Криптограммы в прошлом и настоящем

Анастасия Соколова
8 – 3 КЛАСС
МОУ «СОШ № 151»
Г. ОМСК
под руководством учителя математики В.Ф.Краус

Оглавление:

Введение:

- **Выбор темы «Криптограммы в прошлом и настоящем» был обусловлен тем, что я хотела больше узнать о криптограммах, что это такое, где их можно использовать в настоящем. Как и где произошли первые тайнописи, научиться составлять и читать криптограммы, научиться работать с компьютером, составлять презентации.**
- **Цель исследования:**

Систематизировать исторические сведения о криптограммах.

Изучить различные способы составления криптограмм.

Выявить связь криптограмм с математикой.

- **Задачи:**

1. В стихотворной форме рассказать о криптограммах.

2. Найти исторический материал и составить диаграмму.

3. Различными способами составить криптограммы.

4. Представить отчет о работе в виде презентации.

История развития криптографии

**КРИПТОГРАФИЯ – НАУКА,
ТУТ ТАКАЯ В МИРЕ ШТУКА -
ЕЙ ДАВНО УВЛЕЧЕНЫ
И НИ ГОД, НИ ДВА, НИ ТРИ**

Криптография древнего периода

- Криптография **возникла вместе с письменностью**. В исторических документах древних цивилизаций Индии, Египта, Месопотамии имеются сведения о системах и способах составления шифрованного письма. Так, в древнеиндийских рукописях содержится **изложение 64-х способов преобразования текста**. Среди них написание знаков не по порядку, а вразброс по некоторому правилу. Многие из приводимых способов следует рассматривать как криптографические, т. е. **обеспечивающие секретность переписки**. Приведена система замены букв. Упоминается, что тайнопись является одним их 64-х искусств, которым следует владеть как мужчинам, так и женщинам. Более достоверные сведения о применяемых системах шифров относятся к периоду возникновения государств древней Греции. **В Спарте в V--VI веке** до нашей эры существовала хорошо развитая криптография. К этому времени относятся описания двух известных **приборов для шифрования --- Сцитала и таблица Энея**, которые осуществляют перестановку букв в тексте и замену букв открытого текста отрезками на прямой. Эней в сочинении "Об обороне укрепленных мест" описывает так называемый "книжный шифр". Полибий описывает систему шифра, называемую **"квадрат Полибия",** представляющую собой замену каждой буквы парой чисел --- координатами буквы в квадрате 5x5, в котором написаны буквы алфавита. **Юлий Цезарь** в книге "Записки о галльской войне" описывает шифр, в котором буквы заменяются в соответствии с подстановкой, в которой каждая буква сдвинута на три позиции вправо.

  В математике этого периода накапливается материал, относящийся к началам арифметики и геометрии. *В этот период появляются правила вычисления площади треугольника и трапеции, объемы пирамиды с квадратным основанием, правила решения простейших квадратных уравнений, теорема Пифагора и формула для суммы арифметической прогрессии.*


Криптография арабского мира

В период расцвета арабских государств (VIII век н. э.) криптография получила новое развитие. **Слово "шифр" арабского происхождения, так же как и слово "цифра".** В 855 году появляется **"Книга о большом стремлении человека разгадать загадки древней письменности**", в которой приводятся описания систем шифров, в том числе и с применением нескольких шифроалфавитов. **В 1412 году издается 14-томная энциклопедия, содержащая обзор всех научных сведений** --- "Шауба аль-Аша". Составитель ее Шехаб аль Кашканди. В данной энциклопедии содержится раздел о криптографии, в котором приводятся описания всех известных способов шифрования. В этом разделе имеется упоминание о криптоанализе системы шифра, который основан на частотных характеристиках открытого и шифрованного текста. Приводится частота встречаемости букв арабского языка на основе изучения текста Корана.

Что касается *математики* арабского мира, то следует упомянуть следующие выдающиеся достижения. *Сочинение Мухаммеда бен Муса аль-Хорезми (IX век) по правилам арифметики в позиционной системе счисления, от названия которого появились два термина "алгебра" и "алгоритм". Трактат по тригонометрическим функциям Аль-Баттани (IX век). Вычисление числа "пи" с 17 десятичными знаками (ок. 1427) аль Каши, сотрудником Улугбека.*



Криптография в эпоху Возрождения (XIV--XVI вв.)

До эпохи Возрождения имеется мало сведений о применяемых шифрах. Известен ряд значковых шифров, при котором буквы открытого текста заменяются на специальные знаки. Таким является **шифр Карла Великого (780--814 г.).** Известен так называемый **"еврейский шифр",** в котором замена букв осуществляется по подстановке, в которой нижняя строка образуется так: алфавит разбивается на две половины. Буквы второй половины пишутся под буквами первой половины в обратном порядке. Аналогично поступают с остальными буквами. В 1466 году Леон Альберти, знаменитый архитектор и философ представил трактат о шифрах в папскую канцелярию. В трактате рассматриваются различные способы шифрования, в том числе маскировка открытого текста в некотором вспомогательном тексте. Работа завершается собственным шифром, который он назвал **"шифр, достойный королей".** Это был многоалфавитный шифр, реализованный в виде шифровального диска. Суть заключается в том, что в данном шифре используется несколько замен в соответствии с ключом. Позднее Альберти изобрел код с перешифровкой. Данное изобретение значительно опередило свое время, поскольку данный тип шифра стал применяться в странах Европы лишь 400 лет спустя.

Прогресс *в математике* в этот период характеризуется *трудами Леонардо Фибоначчи, в которых излагается арифметика, алгебра и геометрия. Для вычислений используется сходимость геометрической прогрессии. Н. Орем установил расходимость гармонического ряда, строгое доказательство этого появится только в XVII веке. Кардано при решении уравнений третьей степени вводит отрицательные и мнимые корни и устанавливает известную "формулу Кардано".*


Криптография в XVII – XVIII веках

XVII век называют эрой "черных кабинетов", поскольку в этот период создаются **дешифровальные службы**. Так, в Англии Оливер Кромвель создает "Интеллиженс сервис" --- **разведывательную службу**, в которой появляется дешифровальное отделение. В середине XVII века к дешифровальной работе привлекается известный математик Джон Валлис (1616--1703). Он является автором фундаментального труда "Арифметика бесконечного" (1655). Хорошо известна "формула Валлиса", дающая представление числа "пи" в виде бесконечного произведения. Во Франции при Людовике XIV по предложению кардинала Ришелье создается дешифровальное отделение, которое возглавил Антуан Россиньоль. Россиньолю принадлежит доктрина: **стойкость военного шифра должна быть такой, чтобы обеспечить секретность донесения в течение срока, необходимого для выполнения приказа** Криптография в России развивалась по пути христианских стран. Датой появления криптографической службы следует считать **1549 год (царствование Ивана IV), с момента образования "посольского приказа", в котором имелось "цифирное отделение".** Используемые шифры --- такие же как в западных странах --- значковые, замены, перестановки. **Петр I** полностью реорганизовал криптографическую службу, создав **"Посольскую канцелярию".** В это время применяются для шифрования коды, как приложения к "цифирным азбукам". В знаменитом "деле царевича Алексея" в обвинительных материалах фигурировали и "цифирные азбуки".

Математика XVII--XVIII века получает существенное и качественно новое развитие. Н. Бурбаки называют этот период "героической эпохой". Назовем только некоторых авторов открытий. Изобретатель логарифмов --- Дж. Непер, шотландский математик, его "Описание удивительной таблицы логарифмов" было издано в 1614 году. Декарт Рене, французский математик, заложил основы аналитической геометрии. Его фундаментальный труд "Геометрия" вышел в 1637 году. Блез Паскаль (1623--1662), французский физик и математик. Получил ряд результатов по комбинаторике ("треугольник Паскаля") и геометрии ("теорема Паскаля"). Открыл метод доказательства по индукции. Ньютон Исаак (1643--1727) --- английский физик и математик и Готфрид Лейбниц (1646--1716) --- немецкий философ и математик разработали дифференциальное и интегральное исчисление. Не имеется данных о привлечении этих математиков к шифровальной работе, но есть данные о том, что некоторые их них владели криптографией (Паскаль, Ньютон, Лейбниц).

Криптография в XIX веке

В 1819 году во Франции выходит энциклопедия, в которой приведены известные к тому времени системы шифров и методы дешифрования простейших шифров. В **1844 году С. Морзе изобрел телеграф.** В России телеграф был изобретен П. Ф. Шиллингом в 1832 году. Шиллингу также принадлежит изобретение биграммного шифра. В Англии изобретение биграммного шифра приписывается министру почт при королеве Виктории Леону Плейферу. Изобретение телеграфа оказало существенное влияние на криптографию. Сразу же был опубликован коммерческий код под названием "**Словарь для тайной корреспонденции; приспособлен для применения на электромагнитном телеграфе Морзе".** Развитие коммерческих кодов повлияло и на развитие дипломатических кодов. Специалисты в области шифрованной связи пришли к пониманию, что необходима иерархия в шифрованной связи. Для каждого уровня иерархии требуется своя система шифра. Возрастание скорости передачи потребовало возрастания скорости шифрования. В 1863 году офицер прусской армии майор Фридрих Казисский опубликовал книгу под названием **"Искусство тайнописи и дешифрования", в которой новым вкладом в криптографию было изложение метода вскрытия многоалфавитного шифра с повторяющимся лозунгом на примере шифра Виженера,** который ранее считался недешифруемым. Казисский предложил метод статистического определения числа букв в лозунге, который основан на следующей идее: повторяемость букв в лозунге вместе с повторяемостью букв в открытом тексте дает повторяемость букв в шифрованном тексте. Автор пришел к выводу, что расстояние между повторениями в шифртексте будут равны или кратны периоду лозунга, т. е. его длине. После определения длины лозунга шифрОтекст разбивается на отрезки, равные длине лозунга, и исходная задача сводится к дешифрованию простой замены. Данный метод дешифрования стал называться **"методом Казисского".** В 1883 году появился крупный научный труд под названием "Военная криптография", его автор Огюст Кергоффс, преподаватель иностранных языков и математики во Франции. В данной книге проводится сравнительный анализ шифров. Задача автора --- сформулировать требования к шифрам, применительно к использованию новых средств связи. Он делает вывод, что практический интерес представляют те шифры, которые остаются стойкими при интенсивной переписке.

- Другой его вывод: только криптоаналитики могут судить о качестве шифра. Кергоффс впервые делает различие между секретностью шифрсистемы и секретностью ключа. И вводит требование секретности по ключу и не требует секретности системы. Это требование сохраняет свое значение и в современной криптографии. Важное событие в криптографии было связано с именем французского офицера Э. Базери, который отрицательно относился к официальным шифрам и предложил несколько собственных систем шифров. Одна из них --- это по сути шифратор Джефферсона. **С 80-х годов XIX века криптография во всех ведущих государствах считается наукой и ее изучают в военных академиях.** Для шифрования применяются коды с перешифровкой. Созданы и используются механические устройства для шифрования. Нет свидетельств, относящихся к данному периоду, о привлечении крупных математиков для криптографической работы.
- *Математика XIX века характеризуется революционными открытиями, ломающими привычные представления. В первую очередь следует назвать открытие Н. И. Лобачевским неевклидовой геометрии. Его сочинение " О началах геометрии " было напечатано в журнале "Казанский вестник" в 1829 году.*

Криптография в XX веке

- XX век --- век двух мировых войн, век научно-технического прогресса, век социальных потрясений и передела государственных границ. В этом веке криптография стала электромеханической, затем электронной. Это означает, что основными средствами передачи информации стали электромеханические и электронные устройства. Это преобразило всю криптографию, поскольку расширились возможности доступа к шифрованному тексту и появились возможности влияния на открытый текст.
- Война преобразила криптографию. В связи с применением радио для управления войсками расширились возможности добычи шифртекста. В этот период получили развитие методы дешифрования, основанные на парах открытых и шифрованных текстов, на шифртекстах, полученных на одном ключе, на использовании вероятных ключей. **Находкой для криптографов было использование в качестве лозунгов пословиц, поговорок, патриотических призывов**. В математическом плане получили развитие вероятностно-статистические методы, использующие частоту знаков, биграмм, триграмм и т. д.



- Между мировыми войнами появляются во всех ведущих странах электромеханические шифраторы. Они были двух типов --- на коммутационных дисках или роторах и на цевочных дисках. Примером первого типа является известная шифрмашина "Энигма", которой были оснащены германские сухопутные войска. Примером второго типа является американская шифрмашина М-209. Коммутационный диск представляет собой полый диск с нанесенными с двух сторон контактами, соответствующими алфавитам открытого и шифрованного текста, причем они соединены между собой по некоторой подстановке, называемой коммутацией диска. Эта коммутация определяет замену букв в начальном угловом положении. При изменении углового положения диска изменяется соответствующая замена на сопряженную подстановку. Шифратор представляет собой устройство из коммутационных дисков и механизма изменения их угловых положений. Шифратор "Энигма" состоял из 4-х коммутационных дисков, которые изменяли свои угловые положения по принципу "счетчика". Она имела несколько модификаций. Одну идею в криптографическом отношении можно считать революционной --- каждый диск дважды участвовал в шифровании, что усложняло анализ шифра. Шифрмашина М-209 состояла из 6 колес размера 26, 25, 23, 21, 19, 17, каждое из которых имело выступы и по окружности. Эта 6-мерная комбинация выступов (их число 64) с помощью механического устройства превращалась в число, на которое сдвигается буква открытого текста. Изменение угловых положений дисков осуществлялось равномерным их вращением. Ясно, что шифратор реализует шифр гаммирования. Советский Союз производил шифрмашины обоих названных типов. Таким образом, перед второй мировой войной все ведущие страны имели на вооружении электромеханические шифрсистемы, обладающие высокой скоростью обработки информации и высокой стойкостью. Считалось, что применяемые системы недешифруемы и наступил конец криптографии.



О криптографии нового времени

Начиная с 50-х годов криптография становится "электронной". Это означает, что широкое применение средств электронной техники для построения систем шифров и их исследования. Возможности применения электронной памяти позволили осуществлять обработку открытых текстов целыми отрезками (блоками) и это вызвало применение так называемых блочных шифров. С 70-х годов сфера применения криптографии начинает расширяться, криптография становиться гражданской отраслью. Это означает, что криптографические средства начинают применяться для защиты коммерческой информации. Для этих целей в США в 1978 году был принят стандарт шифрования данных DES, который является блочным шифром с длиной блока 64 бит. Этот процесс получил развитие и в настоящее время все развитые страны имеют свои стандарты шифрования. Разработан криптографический алгоритм IDEA, который рассматривается в качестве кандидата для международного стандарта шифрования.

- В 70-х годах американские ученые Диффи и Хеллман предложили использовать так называемые системы с открытыми ключами, в которых нет канала для распространения ключей, но есть возможность двустороннего обмена информацией между отправителем и получателем. Фиксированная процедура такого обмена позволяет выработать общий секретный ключ. В этот период были предложены несколько систем с открытыми ключами. Среди них --- система RSA, названная так по первым буквам ее авторов --- Райвест, Шамир, Адлеман, в которой открытые сообщения кодируются натуральными числами, а операция шифрования заключается в возведении в степень числа, представляющего открытый текст, и в приведении полученного числа по некоторому модулю. Дешифрование данной системы представляет собой известную математическую задачу "дискретное логарифмирование", для которой к настоящему моменту не найдено эффективных алгоритмов.



- Данные идеи оказались плодотворными. Во-первых, они расширили область средств , применяемых для обоснования шифров. Во-вторых, способствовали притоку математиков к решению криптографических проблем. В-третьих, привели к возникновению новых направлений криптографии. Например, процедура обмена информацией при выработке общего ключа привела к понятию криптографического протокола. В-четвертых, они привели к появлению новых направлений в дискретной математике. Например, возникло понятие однонаправленной функции, для которой имеется простой алгоритм вычисления значения функции, но сложно вычисляется значение аргумента по значению функции. В заключение два слова о будущем криптографии. Ее роль будет возрастать в связи с расширением ее областей приложения (цифровая подпись, аутентификация и подтверждение подлинности и целостности электронных документов, безопасность электронного бизнеса, защита информации, передаваемой через Интернет и др.). Знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией, поэтому **криптография в будущем станет "третьей грамотностью" наравне со "второй грамотностью"** --- владением компьютером и информационными технологиями.

ЕКИТАМЕТАМИЯСТАЧУЕНИК ИТАММАРГИВКУБЗЕБ

$$\begin{pmatrix} 1 & 2 \dots & 37 \\ 37 & 36 \dots & 1 \end{pmatrix}$$

ИКИТАММАРГИВКУБЗЕБ
ЕКИТАМЕТАМИЯСТАЧУЕН

$$\begin{pmatrix} 1 & 2 \dots & 18 & 19 & 20 \dots & 37 \\ 18 & 17 \dots & 1 & 37 & 36 \dots & 19 \end{pmatrix}$$

**Я ИСТОРИЮ УЗНАЛА,
МНОГО КНИГ ПЕРЕЧИТАЛА
И ТЕПЕРЬ ЛЕГКО СМОГУ
РАЗГАДАТЬ ШИФРОВКУ ТУ**

ТОТ ШИФРОВКУ ПРОЧИТАЕТ
КТО БЫСТРЕЕ КЛЮЧ УЗНАЕТ
БУКВУ ЦИФРОЙ ЗАМЕНЯЙ
И ЗАГАДКУ ЗАГАДАЙ

КТО ЗАГАДКУ УГАДАЕТ
ЧИСЛО БУКВОЙ ЗАМЕНЯЕТ
КТО ШИФРОВКУ ПРОЧИТАЛ
ТОТ СЕКРЕТЫ ВСЕ УЗНАЛ

7	12	17	15	18
в	е	с	т	ь

Сообщение

11	19	3	10	16
к	а	л	ы	м

выкуп за невесту

4	1	2	19	3	6
п	у	г	а	л	о

Огородное страшило

14	6	13
ж	о	р

Прекрасный клев рыбы

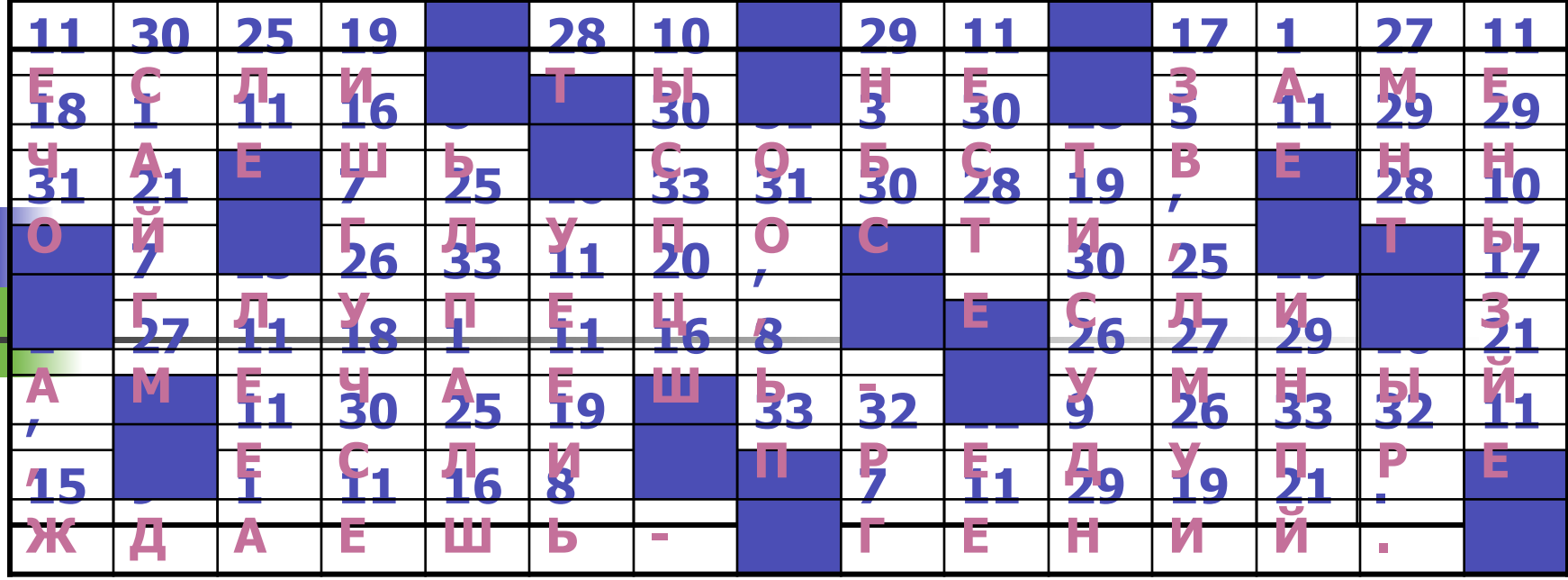
9	19	13	8
з	а	р	я

«Вставать ни свет ни …»

1	2	3	1	4	5	6	7	8	9	10	11
у	г	л	у	п	ц	о	в	я	з	ы	к
	4	12	13	12	14	19	12				
о	п	е	р	е	ж	а	е	т			
			16	10	17	3	18	.			
			м	ы	с	л	ь	.			

5	1	2
ц	у	г

Упряжка лошадей



Омская газета «Класс» Напечатала про нас. Вильни извилиной - давай, Криптограмму отгадай!

- *1} 28, 11, 27, 33. 11, 32, 1, 28, 26, 32, 1 - как и давление, она нормальной тоже должна быть,*
- *2) 9, 1. 7. 1 - этот летний теремок, закрыт зимою на замок,*
- *30, 31. 25. 31, 27, 1 — мягкая подстилка для будущего падения,*
- *9, 11. 29, 8, 7, 19 — средство от недостатка.*
- *5. 31, 30. 23 в церкви для свечей он служит, пчелам он для мёда нужен.*
- *11. 15. 11. 5, 19. 23. 1 ягода, но не малина, не клубника, не калина, у неё чернильный цвет, но не черника это, нет.*
- *7) 3. 26. 23, 11, 28 — красивый, неясный, ароматный, подарок очень он приятный.*
- *8) 16. 19. 33 - колючка розы.*
- *9) 9. 11, 29. Я с зарей родился, чем больше рос, тем меньше становился.*
- *10} 32. 10. 3. 1 у .маленькой скотинки, 100 серебряных монеток в спинке.*
- *27. 11. 30., 2, 20 то блин, то полблина, то та, то эта сторона.*
- *28. 1,21,29, (2,23 в помещении много лет, можно там хранить секрет. Оно было во дворцах, и в старинных крепостях.*
- *11. 7, 31, 17, 1 — непоседлив коль ребёнок, как зовут его с пеленок?*

Расшифровав ключевые слова и подставить вместо цифр соответствующие буквы вы, прочтёте замечательный афоризм Станислава Ежи ***Левца.***

2	Б	19	10	У	2	Б	В		19	16	Е	Д	У	Е	10
	9	7		М	20	19	16	21	12	,		8	Б		
	17	Б	Р	Е		8	7	Ы	,		Е	19	16	22	
	Б	8		Е	15		Б	Ь	17	Б	8	З	Е	10	.

«Ореол» газета взрослых
И печатает как раз
Изреченье - высший класс!
Дешифруешь их сейчас
И узнаешь мудрость глас.

КЛЮЧЕВЫЕ СЛОВА

- **9, 22,10, 7 - имя одной из сестёр в знаменитом индийском фильме.**
- **17, 5,16,1,14, 21 - птица, преимущественно с серо-голубым или белым**
- **оперением.**
- **19, 10, 4, 16, 7 - вертикальный памятный знак, обычно с надписью,**
- **рельефным изображением.**
- **12, 8,17, 7 - матрос-подросток.**
- **3, 22,6 - российский бард.**
- **19,10, 20,11 - чувство сильного смущения от сознания вины.**
- **2,13,10,15,18, 3, 7 - отличная школьная оценки**

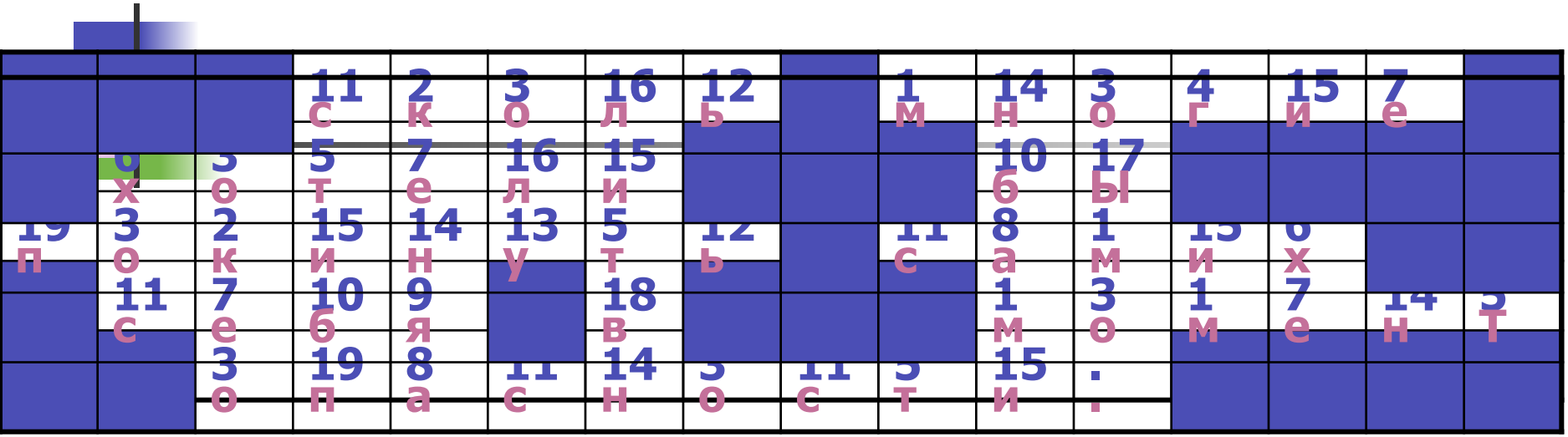
КРИПТОГРАММА составленная учеником 12 класса ВСО школы №3 Суриковым Дмитрием

Расшифровав ключевые слова и подставив вместо цифр соответствующие буквы вы, прочтёте замечательный афоризм

к	т	о		о	б	л	а	д	а	е	т
	т	е	р	п	е	н	и	е	м	,	
м	о	ж	е	т		д	о	с	т	и	ч	ь
	в	с	е	г	о	.					
Ф	р	а	н	с	у	а		Р	а	б	л	е

КЛЮЧЕВЫЕ СЛОВА

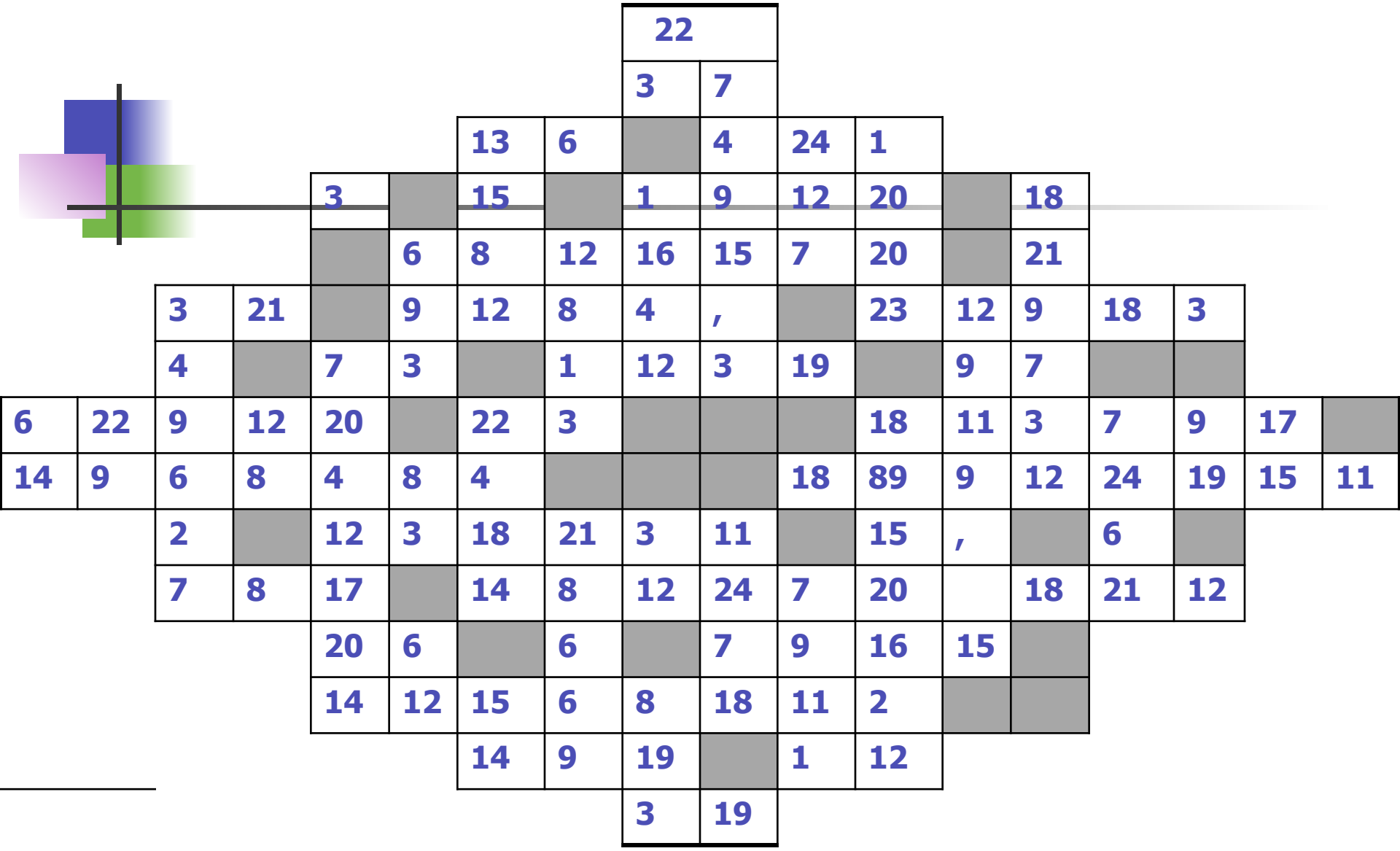
- **13, 10, 6, 12 – ПАЖ НА ЗАПЯТКА.**
- **13, 3, 16, 17, 18 – ГЛАВНЫЙ СОЛИСТ СРЕДИ МИНЕРАЛОВ.**
- **18, 3, 18, 15, 19, 3 – ВОРОВСТВО НА СТАРОРУССКИЙ ЛАД.**
- **19, 2, 7, 3 – КУПЮРА ПЕНСИОННОГО ВОЗРАСТА.**
- **20, 3, 4, 17, 18, 17 –ОЛЕНЬ ИЗ БЛАГОРОДНЫХ.**
- **16, 15, 7, 2, 20, 2, 21 – КТО РАСТИТ ДОЛГУНЕЦ.**
- **20, 5, 1, 10, 17, 1 – ИСТЕРИЧЕСКАЯ НОТКА В ГОЛОСЕ.**
- **8, 3, 5, 2, 7 – МОДНЫЙ КАПРИЗ.**
- **21, 9, 11, 12 – ЖЕЛЕ К ЧАЮ.**
- **18, 3, 14, 1, 3 – КОЛЕСНИЦА ДАЧНИКА.**

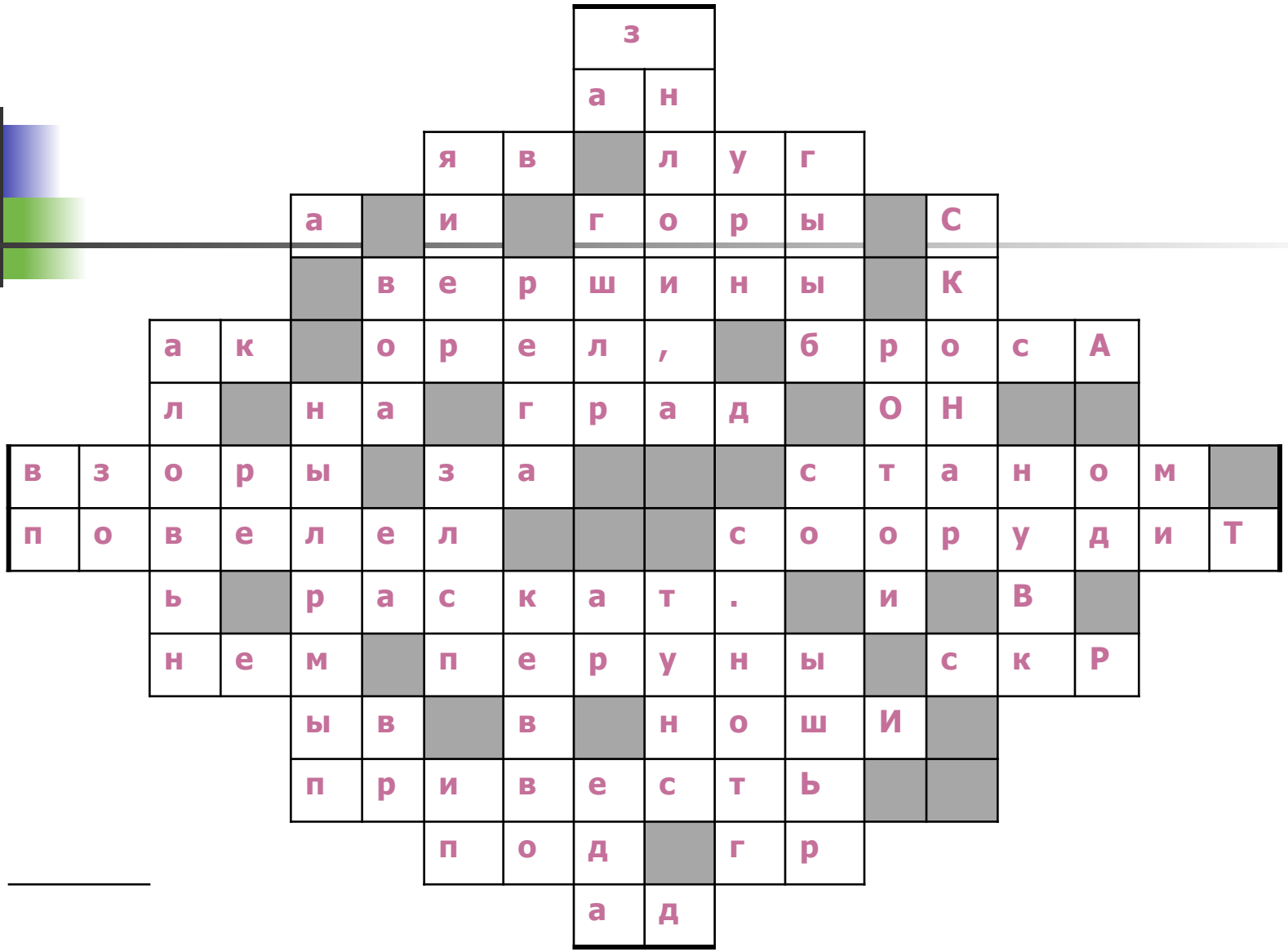


- 19, 12, 7, 6, 8, - российская эстрадная певица,
- 1, 13, 16, 8, 5 - потомок от брака белого человека с негром,
- 10, 8, 16, 8, 14,11 - равновесие, уравновешивание,
- 9, 10, 16, 3, 2, 3 - согласно греческой мифологии, этот фрукт явился причиной раздора между богинями Герой, Афиной и Афродитой,
- 18, 17, 2, 13, 19 - плата за освобождение пленного, невольника или преступника,
- 3, 4, 3, 14,12 - с ним лучше не играть, так как это чревато опасными последствиями.

Все шифровки разгадала
и придумала сама
Криптограммы раз, да два,
вот и три и рядом пять
можно книжку создавать.

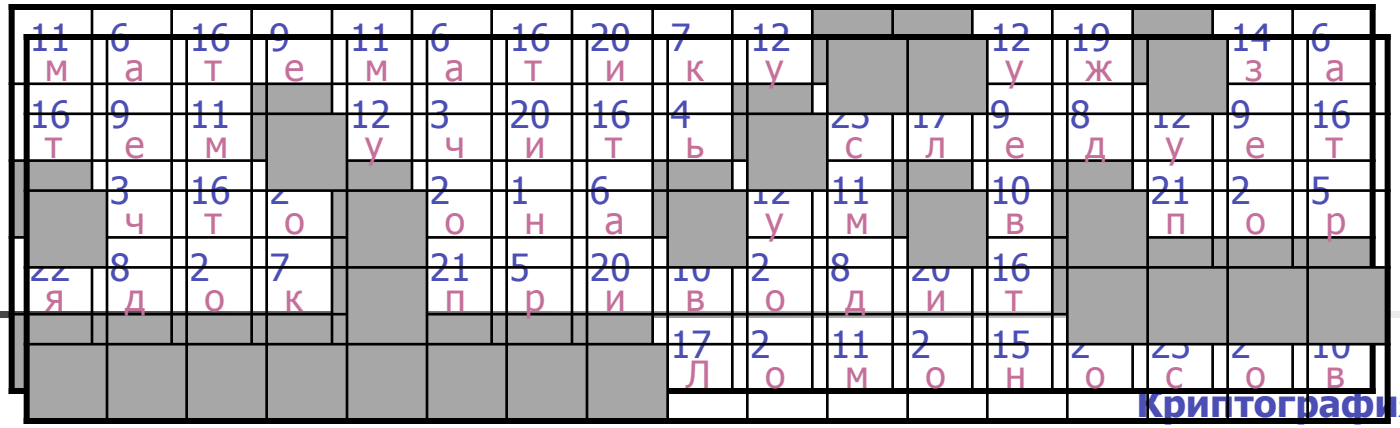
- **Прибор служащий для обнаружения в цепи электрического тока – 1,3,4,2,6,3,7,9,10,8,11,12**
- **Колючка роз – 16,15,14**
- **Образ, максимально обобщено и экспрессивно выражающий идею или отличительные черты какого – либо события или явления – 18, 17, 6, 8, 4**
- **Самые большие млекопитающие нашей планеты – 21,15,11,20**
- **Самая маленькая птица – 21,11,4,15,13,15**
- **Какой элемент является главной составляющей земной атмосферы – 3,22,11,12**
- **Как называется спиралевидная трубка во внутреннем ухе – 24,4,15,12,21,3**
- **Отличная школьная оценка от сознания вины – 18,11,20,19.**


22
3 7
13 6 4 24 1
3 15 1 9 12 20 18
6 8 12 16 15 7 20 21
3 21 9 12 8 4 , 23 12 9 18 3
4 7 3 1 12 3 19 9 7
6 22 9 12 20 22 3 18 11 3 7 9 17
14 9 6 8 4 8 4 18 89 9 12 24 19 15 11
2 12 3 18 21 3 11 15 , 6
7 8 17 14 8 12 24 7 20 18 21 12
20 6 6 7 9 16 15
14 12 15 6 8 18 11 2
14 9 19 1 12
3 19


з
а н
я в л у г
а и г о р ы С
в е р ш и н ы К
а к о р е л , б р о с А
л н а г р а д О Н
в з о р ы з а с т а н о м
п о в е л е л с о о р у д и Т
ь р а с к а т . и В
н е м п е р у н ы с к Р
ы в в н о ш И
п р и в е с т Ь
п о д г р
а д

С Эдгаром По читатель
Выискивал, где спрятан клад.
Решить криптограмму очень
Был каждый из нас рад.
Тайну пляшущих человечков
Конан Дойл поведал миру.
Много зашифрованных словечков
имели для героини
зловещую силу.

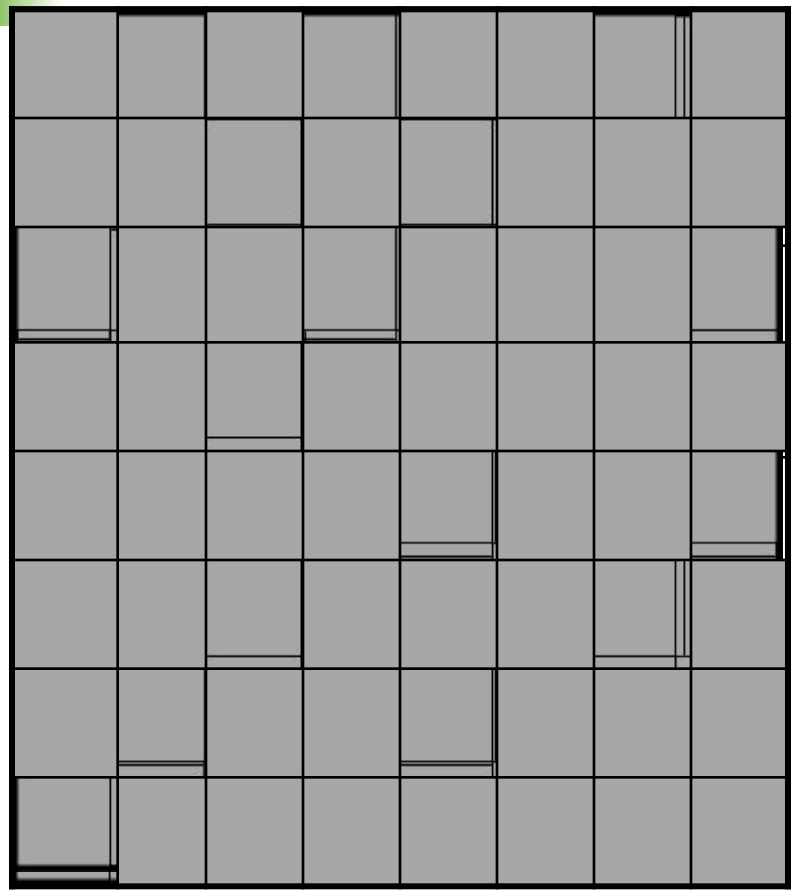
«ПРИХОДИ НЕМЕДЛЕННО».

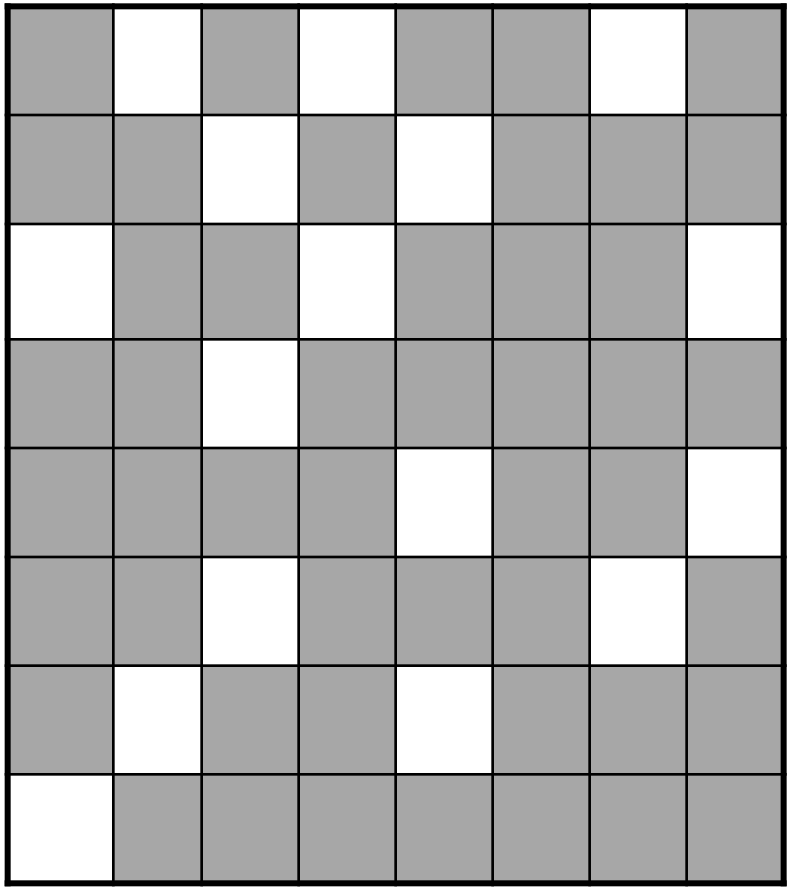


Криптография – наука
Увлекает всех она
Математик и философ
И профессор и студент
А теперь и Интернет
Конференции проводят
Где задачи стоят в ряд
Их ребята все решают
Вот себя и развивают

8,9,5,9,10,2 - Летом холодит, зимой согревает
11,12,13,2,11,2,5 – Стоит на полянке в красном платье Тальянке, вся в белых крапинках.
14,2,15,16 – Есть и корешок и шляпка, а не гриб.
17,18,19,20 – бегут по дорожке доски да ножки.
21, 2,22,23 – Днем обручем, ночью змеей.
1,2,3,4 – Махнула птица крылом и покрыла весь свет одним пером.
5,6,7 – кто от горя краснеет.

Я сама составила решетку для тайной переписки (их можно составить16^4 способами при трех самосовмещениях)





Секрет составления решетки

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	10	7	6	5
1	5	9	13	4	3	2	1

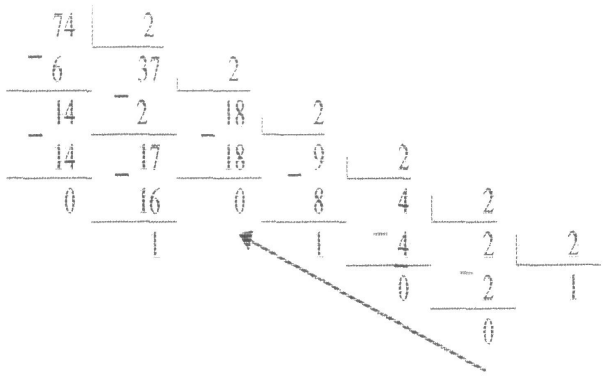
Зная, что общий вид числа записывают так:

$\overline{a_n a_{n-1} a_{n-2} \ldots \; a_2 a_1 a_0}$

Это число в десятичной системе счисления может быть представлено записью:

$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10^1 + a_0 \cdot 10^0$

Чтобы перевести запись числа из десятичной системы счисления в двоичную(или любую другую) нужно последовательно делить его на основание, как показано па примере числа 74



Получаем число: 1001010

Можно закодировать

решетку, запомнив 8 чисел

Секрет запоминания решетки

Из двоичной системы в десятичную

Записи:

0	1	0	1	0	0	1	0	=	82
0	0	1	0	1	0	0	0	=	40
1	0	0	1	0	0	0	1	=	145
0	0	1	0	0	0	0	0	=	32
0	0	0	0	1	0	0	1	=	9
0	0	1	0	0	0	1		=	34
0	1	0	0	1	0	0		=	72
1	0	0	0	0	0	0		=	128
128	64	32	16	8	4	2	Ед.		

Все поведала я вам.
Если хочешь погадай,
почитай и посмотри
Криптограммы ты мои.
Чтоб тебе не скучно было,
Ты придумай - ка свои,
Станешь книги ты читать,
будешь много понимать.
Ну, а я уже узнала,
Разгадала, прочитала,
Если хочешь так и ты,
Библиотеку посети
иль на сайте побывай,
новости криптограмм узнай
Будем вместе мы шагать,
Тему дальше развивать.

Заключение:

В результате проделанной работы, я

- **Нашла исторические сведения о криптограммах.**
- **Изучила различные способы составления криптограмм.**
- **Составила различные криптограммы**
- **Узнала что такое двоичное кодирование и как его можно использовать для запоминания решетки**
- **Научилась расшифровывать криптограммы**
- **Научилась работать с Power Point.**
- **Выявила связь криптограмм с математикой.**

Литература:

1. Перельман Я. И. «Живая математика» и «Занимательная Алгебра»
2. Гайшут А. Г. «Приемы интенсификации обучения математике»
3. Соболева Т. А. Тайнопись в истории России. М.: 1994.
4. Жельников В. Криптография от папируса до компьютера. М.: 1996.
5. Журнал Квант
6. Дойл А. К. «Рассказы о Шерлоке Холмсе»