Муниципальное бюджетное

общеобразовательное учреждение

«Средняя общеобразовательная

школа №8»

**Математика и криптография**

Прикладная математика

**Работу выполнила**

Мошкова Кристина Андреевна,

обучающаяся 7А класса

**Руководитель**

учитель математики первой

квалификационной категории,

Двойникова Алла Юрьевна

Бердск, 2013

**Оглавление**

Введение…………………………………………………..………………………….3

1. Основная часть

1.1. Понятие криптографии…………………………………………………………4

1.2. История криптографии…………………………………………………...……..4

2. Шифры

2.1. Диск Альберти……………………………………………………………..……5

2.2. Шифратор Джефферсона…………………………………………………...…..5

2.3. Линейка Сен - Сира…………………………………………………………5-6

2.4. Шифровальная машина «Энигма»…………………………………………......6

2.5. Одноразовые блокноты………………………………………………................6

2.6. Шифр Гронсфельда……………….…………………………………………….7

2.7. Ребусы……………………………………………………………………..……..7

3. Решение задач………………………………………………………..………...8-11

4. Авторские задачи…………………………………………………………….....12

Заключение…………………………………………………………………….........13Список использованной литературы……………………………………………...14

Список использованных источников информации………....................................14

Приложение……………………………………………………………………..15-19

**Введение**

Работа «Математика и криптография» является продолжением моего проекта «Шифры и математика», с которым я выступала в 2012 году на городской НПК. Тема заинтересовала меня. Осенью 2012 года я участвовала в работе трёх вебинаров по подготовке к межрегиональной олимпиаде по математике и криптографии, и приняла участие в заочном и очном турах олимпиады. Олимпиада проходила для учащихся 8-11 классов, но мне разрешили в ней участвовать. Я решила 2 задачи из 6. С каждым годом я буду стараться усовершенствовать свой результат, т.к. диплом победителя или призера олимпиады является основанием для зачисления без экзаменов на специальности, связанные с информационной безопасностью, либо засчитывается 100 баллов за ЕГЭ по математике на другие специальности.

Приступая к работе над проектом, я поставила перед собой **цель**:

* Изучение истории развития криптографии и некоторых способов шифрования.

Для достижения цели мне нужно было выполнить следующие **задачи:**

* познакомиться с историей криптографии;
* изучить некоторые способы шифрования и дешифрования информации;
* научиться применять полученные знания при решении задач;
* познакомить одноклассников с методами решения задач по криптографии;
* придумать собственную задачу по криптографии.

1. **Основная часть** 
   1. **. Понятие криптография**

Криптография - это:

а) раздел прикладной математики, в котором широко используются теория чисел, комбинаторика, теория вероятностей;

б) специальная система изменения обычного письма, используемая с целью сделать текст понятным лишь для определенного числа лиц, знающих эту систему.

Цели криптографии:

а) защита данных или личной информации пользователя от несанкционированного просмотра;

б) защита данных от несанкционированного изменения;

в) проверка того, что данные исходят действительно от конкретного лица.

* 1. **. История криптографии**

История криптографии насчитывает уже не одну тысячу лет. По утверждению ученых криптография по возрасту – ровесница египетских пирамид.

В середине XVIII века русская криптологическая службы достигла европейского уровня и в некоторых моментах превосходила его. С этого времени русская криптология окончательно занимает одну из ведущих позиций в криптологии европейской и является эффективным орудием в руках дипломатических и военных ведомств страны.

Активное развитие криптографии в Европе пришлось на XVI-XVIII века. Этот период времени вошел в историю криптографии как эра «черных кабинетов»

«Черные кабинеты» - это специальные службы, которые занимались перехватом, шифрованием, дешифровкой информации. В них входили люди, агенты по перехвату писем, специалисты по имитированию почерка, по подделке печатей, переводчики и многие другие. Эти люди очень высоко ценились.

Слабость своих шифровальных систем Советы осознавали. Михаил Фрунзе информировал Москву: "Из представленного мне сегодня бывшим начальником врангелевской радиостанции Ямченко доклада устанавливается, что решительно все наши шифры вследствие их несложности расшифровываются врагами. Вся наша радиосвязь является великолепнейшим средством ориентирования противника".

Развитие письменности, созданной в IX веке болгарами Кириллом и Мефодием, содействовало применению криптографии на Руси.

Шифрование использовалось также в Библии. Некоторые фрагменты библейских текстов зашифрованы с помощью шифра, который назывался атбаш.

Криптография дошла и до нашего времени и сейчас является популярной, особенно в компьютерных технологиях.

1. **Шифры**

**2.1. Диск Альберти**

Для зашифрования текста использовался вращающийся диск, центр которого находится на оси, закрепленной на неподвижном основании. Диск разделен на 32 равных сектора, в которые в неизвестном порядке вписаны все буквы русского алфавита (по одной в каждый сектор; буквы Е и Ё не различаются). На основании, по одной напротив каждого сектора, выписаны буквы в алфавитном порядке по часовой стрелке. Каждое положение диска, получающееся из исходного поворотом на угол, кратный величине сектора, задает соответствие между буквами на основании и на диске.



* 1. **Шифратор Джефферсона**

Конструкция шифратора: деревянный цилиндр разрезается на 36 дисков. Эти диски насаживаются на одну общую ось таким образом, чтобы они могли независимо вращаться на ней. На боковых поверхностях каждого из дисков выписывались все буквы английского алфавита в произвольном порядке. Порядок следования букв на различных дисках - различный. На поверхности цилиндра выделялась линия, параллельная его оси. При шифровании открытый текст разбивался на группы по 36 знаков, затем первая буква группы фиксировалась положением первого диска по выделенной линии, вторая - положением второго диска и т. д. Шифрованный текст образовывался путем считывания последовательности букв с любой линии параллельной выделенной.



**2.3. Линейка Сен – Сира**

Свой собственный военно-полевой шифр был разработан военнной академией Сен-Сир, получивший название «Линейка Сен-Сира». Линейка представляет собой длинный кусок картона с напечатанными буквами алфавита. Эта последовательность букв называется «неподвижной шкалой». Под неподвижной шкалой, в линейке были сделаны вырезы, через которые перемещался «движок» с нанесенным на него тем же алфавитом. Алгоритм шифрования: полоска (движок) перемещается в положение, когда буква ключа-лозунга окажется под буквой «А» неподвижной шкалы. Образуется простая замена первой буквы открытого текста. При шифровании второй буквы открытого текста вторая буква ключа-лозунга путем передвижения движка встает под буквой «А» неподвижной шкалы и т. д. Таким образом, линейка Сен-Сира является простым механическим воплощением шифра Виженера.



**2.4. Шифровальная машина «Энигма»**

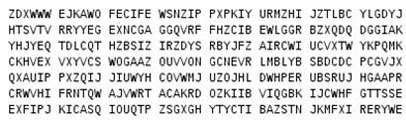
Шифровальная машина была создана немцами во время Второй Мировой войны. «Энигма» очень похожа на печатную машинку, её использовали в основном на фронте. Она состояла из трех частей соединенных кабелями: клавиатура, шифровальный механизм, состоявший из нескольких роторов, в

результате на панели с подсветкой загоралась буква кода. Перед началом работы шифровальщик устанавливал роторы в заранее условленную позицию, и таким образом задавалась определенная кодировка. Количество шифров производимых машиной около 70 триллионов.



**2.5. Одноразовые блокноты**

Одноразовые блокноты были изобретены в 1917 году Моборном и Вернамом. Одноразовый блокнот является большой неповторяющейся последовательностью символов ключа, распределенных случайным образом, написанных на кусочках бумаги и приклеенных к листу блокнота. Первоначально это была одноразовая лента. Отправитель использовал каждый символ ключа блокнота для шифрования только одного символа открытого текста. Шифрование представляет собой сложение по модулю 26 символа открытого текста и символа ключа из одноразового блокнота. Каждый символ ключа используется только единожды и для единственного сообщения. Новое сообщение – новые символы ключа.



**2.6. Шифр Гронсфельда**

Принцип этого шифра довольно прост: берется легко запоминаемый лозунг. При шифровании знаки текста вписываются под цифрами лозунга. Очередная буква открытого текста заменялась буквой алфавита, отстоящей от нее вправо на количество букв, равной соответствующей цифре лозунга.

**2.7. Ребусы**

Некоторые криптографические способы служат для игры в разгадывание или в так называемые ребусы. Предложение или слово зашифровывается с помощью картинок или условных знаков. Разгадывающему необходимо перебирать варианты и догадываться о смысле сообщения. Ребусы развивают логику и ассоциативное мышление.



Ответ: «хорошего человека должно быть много».

Ответ: «на словах густо, а в голове пусто».

1. **Решение задач**

**Задача №1:** В таблице приведена переписка двух абонентов (Годзиллы и

Фунтика) в чате.

|  |  |  |
| --- | --- | --- |
| **Дата/ время** | **Отправитель** | **Сообщение** |
| 10:11  28.11.2010 | Годзиллa | Привет**.** Как дела**?** Пришли пароль для почты**.** |
| 10:14  28.11.2010 | Фунтик | И усцрмс щюуьсэ ц Яспар**-**Дюрюмгщмт пс вцю пювючж**.** Дсмычз**:** Гщмтщпвжи**.** |
| 10:21  28.11.2010 | Годзиллa | Когда доберешься до Питера**,** позвони**.** |

Фунтик отвечает Годзилле и для конспирации каждую букву заменяет другой буквой (при этом разные буквы заменяются разными, а одинаковые – одинаковыми). Восстановите зашифрованное сообщение и пароль.

**Решение:** Отметим, что восстановить исходный текст короткого сообщения, зашифрованного с использованием такого шифра ( называемого шифром простой замены) не так-то просто. Помогает здесь то, что в сообщении сохранена разбивка на слова, оставлены знаки препинания и заглавные буквы. Если обратить внимание на сочетание Яспар**-**Дюрюмгщмт и содержащееся в ответе Годзиллы упоминание города Питера**,** то можно предположить, что речь идёт о Санкт**-**Петербурге. Составим таблицу соответствий:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ё | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |
| к |  |  | б | п |  |  |  |  |  |  |  |  | р |  |  | н | т | а | г |  |  |  |  |  | у |  |  |  |  |  | е | с |

В соответствии с этими заменами некоторые буквы в шифрованном тексте можно восстановить: **. .**А**.**ТРА УЕ**..**А**. .** САНКТ**-**ПЕТЕРБУРГ НА **..**Е НЕ**.**Е**.. .** ПАР**...:** БУРГУН**...** Далее подбираем некоторые слова по смыслу. Весьма вероятно, что **.**А**.**ТРА—это ЗАВТРА, ПАР**...—**это ПАРОЛЬ. С учётом этих предположений сообщение примет вид: **.** ЗАВТРА УЕЗ**.**А**.** В САНКТ**-**ПЕТЕРБУРГ НА **.**ВЕ НЕ**.**ЕЛ**. .** ПАРОЛЬ**:** БУРГУН**...** Затем по смыслу окончательно получаем искомое сообщение.

**Ответ:** Я завтра уезжаю в Санкт**-**Петербург на две недели**.** Пароль**:** Бургундия**.**

**Задача №2:** Для открытия подземелья в волшебной стране надо правильно назвать три целых числа *a,b,c,* служащих коэффициентами квадратичной функции *f(x) = ax2 +bx +c.* Представителям четырёх рас были переданы следующие значения функции: троллям – значение *f*(21), эльфам – *f*(24), гномам – *f*(25), оркам – *f*(28). Когда представители рас встретились, чтобы совместно найти *a,b,c,*  и открыть подземелье, один из представителей, чтобы сорвать мероприятие, предъявил неверное значение. Выясните, кто это был, если известно, что тролли предъявили число 273, эльфы – 357, гномы – 391, орки – 497.

**Решение:** Разность значений квадратичной функции должна делиться на разность значений аргументов. Проверим выполнение этого факта для различных пар значений: - для первого и второго: 357–273=84 делится на 3;

- для третьего и четвертого: 497–391=106 не делится на 3; следовательно, значение исказили или гномы, или орки;

 - для первого и третьего: 391–273=118 не делится на 4, следовательно, значение исказили тролли или гномы;

- для второго и четвертого: 497–357=140 делится на 4.

**Ответ:**  Гномы сообщили неверное значение

**Задача №3:** На клавиатуре мобильного телефона каждой кнопке сопоставлено по нескольку букв: кнопке 2 соответствуют буквы ABC, 3 – DEF, 4 – GHI, 5 – JKL, 6 – MNO, 7 – PQRS, 8 – TUV, 9 – WXYZ. Выбор нужной буквы определяется числом нажатий на кнопку. Например, нажав на кнопку 4 один раз, получим букву G, а два нажатия на кнопку 4 дадут или букву H (если нажимать быстро) или две буквы G (если нажимать с паузой).Известно, что при наборе пароля из 10 букв были нажаты последовательно кнопки 777255899999.

Определите число возможных вариантов паролей.

**Решение:** Обозначим через х число букв, получившихся при наборе цифры 7 (их может быть от 1 до 3), у – число букв при наборе цифры 5 (1 или 2) и *z* – число букв при наборе цифры 9 (от 2 до 5). Перечислим возможные варианты

представления числа 10 в виде суммы *x*+1+*y*+1+*z*: 1) 3+1+2+1+3; 2) 3+1+1+1+4; 3) 2+1+2+1+4; 4) 2+1+1+1+5; 5) 1+1+2+1+5. Для варианта 1 получить три буквы, нажимая 7, можно только одним способом; получить две буквы, нажимая 5, можно опять-таки только одним способом; а вот получить три буквы с помощью пяти девяток можно 6 способами. В итоге, для варианта 1 имеем 1 ×1×6 вариантов паролей, аналогично для варианта 2 будет 1×1× 4 вариантов паролей и т.д. Всего получаем 6+4+2×4+2+1=21 вариант.

**Ответ:** 21

**Задача №4:** Крокодил Гена посылает Чебурашке по радиоканалу сообщение, заменяя его буквы наборами из нулей и единиц согласно таблице (другие буквы не встретились).

|  |  |  |  |
| --- | --- | --- | --- |
| А (0,0,0,0,0,0,0) | Е (0,1,1,0,1,0,0) | Р (1,1,0,1,0,0,0) | Х (1,0,1,1,1,0,0) |
| В (1,1,1,0,0,0,1) | И (1,0,0,0,1,0,1) | С (0,0,1,1,0,0,1) | Ч (0,1,0,1,1,0,1) |
| Г (1,0,1,0,0,1,0) | М (1,1,0,0,1,1,0) | Т (0,1,1,1,0,1,0) | Ы (0,0,0,1,1,1,0) |
| Д (0,1,0,0,0,1,1) | О (0,0,1,0,1,1,1) | У (1,0,0,1,0,1,1) | Я (1,1,1,1,1,1,1) |

Из-за помех некоторые биты исказились, но не более двух в одном наборе. Определите, какое сообщение отправил крокодил Гена, если Чебурашка получил:

(1,0,0,1,0,1,1), (0,1,0,0,0,1,1), (0,0,1,0,0,0,0), (1,1,0,1,0,0,0), (1,0,1,0,1,1,0), (0,0,0,0,0,0,0), (0,0,1,1,0,0,0), (0,1,1,1,0,1,0), (0,0,1,0,1,0,0), (1,1,0,1,0,0,0), (0,0,0,0,0,0,1), (1,0,1,1,0,0,0), (0,1,1,1,0,1,0), (0,0,1,0,1,1,0), (1,0,0,0,1,0,1), (0,1,1,0,0,1,0), (0,1,1,1,0,1,0), (1,0,0,1,1,1,0), (0,0,1,1,0,0,1), (1,1,1,0,1,1,1), (0,1,0,1,1,0,1), (1,0,0,0,0,0,1), (0,1,0,0,0,1,1), (1,1,0,1,0,1,1), (1,0,0,1,0,1,1), (1,0,1,0,0,0,0), (1,0,0,0,1,0,1), (1,0,1,1,1,0,0), (1,0,0,0,0,1,0), (0,1,0,0,0,1,1), (1,0,0,0,0,1,0), (1,1,0,1,0,0,0), (0,0,0,0,1,1,1), (1,0,0,0,0,0,1).

**Решение:** по условию задачи в каждом наборе искажено не более двух бит. Заметим, что наборы из табл. 1, соответствующие различным буквам, отличаются по крайней мере в трех позициях. Отсюда следует, что искажение одного или двух битов в любом наборе из табл. 1, не делает его другим набором из табл. 1 (на это потребовалось бы по крайней мере три искажения). Значит все те наборы из письма Гены, которые соответствуют наборам из табл. 1, просто не были искажены. Выпишем, соответствующие им буквы: УД\*Р\*А\*Т\*Р\*\*Т\*И\*Т\*С\*Ч\*Д\*У\*ИХ\*Д\*Р\*\* (“\*” отмечены пока не известные буквы). Итак, уже имеется некоторая основа сообщения, которая поможет нам подобрать остальные буквы. Для восстановления третьей буквы требуется посмотреть, какие наборы из табл. 1 могли при искажении одного/двух битов стать набором (0,0,1,0,0,0,0), и выбрать тот набор, которому соответствует буква, подходящая по смыслу. Так, набор (0,0,1,0,0,0,0) мог быть получен из набора (0,0,0,0,0,0,0) (при искажении третьего бита) или из набора (1,0,1,0,0,1,0) (при искажении первого и седьмого битов) или из набора (0,0,1,1,0,0,1) (при искажении четвертого и седьмого битов). Очевидно, что по смыслу подходит только набор (0,0,0,0,0,0,0), соответствующий букве А. Аналогичным образом восстанавливаются остальные неизвестные буквы. В результате, получаем письмо Гены.

**Ответ:** удар мастера стоит тысячи других ударов

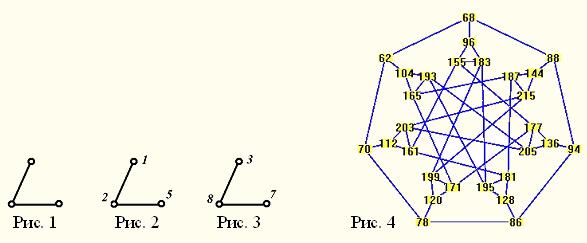
**Задача №5:** При передаче сообщения по факсу произошел сбой. В результате на листе было напечатано (изображение увеличено):



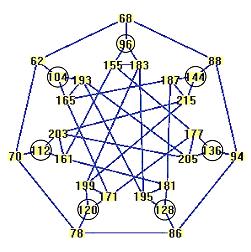
Восстановите текст (ответ обоснуйте). Известно, что исходный шрифт выглядел так: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

**Ответ:** Глобальное потепление.

**Задача №6:** Для зашифрования натурального числа *m*  используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединенные друг с другом, называют *соседними*. Зашифрование состоит в выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна *m*. Затем к числу в вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число  *m*. Пример: для зашифрования числа 8 будем использовать граф на рис. 1. В его вершины поместим числа, сумма которых равна 8 (рис. 2). Затем к каждому числу прибавим числа в соседних вершинах. Результат зашифрования указан на рис. 3. На рис. 4 приведен результат зашифрования некоторого числа. Найдите его.



**Решение:** Граф, используемый в задаче, обладает следующим свойством: из множества всех его вершин можно выделить такое подмножество *V* (отмеченное на рис. 5 кружочками), что любая вершина графа лежит в окрестности ровно одной вершины из *V*. Окрестностью вершины графа называют множество соседних с ней вершин, включая её саму. Очевидно, что искомое число равно сумме чисел, расположенных в вершинах из множества *V*:



**Ответ:** 840

**Задача №7:** В осмысленном сообщении на русском языке, записанном без знаков препинания и пробелов, переставили буквы. ПАИМРВЯСЕЕЬТЕТОЛДИНТ. Затем первую букву заменили на ту, которая следует за ней через некоторое число позиций в алфавите, выписанном по кругу, вторую букву – на ту, которая следует за ней через другое число позиций в алфавите и т. д., при этом одинаковые буквы могли перейти в разные, а разные – в одинаковые.

ИКЛМНОИКЛМНОИКЛМНОСТ. Затем эти буквы выстроили в исходном порядке ОИТМНИЛНСЛМКЛКМОКОНИ. Необходимо восстановить исходное сообщение.

**Решение:** выпишем все три набора букв в три строки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | А | И | М | Р | В | Я | С | Е | Е | Ь | Т | Е | Т | О | Л | Д | И | Н | Т |
| И | К | Л | М | Н | О | И | К | Л | М | Н | О | И | К | Л | М | Н | О | С | Т |
| О | И | Т | М | Н | И | Л | Н | С | Л | М | К | Л | К | М | О | К | О | Н | И |

Теперь берем букву из третьей строки, ищем её во второй и смотрим, какая буква стоит над ней.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **В** | П | Т | М | **Р** | **П** | И | Р | Н | **И** | **М** | **А** | И | А | М | В | А | В | Р | П |
| Т | Я | **Т** | **Е** | Ь | Я | Е | Ь | **Н** | Е | Е | С | **Е** | С | Е | Т | **С** | **Т** | **Ь** | **Я** |
| И | **Е** | Т | Л | Д | Е | **О** | **Д** | Н | О | Л | Т | О | **Т** | **Л** | **И** | Т | И | Д | Е |

**Ответ:** Ветер поднимает листья

1. **Авторские задачи**

**Задача №1:** При передаче сообщения по электронной почте произошел сбой. В результате на листе было напечатано (изображение увеличено):

C:\Users\Мы\Desktop\Новая папка (2)\готовое первая половина.jpg

C:\Users\Мы\Desktop\Новая папка (2)\2 часть.jpg

Восстановите текст (ответ обоснуйте). Исходный шрифт выглядел так:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

**Ответ:** Кто владеет информацией, тот владеет миром

**Задача №2:** В осмысленном сообщении на русском языке, записанном без знаков препинания и пробелов, переставили буквы ЕМИЦТМТАРАНИУАКАЦАКА. Затем первую букву заменили на ту, которая следует за ней через некоторое число позиций в алфавите, выписанном по кругу, вторую букву – на ту, которая следует за ней через другое число позиций в алфавите и т. д. При этом буквы ЁЙЪ в расчет не брались, а одинаковые буквы могли перейти в разные, а разные – в одинаковые. Получилось: ЯХЛЦПЧЬШХЖЮДЦЧЖБОЕОА. Затем эти буквы выстроили в исходном порядке ХЧПЯЧШЬЛЖАОЕХЛЦЖЮБЦО. Необходимо восстановить исходное сообщение.

**Решение:** выпишем все три набора букв в три строки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Е | М | И | Ц | Т | М | Т | А | Р | А | Н | И | У | А | К | А | Ц | А | К | А |
| Я | Х | Л | Ц | П | Ч | Ь | Ш | Х | Ж | Ю | Д | Ц | Ч | Ж | Б | О | Е | О | А |
| Х | Ч | П | Я | Ч | Ш | Ь | Л | Ж | А | О | Е | Х | Л | Ц | Ж | Ю | Б | Ц | О |

Теперь берем букву из третьей строки, ищем её во второй и смотрим, какая буква стоит над ней.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| М | М | Т | Е | М | А | Т | И | А | А | Ц | А | М | И | Ц | А | Н | А | Ц | Ц |
| Р | А | Т | Е | А | А | Т | И | К | А | К | А | Е | И | У | К | Н | А | У | К |

**Ответ:** Математика – царица наук

**Задача №3:**

****

**Ответ:** Криптография

**Заключение**

В настоящее время криптография присутствует во многих аспектах повседневной жизни. Такие явления, как мобильная связь, платное телевидение или интернет – коммерция не были бы возможны без применения криптографических методов, позволяющих гарантировать безопасность и неприкосновенность данных. Криптография необходима для сохранения тайны

электронного голосования и для того, чтобы голосовать могли только зарегистрированные пользователи и только единожды.

Изучая материал по теме «Математика и Криптография» я познакомилась с большим количеством теоритического материала, разобрала и смогла решить несколько типов задач по криптографии, составила собственные задачи.

Считаю, что представленные мной в этой работе задачи, можно использовать как дополнительный материал для подготовки учащихся к различного уровня олимпиад по математике и криптографии. В дальнейшем планирую научиться решать более сложные задачи по криптографии.

**Список использованной литературы**

1. Жарковская Н.А. Математический Кенгуру клуб: шифры и математика. СПб, 2006. Выпуск №14 (6-8 класс). 27 с.
2. //Занимательные головоломки. Коллекция логических игр от Deagostini №3 и. ООО «Де Агостини», Россия 2012. №6. 20 стр.//

**Список использованных источников информации**

1. Вебинары по подготовке к олимпиаде по математики и криптографии Сотрудника кафедры КИБЭВС Томского государственного университета систем управления и радиоэлектроники
2. Диск Альберти.// Система поддержки проведения интеллектуальных соревнований школьников и студентов:URL:http://www.cryptolymp.ru/

cryptolymp/archive\_task/423/2910/(2013. 10 фев.)

1. Линейка Сен-Сира.//История защиты информации: URL: http://odda19.narod.ru/Sen-Sir.html (2013. 13 февр.)

**Приложение №1**

**Интересные факты**

В ноябре 2012 года в Англии были найдены останки голубя вместе с капсулой с зашифрованным сообщением. Голубь был найден в камине. Все британские дешифровщики бились над загадочным сообщением целый месяц. Спустя месяц с головоломкой справился канадец Гордон Янг . Он разгадал всего за 17 мин. В работе ему помогала специальная книга по кодированию, доставшаяся рекордсмену от двоюродного дедушки. Он считает, что записка была написана в 1944 году. В послании было зашифровано расположение немецких войск. Британские дешифровщики не хотят признавать победу канадца.



**Числа Биля**

В 1817 году, охотясь на бизонов в штате Нью-Мексико, Томас Дж.Биль обнаружил золотое месторождение. За пару лет Биль нажил целое состояние, после смерти он оставил сундучок. Получатель Роберт Морис, открыв сундук, нашел в нем три криптограммы. Расшифровать их он не смог. В 1863 году Морис передал криптограммы Джеймсу Б.Уорду, он открыл ключ криптограммы номер два. Ключевым текстом оказалась Декларация независимости США. Криптограмма поведала о содержимом клада, оставленного Билем. Уорд, после 20 лет попыток «взломать» другие две криптограммы, решил опубликовать их. Братья Харт, Джордж и Клэйтон 15 лет

кропотливо изучали Декларацию независимости, Библию и другие известные тексты в надежде найти шифровальный ключ. В 1966 году банкир из штата Теннесси нанял бригаду землекопов с тяжелой техникой, буквально переворотившую земли, где, как предполагалось, было зарыто сокровище. Безрезультатно. В 1968 году была образована специальная Ассоциация по разрешению загадки давно умершего авантюриста. В 1971 году доктор Карл Хаммер провел анализ криптограмм с применением современных математических методов и пришел к выводу, что в закодированных сообщениях Биля имеются циклические шаблоны, свидетельствующие о том, что ряд чисел в них не случаен и, вероятнее всего, действительно содержит некую информацию.

**Приложение №2**

Со своей работой «Шифры и математика» я выступила перед учениками 3А класса. Всем ребятам очень понравилось расшифровывать пословицы с помощью квадрата Кардано, а некоторые даже заинтересовались темой «Шифры и математика».

|  |
| --- |
| L:\CIMG2021.JPG |
| C:\Users\Мы\Desktop\Новая папка (2)\DSC00462.JPG |
| C:\Users\Мы\Desktop\Новая папка (2)\DSC00477.JPG |

**Приложение №3**

Со своей работой «Математика и криптография» я выступила перед своими одноклассниками. Я предложила решить несколько задач и самим дома придумать 1-2 ребуса, зашифровав в нем одно из предложенных слов и словосочетаний: стеганография, криптография, шифрование, дешифровка,

одноразовые блокноты, шифратор, линейка Сен-Сира и Энигма.

|  |  |  |
| --- | --- | --- |
| L:\Кристина\CIMG2098.JPG | | L:\Кристина\CIMG2096.JPG |
| D:\Картинки\2013\07.03.13 8 марта школа\DSC00437.JPG | C:\Users\Мы\Desktop\Новая папка\Безимени-2.jpgC:\Users\Мы\Desktop\Новая папка\Безимени-1.jpg | |
| D:\Картинки\2013\07.03.13 8 марта школа\DSC00439.JPG | C:\Users\Мы\Desktop\Новая папка\маша1.jpgC:\Users\Мы\Desktop\Новая папка\маша2.jpg | |
| D:\Картинки\2013\07.03.13 8 марта школа\DSC00441.JPG | C:\Users\Мы\Desktop\Новая папка\Безимени-3.jpg | |
| D:\Картинки\2013\07.03.13 8 марта школа\DSC00460.JPG | C:\Users\Мы\Desktop\Новая папка\Миша.jpg | |

|  |  |
| --- | --- |
| C:\Users\Мы\Desktop\Безимени-4.jpg | |
| D:\Картинки\2013\07.03.13 8 марта школа\DSC00459.JPG | |
| C:\Users\Мы\Desktop\DSC00480.jpg | C:\Users\Мы\Desktop\Безимени-7.jpg |