**Окружная научно – практическая конференция младших школьников**

**«Я познаю мир – 2014»**

**Направление « Математика и информационные технологии»**

**Тайны за семью печатями**

**Выполнил:**

Поздеев Кирилл

ученик 3 «Б» класса

ГБОУ СОШ № 10 г.о. Кинель

**Руководитель:**

Хлынцева Юлия Викторовна

учитель начальных классов

ГБОУ СОШ № 10 г.о. Кинель

Кинель

2014

ОГЛАВЛЕНИЕ

Введение 3

Основная часть 5

С чего всё начиналось? 5

Стеганография 7

Сцитала 7

Узелковое письмо 8

ROT 110

Шифр Цезаря 11

Тарабарская грамота 11

Код Морзе 12

Код Энигма 13

Криптография с открытыми ключами 14

Основные методы криптографии15

Применение криптографии15

Заключение 17

Список литературы 18

Приложения 19

**ВВЕДЕНИЕ**

Все когда-нибудь пробовали передавать свои сообщения, зашифровав информацию. Во дворе с друзьями мы пытаемся договориться о каких-то особенных словах в общении, в классе с одноклассниками отгадываем зашифрованные названия произведений.

Сообщения шифруют по разным причинам – например, в игре или в ситуации борьбы – противостояния. В первом случае я имею дело с другом, над которым хочу подшутить, а во втором – с соперником, которого надо одурачить, например, в игре «Казаки-разбойники» мы с друзьями шифровали пароль.

Трудно найти человека, который бы не смотрел сериалы «Приключения Шерлока Холмса и доктора Ватсона», «Семнадцать мгновений весны», где использовались зашифрованные тайные сообщения. Посмотрев эти фильмы, я заинтересовался кодированием различных фраз и решил более подробно изучить этот вопрос. Осталось только дать немного понятий и можно идти в бой... Точнее, на разбор конкретных **шифров**.

**АКТУАЛЬНОСТЬ**

Шифры - это не такое уж узкое ремесло. С ними сталкиваются многие из нас. От школьников-запискокидателей Пети и Маши, не готовых каждого посвятить в свои шуры-муры, до агентов служб безопасности.

Необходимость скрывать содержание важных сообщений существует уже тысячи лет. Со временем люди находили все более и более сложные способы кодирования сообщений, поскольку простые способы кодировки декодируются с большей легкостью.

«Кто владеет информацией, тот владеет миром» – гласит известная фраза. Неудивительно, что в современном мире средства защиты информации приравниваются к самому смертельному оружию.

**Цель работы:** познакомиться с разными видами шифров**.**

**Задачи:**

* узнать о различных способах шифрования;
* изучить сферы использования шифров;
* попытаться воспроизвести старинные способы шифрования;
* осуществить шифровку и дешифровку текста.

**ОСНОВНАЯ ЧАСТЬ**

**С ЧЕГО ВСЁ НАЧИНАЛОСЬ?**

Вся эта хитрая наука называется **криптографией**. Она занимается методами, которые не позволяют прочесть данные посторонним субъектам, а также методами информационной защиты авторских прав, предотвращения подделок, создания электронно-цифровых подписей и т.д. Умнее говоря, обеспечиваются *конфиденциальность* и *аутентичность*.

Исторически криптография зародилась из потребности передачи секретной информации.

**Криптография** - тайная система изменения письма с целью сделать текст непонятным для непосвященных лиц.

**Крипто -** (греч. kryptos - тайный, скрытый) - часть сложных слов, указывающая на какое-либо скрытое, тайное действие или состояние.

Начало криптографии совпадает с началом письменности, так как написанные тексты мог понять, только умеющий читать. Издавна люди изыскивали способы уберечь некоторые важные сообщения от посторонних глаз. Рассказывают, как один царь обрил голову гонца, написал на ней послание и отослал гонца к своему союзнику лишь тогда, когда волосы на его голове отросли.[3,416]

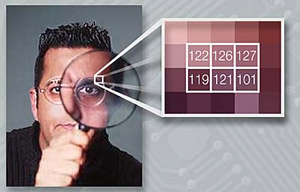
Развитие химии дало удобное средство для тайнописи: симпатические чернила, записи которыми не видны до тех пор, пока бумагу не нагреют или обработают каким-нибудь химикатом. Идея экзотической защиты секретных текстов (в том числе и с применением) дошла до наших дней. А. Толстой в известном произведении «Гиперболоид инженера Гарина» описал способ передачи сообщения путем его записи на спине симпатических чернил посыльного - мальчика. Во время II Мировой войны таким же образом иногда передавались агентурные сообщения.[5,52] Секретные послания записывались симпатическими чернилами и на предметах нижнего белья, носовых платках, галстуках и т. д. Но чаще стали применять шифры: сначала ими пользовались пираты, отмечая расположение кладов, алхимики, купцы, заговорщики. Впоследствии – дипломаты, стремящиеся сохранить тайны переговоров, военачальники, скрывающие от противника отданные распоряжения, разведчики и другие.

Первым описал использование шифровального устройства Плутарх, первым дешифровальщиком был Аристотель. Расцвет криптографии приходится на средние века. Один из шифров продержался до второй мировой войны. Некоторые историки считают одной из причин неудачного завершения для России Первой мировой войны некорректное отношение к шифрам. [2,239]

Математика издавна применялась в теории шифров. Еще в конце XVI века расшифровкой переписки между противниками французского короля занимался один из создателей современной алгебры Франсуа Виет. Будучи молодым офицером разведки, он нашел ключ к шифру испанского короля, содержащего 500 символов. Не поверив, что шифр можно было разгадать, испанцы обратились с жалобой к Папе Римскому, обвиняя французов в колдовстве.

А английские монархические заговорщики в XVII веке поражались быстроте, с которой вождь английской революции Оливер Кромвель проникал в их замыслы. Впоследствии выяснилось, что все эти шифры разгадывал один из лучших математиков того времени профессор Оксфордского университета Валлис. Валлис – сын священника из Кента. Уже в молодости вызывал восхищение как феноменальный счетчик в уме. Однако никакого математического образования он не получил, занимался самостоятельно. Он считал себя основателем новой науки – криптографии.[4,146]

Рассмотрю более подробно разные виды криптографии.

**СТЕГАНОГРАФИЯ**

Стеганография является более древней, чем коды и шифры, и обычно её называют тайнописью, искусством скрытой записи. Например, сообщение может быть написано на бумаге, покрытой воском, и гонец должен проглотить его и таким образом обеспечить скрытность, а в нужный момент отрыгнуть, чтобы сообщение можно было прочитать. Лучший способ тайнописи — это использование обычных предметов для сокрытия сообщения. В Англии был популярен метод тайнописи, для которого использовали обычную газету с крошечными точками под буквами на первой странице, которые указывали, какие буквы следует читать, чтобы получить сообщение. Некоторые люди могли составить сообщение, используя первые буквы каждого слова в каком-либо тексте или используя невидимые чернила. Конкурирующие страны могут так уменьшить текст, что целая страница текста становится размером с пиксель, который будет незаметен для постороннего глаза. Стеганографию лучше всего использовать в сочетании с кодом или шифром, так как существует риск, что тайное послание может быть обнаружено.

**СЦИТАЛА**

Самый древний из механических способов тайнописи – так называемая сцитала – известна со времен войны в V веке до нашей эры. Сциталой назывался специальный жезл, на который наматывалась без зазоров и нахлестов полоска папируса. Далее вдоль оси жезла писалось сообщение, полоска разматывалась и посылалась адресату. Для постороннего человека записанная информация представлялась бессмысленным набором букв – получатель же, имеющий в распоряжении точно такую же сциталу, без труда читал сообщение. Чтобы сделать сообщение еще более запутанным, в пробелы добавляли специально выбранные для этого буквы.

## http://img0.liveinternet.ru/images/attach/c/1/61/115/61115125_p9.jpg УЗЕЛКОВОЕ ПИСЬМО

«Узелковое письмо» («кипу») получило распространение у индейцев Центральной Америки. Свои сообщения они также передавали в виде нитки, на которой завязывались разноцветные узелки, определявшие содержание сообщения.

**Обозначения цветов:**

* [Чёрный](http://ru.wikipedia.org/wiki/%D0%A7%D1%91%D1%80%D0%BD%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) — [время](http://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%BC%D1%8F). То есть на чёрных нитях записывалось «время», «срок», годы, исторические события, понятие «от начала чего-либо (напр., от начала правления короля инков)»; чёрный цвет потому, что «кипу сообщало, сколько ночей прошло с момента того или иного события». Также — болезнь (при наличии ключа в главном шнуре). Этот цвет когда выцветает на нитях, то может быть перепутан с тёмно-тёмно-коричневым.
* [Кармазиновый](http://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BB%D0%B8%D0%BD%D0%BE%D0%B2%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) (ярко-красный; малиновый) — обозначение Инки (Короля, Монархии). На такой нити могли располагаться также узлы «времени», то есть для указания на срок правления Инки. Например, 4 узла — это четыре года правления Инки. Этот цвет упоминается только в письменных источниках.
* [Бурый](http://ru.wikipedia.org/wiki/%D0%91%D1%83%D1%80%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) (в колониальных источниках известен как *земляной*) — обозначал «подчинение», «общественный порядок», «правление», «управление»; например, осуществление подчинения правителем Инкой таких-то провинций (во время завоевания). А также — [картофель](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%80%D1%82%D0%BE%D1%84%D0%B5%D0%BB%D1%8C) (при наличии ключа в главном шнуре кипу). Этот цвет упоминается только в письменных источниках; вероятнее всего, он сопоставим с одним из тонов коричневого цвета.[6]
* Коричневый (точнее [каштановый](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%88%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82)). В кипу встречается наравне с белым чаще всего. Существует четыре тона:
  + светло-коричневый — значение неизвестно,
  + светло-светло коричневый (почти желтовато-белый) — значение неизвестно,
  + тёмно-коричневый — значение неизвестно,
  + тёмно-тёмно-коричневый (почти чёрный) — значение неизвестно.
* [Зелёный](http://ru.wikipedia.org/wiki/%D0%97%D0%B5%D0%BB%D1%91%D0%BD%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) — «завоевание»; обозначение противника, или количество человек, умерших у противника. На этой нити расположение было таким: первым шло сообщение о тех, кому за шестьдесят и старше, а дальше в соответствии со своими возрастами шли другие младше на десять лет и т. д. На нитях археологических встречается довольно редко. Мог быть двух тонов:
* светло-зелёный,
* тёмно-зелёный.
* [Красный](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B0%D1%81%D0%BD%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) — [война](http://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B9%D0%BD%D0%B0); собственное войско, а также собственные потери на войне. На нитях археологических кипу встречается довольно редко. Мог быть двух тонов:
* собственно синий,
* голубой.
* [Жёлтый](http://ru.wikipedia.org/wiki/%D0%96%D1%91%D0%BB%D1%82%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) — золото (например, военная добыча, состоявшая из золота весом во столько-то единиц измерения; однако какие именно единицы использовались из [инкской системы мер и весов](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D1%91%D1%82%D0%B0,_%D0%BC%D0%B5%D1%80_%D0%B8_%D0%B2%D0%B5%D1%81%D0%BE%D0%B2_%D0%B8%D0%BD%D0%BA%D0%BE%D0%B2) — неизвестно). А также —[кукуруза](http://ru.wikipedia.org/wiki/%D0%9A%D1%83%D0%BA%D1%83%D1%80%D1%83%D0%B7%D0%B0) (при наличии вставленного в главный шнур маленького кукурузного початка, имевшего значение ключа для прочтения кипу). Например, жёлтая нить означала кукурузу, и если к ней была привязана синяя нить (определённая провинция), с тем или иным числом узелков, то это говорило о том или ином урожае в этой провинции. На нитях археологических кипу встречается реже всего.
* [Белый](http://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%BB%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) — серебро; мир. В кипу встречается наравне с каштановым чаще всего. Существует два тона (какой тон что значил — неизвестно):
* [фиолетовый](http://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%BE%D0%BB%D0%B5%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82) ([тёмно-лиловый](http://ru.wikipedia.org/wiki/%D0%9B%D0%B8%D0%BB%D0%BE%D0%B2%D1%8B%D0%B9)) — обозначение начальника, который бы правил над селением, территорией, людьми; [курака](http://ru.wikipedia.org/wiki/%D0%9A%D1%83%D1%80%D0%B0%D0%BA%D0%B0" \o "Курака); правитель одного или двух селений. Этот цвет упоминается только в письменных источниках.
* [Синий](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BD%D0%B8%D0%B9_%D1%86%D0%B2%D0%B5%D1%82). На нитях встречается довольно редко. Двух тонов (значения неизвестны).
* [Соломенный](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BE%D0%BB%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%86%D0%B2%D0%B5%D1%82&action=edit&redlink=1) или палевый ([Straw](http://en.wikipedia.org/wiki/Straw_%28colour%29" \o "en:Straw (colour))) — обозначал *отсутствие*; беспорядок в управлении; «варварство». «Из отсутствий [цветов нитей] они извлекали представление о том, чего не было, а по Кипос — то, что произошло». Этот цвет упоминается только в письменных источниках; вероятно, сопоставим с одним из тонов светло-коричневого.

**ROT1**

## 10 фактов о кодах и шифрахЭтот шифр знаком многим детям. Ключ к шифру очень прост: каждая буква алфавита заменяется на последующую букву, поэтому, А заменяется на Б, Б заменяется на В, и так далее. «ROT1» буквально означает «вращать на 1 букву вперед по алфавиту». Фраза, «Тайны за семью печатями» превратится в секретную фразу « Убкоь иб тёнэя рёшбуанй». Этот шифр предназначен для развлечения, потому что его, легко понять и использовать, и столь же легко расшифровать, даже если ключ используется в обратном направлении.

## ШИФР ЦЕЗАРЯ

## 10 фактов о кодах и шифрах

## Шифр Цезаря (сдвижной), называется так потому, что он использовался Юлием Цезарем. Шифр состоит на самом деле из 33 различных шифров (количество шифров меняется в зависимости от алфавита используемого языка), по одной на каждую букву алфавита. «ROT1» является лишь одним из этих шифров. Человек должен был знать, какой шифр Цезаря использовать для того, чтобы расшифровать сообщение. Если используется шифр Ё, то, А становится Ё, Б становится Ж, В становится З, и так далее по алфавиту. Если используется шифр Ю, то, А становится Ю, Б становится Я, В становится, А, и так далее. Данный алгоритм является основой для многих более сложных шифров, но сам по себе не обеспечивает надежную защиту тайны сообщений, поскольку проверка 33-х различных ключей шифра займет относительно небольшое время.

## Тарабарская грамота - условная азбука, шифры, тайнопись. Для переписки с посольствами России в других странах в XVI веке использовалась так называемая тарабарская грамота. Этот шифр основывался на замене одной согласной буквы на другую: б-ш, в-щ, г-ч, д-ц, ж-х, з-ф, к-т, л-с, н-р, н-п. При использовании тарабарской грамоты строка букв "Чолуцамь шлея моллии" есть зашифрованная фраза "Государь всея России".

## КОД МОРЗЕ (Азбука Морзе)

## 10 фактов о кодах и шифрах

## Несмотря на свое название, код Морзе не является кодом — это шифр. Каждая буква алфавита, цифры от 0 до 9 и некоторые символы пунктуации заменены на последовательность коротких и длинных звуковых сигналов, которые часто называют «точка и тире». А становится «• — », Б становится « — • • •» и так далее. В отличие от большинства других шифров, код Морзе не используется для сокрытия сообщений. Код Морзе начал широко применяться с изобретением телеграфа Сэмюэлем Морзе. Это было первое широко используемое электрическое приспособление для передачи сообщений на дальние расстояния. Телеграф позволял немедленно передавать сообщения о событиях, произошедшие в одной стране, по всему миру. Код Морзе изменил характер войны, позволяя обеспечивать мгновенную связь с войсками на большом расстоянии.[7]

ROT1, шифр Цезаря, тарабарская грамота и азбука Морзе относятся к одному и тому же типу — моноалфавитной замене, а это означает, что каждая буква алфавита заменяется в соответствии с ключом, другой буквой или символом. На самом деле их легко расшифровать, даже не зная ключа.

Примером моноалфавитной замены может служить и шифр, описанный в рассказе Конан Дойла «Пляшущие человечки», где Шерлок Холмс расшифровывает нарисованные сообщения. Великий сыщик исходил из предположения, что:

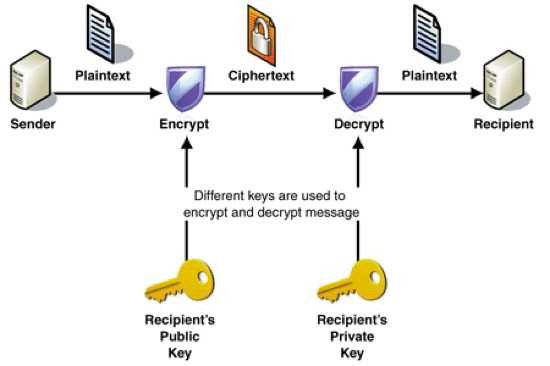
* каждый человечек обозначает одну букву;
* Е – наиболее часто встречающаяся буква в английском языке;
* Илси – имя женщины, замешанной в этом деле;
* флажок в руках человечка обозначает последнюю букву отдельного слова.

Узнав ключ, Холмс готовит преступнику ловушку, посылая ему зашифрованное сообщение.

## КОД ЭНИГМА

## Код Энигма, который был очень сложным шифром, использовался немцами во время Второй Мировой войны. Для этого использовали машину Энигма, которая очень похожа на пишущую машинку, при нажатии на определенную букву на экране загоралась буква шифра. Машина имела несколько колес, которые были связаны с буквами проводами, для определения, какая буква шифра будет высвечиваться. Все машины Энигма были одинаковы, и начальная конфигурация колес была ключом к шифрованию сообщений. Чтобы усложнить процесс, колесо должно было вращаться после того, как определённое количество букв было напечатано. Немецкое командование каждый день выдавало списки начальной конфигурации колес для использования в шифровании, так что все немецкие командиры использовали одну и ту же конфигурацию, и могли расшифровать сообщения друг друга. Даже когда союзники заполучили копию машины, они все равно не могли расшифровать сообщения, поскольку машина выдавала сотню триллионов возможных начальных конфигураций колес. Код Энигма был взломан польскими умельцами и окончательно расшифрован английскими математиками, которые использовали смекалку и компьютеры.[8] Знание немецких коммуникационных систем дало союзникам значительное преимущество в ходе войны, а процесс взлома кода Энигма позволил создать первый прообраз компьютера.

## КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ

Это самый современный шифр, и он имеет несколько вариантов. Это шифр, который используется во всем мире, и имеет два ключа: один открытый и один личный. Открытый ключ — это большое число, доступное всем. Ключ является таким сложным потому что при делении можно получить только два целых числа (кроме 1 и самого числа). Эти два числа и есть личный ключ, и, если их перемножить, получится открытый ключ. Например, открытый ключ может быть 1961, следовательно, личный ключ — это 37 и 53. Открытый ключ используется для шифрования сообщения, и сообщение невозможно расшифровать без личного ключа. При отправке личных данных в банк, или когда банковская карта обрабатывается машиной, данные зашифрованы именно таким образом, и только банк со своим личным ключом может получить к ним доступ. Причина, почему этот способ является настолько безопасным, заключается в том, что математически очень трудно найти делители больших чисел.[9]

**ОСНОВНЫЕ МЕТОДЫ КРИПТОГРАФИИ**

Два главных способа шифрования информации – это метод перестановок и метод подстановки. В первом случае буквы в сообщении остаются те же, но меняется их порядок. Путем перестановки букв составляется анаграмма, то есть новое слово.

При использовании метода подстановки буквы заменяются цифрами, знаками или другими буквами; ответ на загадку, какая буква скрывается под каким знаком, содержится в ключе.

В целях повышения криптографической стойкости кода в одной системе шифрования вместе или по очереди могут использоваться и перестановки, и замена.

**ПРИМЕНЕНИЕ КРИПТОГРАФИИ**

**В настоящее время криптография присутствует в повседневной жизни, хотя не всегда ее можно заметить невооруженным глазом. Такие явления, как мобильная связь, платное телевидение или интернет-покупки не были бы возможны без применения криптографических методов, позволяющих гарантировать безопасность и неприкосновенность данных. У электронных голосований также есть проблемы с безопасностью, и криптография необходима для сохранения тайны голосования и для того, чтобы голосовать могли только зарегистрированные пользователи и только единожды. [9] Да и просто умные люди могут как-то шифровать свою переписку, если не хотят, чтобы её содержимое кто-то знал. Кто-то может просто стесняться. А кто-то ведёт речь о крупной сумме денег.

**ЗАКЛЮЧЕНИЕ**

И в заключении мне хочется сказать, что моя тема очень актуальна, потому что нас постоянно окружают различные знаки и символика.

Эта работа помогла мне познакомиться с применением математики для решения задач кодирования и декодирования. В ней я рассмотрел различные виды шифров.

В общем, это вполне полезный для всех материал, а не пособие для начинающего шпиона.

Я думаю, что на следующий год можно рассмотреть и изучить более сложные шифры, а также попробовать придумать свой шифр.

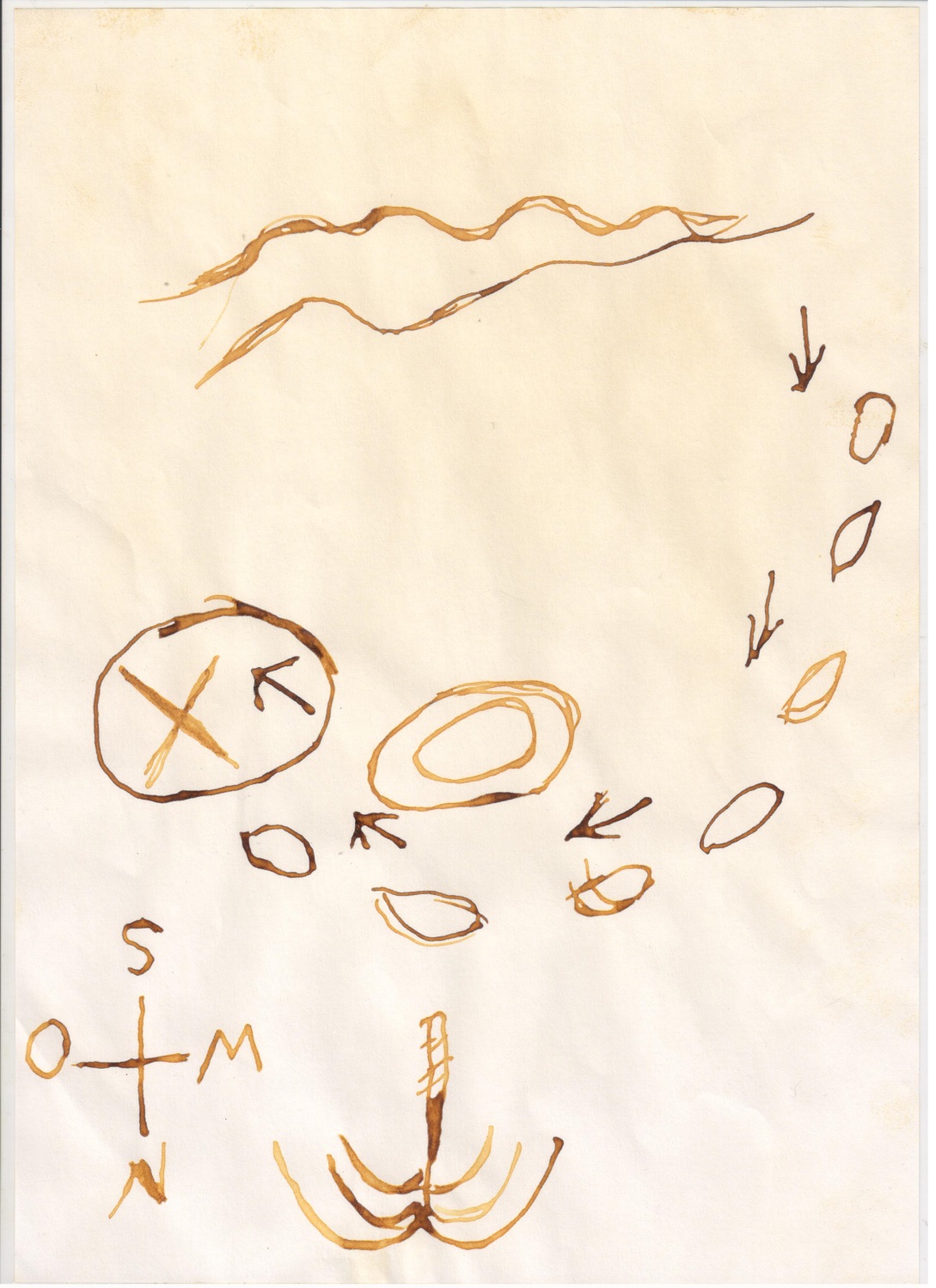
**СПИСОК ЛИТЕРАТУРЫ**

1. Большая Советская Энциклопедия Т.13 - М.: "Советская энциклопедия", 1973 , 763с.
2. Энциклопедический словарь юного математика/ составитель Э-68 А.П.Савин - М.: Педагогика, 1989, 352 с.
3. Энциклопедия для детей Т.10 - М.: "Языкознание. Русский язык", "Аванта+", 1999, 702 с.
4. Жельников В. Криптография от папируса до компьютера. - М.: "АВF", 1996, 335 с.
5. Серов Е., Волгин В. Тайны военной разведки (1918 -1945). // Армия. - М., 1994 - № 7 - с. 52 -55.
6. Гонина Е.Е. Шифры, коды, тайны. – Живая математика, № 1, 2008.
7. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах: Популярное издание
8. Г. Фролов. Тайны тайнописи. - М., 1992.
9. [http://genius.pstu.ru/file.php/1/pupils\_works\_2012/](http://genius.pstu.ru/file.php/1/pupils_works_2012/Verkholancev_Vladislav.pdf)

**ПРИЛОЖЕНИЯ**

**МОЯ ПОПЫТКА ТАЙНОПИСИ**

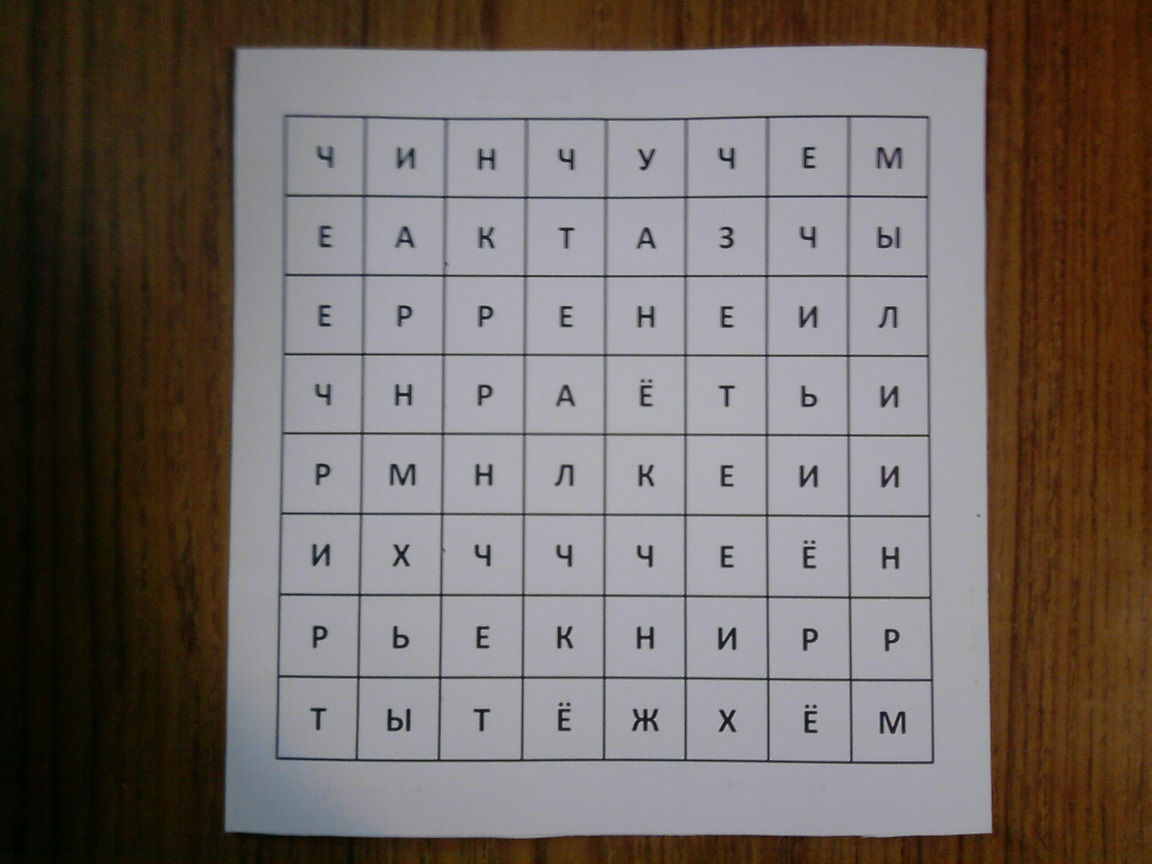
**С помощью молока я нарисовал карту спрятанных сокровищ**

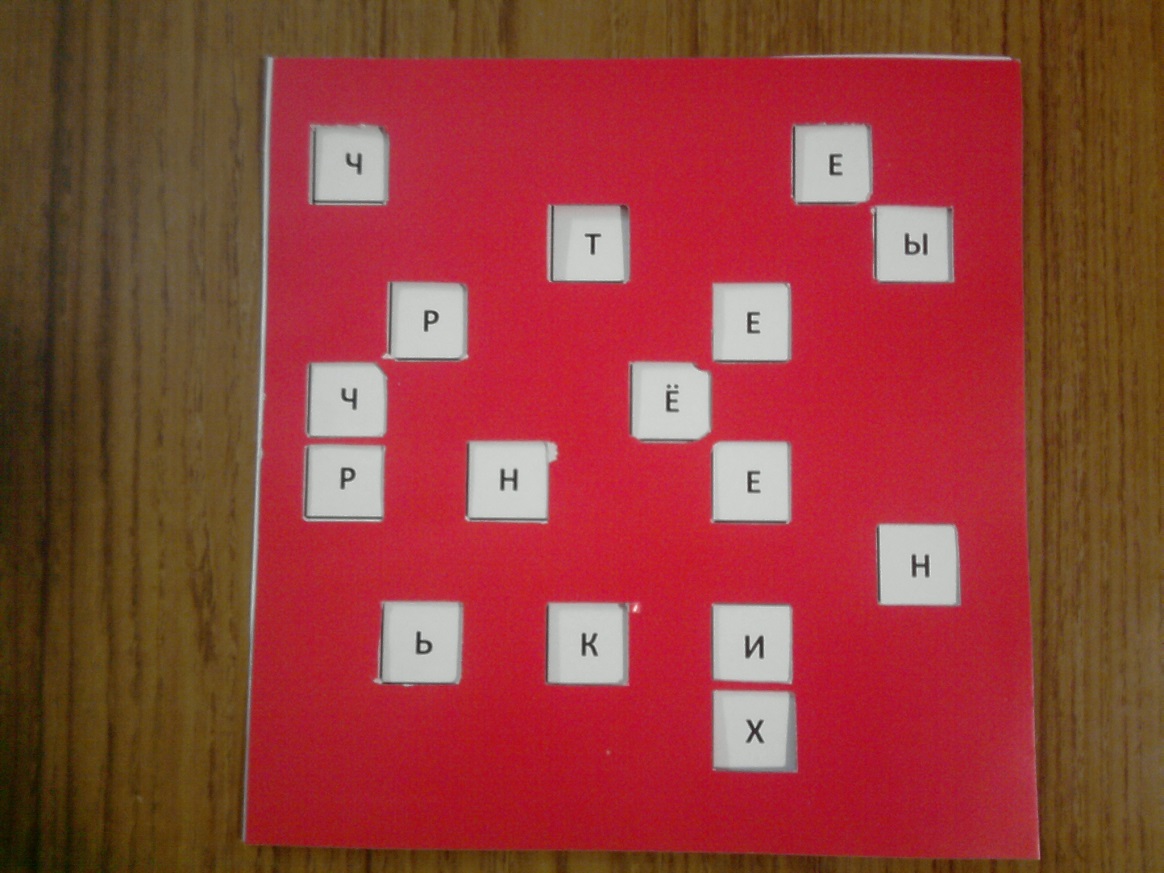
****

**МОЯ СЦИТАЛА**

****

**МОЙ ШИФР ЦЕЗАРЯ**

****

****