты информации;

Практической значимостью данной работы является привлечение внимания к изучению проблем защиты информации в общеобразовательной школе. Часть вопросов защиты информации может быть изучена в рамках школьной программы по информатике и математике, ведь наука криптографии в наши дни получила новое развитие. Алгоритмы шифрования можно использовать при изучении основ криптографии на уроках информатики, элективных курсах по информатике и математике.

В нашей жизни мы часто встречаем шифры. Их можно найти во многих областях: играя на музыкальных инструментах, читая литературные произведения, находя по координатам нужное место, изучая генетический код своего рода, общаясь с помощью азбуки Морзе. Я рассмотрела разнообразные виды шифров и попыталась создать свой, применяя полученные в ходе работы над проектом знания.

И это совсем не скучно, изучать криптографию. Надо только увидеть ее присутствие вокруг нас и понять, что она – наш добрый друг и помощник.

Список использованной литературы:

1. В. Волина. Веселая математика. М: ООО «Фирма «Издательство АСТ»», 1998г.
2. Я. Перельман. Живая математика. М: Издательство «Наука», 1967г.
3. В. Каверин. Собрание сочинений в 6 т., т. 2. («Исполнение желаний» С. 211–552). М.: Художественная литература, 1964г.
4. Э. По. Стихотворения. Проза («Золотой жук» С. 433–462). М.: Художественная литература, 1976г.
5. А. Конан Дойл. Записки о Шерлоке Холмсе. («Пляшущие человечки» С. 249–275). М.: Правда, 1983г.
6. Ж. Верн. Собрание сочинений в 12 т. («Путешествие к центру Земли» С. 7–225). М.: Художественная литература, 1995г.
7. Введение в криптографию. Под редакцией В. В. Ященко. Издание четвертое, дополненное. М: Издательство МЦНМО, 2007г.
8. Интернет-источники.