ЗАГАДКИ РАЗНЫХ ШИФРОВ

Ищуков И.С.

МОБУ СОШ №8 им. А.Г. Ломакина, 2 «А» класс

Руководитель: Черныш Е.Н., МОБУ СОШ №8 им. А.Г. Ломакина, учитель начальных классов

Моя мама работает в Южном Федеральном Университете на кафедре Безопасности информационных технологий. Она занимается криптографией. Криптография – это наука о шифрах.

В ноябре 2017 года мама придумала и провела квест для школьников. В этом квесте школьники решали различные задачи, в том числе расшифровывали разные шифры.

Я наблюдал, как мама готовила задания, а потом – как ребята их решали. Мне стало интересно смогу ли я сам сделать такие шифровки? Сможет ли кто-нибудь такие шифровки прочитать?

С помощью учителя я провел опрос среди учеников МОБУ СОШ №8 им. А.Г. Ломакина. Всего было опрошено 44 ученика в возрасте от 7 до 14 лет. На вопрос «Ты знаешь, что такое криптография?» 18 учеников ответили «ДА» и 26 учеников «НЕТ». Книги о шифрах читали всего 4 ученика из опрошенных 44 человек. 14 человек пробовали делать свой собственный шифр. Большинство ребят (34 человека) указали, что хотели бы больше узнать о разных способах шифрования информации. Мой опрос подтвердил, что выбранная мной тема будет интересна большинству учеников.

Цель моего исследования: узнать принцип построения различных шифров, научиться шифровать сообщения; понять, как можно восстановить исходное сообщение по анализу шифровки.

Задачи моего исследования:

• Познакомиться с историей создания первых шифров.

• Узнать секреты разных шифров, понять как можно зашифровать и расшифровать сообщение разными способами.

• В домашних условиях провести опыты по созданию различных приспособлений для шифрования.

• Изучить свойства зашифрованных сообщений, использовать эти свойства для того, чтобы раскрыть секрет шифра.

• Провести праздник в нашем классе «Шерлок Холмс идет по следу».

Гипотеза. Если известно, какой был использован шифр, то можно расшифровать сообщение.

Методы исследования: анализ литературы, опрос, создание простейших устройств для шифрования информации, проведение опытов, сравнение и обобщение результатов.

Практическая направленность. Моя работа может быть использована при проведении праздников (квестов) для создания загадок в стиле Шерлока Холмса, на уроках математики, для расширения умственного кругозора детей и взрослых, которые желают узнать секреты разных шифров.

1. История тайнописи

Для того, чтобы познакомиться с историей разных шифров, я обратился к маме. Она рассказала мне много полезной информации. А потом мы вместе с ней нашли в сети Интернет картинки и описания разных шифров.

Пишут, что после возникновения письменности еще в глубокой древности у людей появилась потребность скрыть важные сведения. По мере развития общества данная проблема вышла на новый уровень и способствовала возникновению науки криптографии (от греч. kryptys – тайный, сокрытый, и греч. grapho – пишу, черчу, рисую) или тайнописи. Криптография (тайнопись) – это наука о возможных способах изменения обычного письма, используемых с целью сделать текст понятным лишь для ограниченного числа лиц.

Криптография зародилась в древности. Дошедшая до наших дней надпись, вырезанная примерно в 1900 году до н. э. на гробнице знатного человека по имени Хнумхотеп, лишь в отдельных местах состоит из необычных иероглифических символов вместо более привычных иероглифов [1]. Безымянный писец старался не затруднить чтение текста, а лишь придать ему большую важность, подобно тому, как в каком-нибудь заявлении по важному поводу пишут, например, «в год одна тысяча восемьсот шестьдесят третий от Рождества Христова», вместо того чтобы просто и без затей написать: «в 1863 году». Вместе с тем, хотя писец применил не тайнопись, он, бесспорно, воспользовался одним из существенных элементов шифрования – умышленным преобразованием письменных символов. Это самый древний известный нам текст, который претерпел такие изменения.

История криптографии насчитывает несколько тысячелетий. Первые письменные источники относятся к 1900–м годам до н. э. Именно этим периодом датируются найденные в Египте свитки, в которых использованы видоизмененные иероглифы, по-видимому, применявшиеся для тайного обмена сведениями. Мама объяснила мне, что запись на неизвестном языке – это уже тайная запись. На рис. 1 показаны иероглифы различных народов земли. Не зная их значений, я не могу прочитать то, что там написано.

2. Мое первое знакомство с шифрами

Мама рассказала мне, что есть много интересных книг, в которых описаны различ-

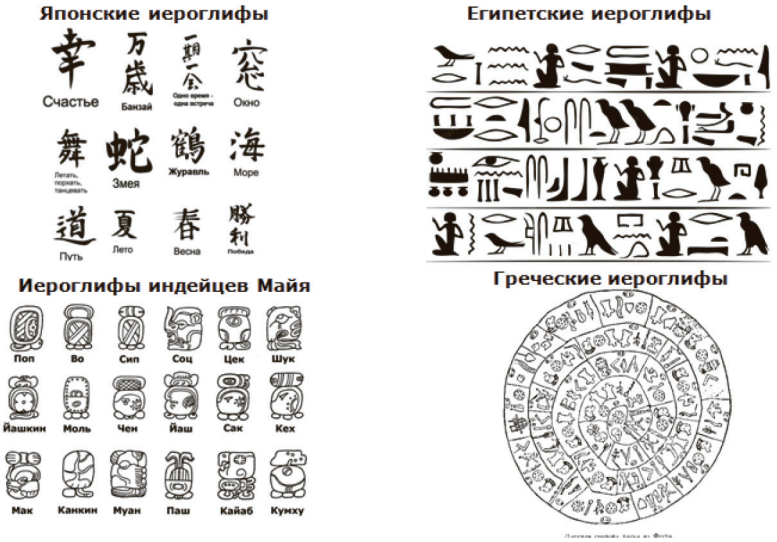


Рис. 1. Иероглифы различных народов

В 600–500 годы до н. э. на Ближнем Востоке древними евреями был разработан один из первых систематических шифров; этот метод называется темура – «обмен» [2]. Буквы еврейского алфавита делились на две части, причем одна помещалась над другой; затем верхние буквы заменялись на нижние или наоборот. При этом можно было составлять всевозможные комбинации в зависимости от места разделения алфавита и направления перемещаемых букв. Самый простой способ заключался в разделении алфавита посередине так, чтобы первые две буквы, А (Алеф) и Б (Бет), совпадали с двумя последними, Т (Тае) и Ш (Шин). Эти буквы и дали название методу шифровки – «Атбаш». В России система шифрования «Атбаш» получила широкое распространение в 16–18 веках и название «тарабарская грамота» [2].

Мама рассказала мне, что есть много интересных книг, в которых описаны различные шифры. Мы выбрали одну из них. Рассказ называется «Пляшущие человечки», его написал Артур Конан Дойл [3]. В этом рассказе Шерлоку Холмсу необходимо было прочитать тексты пяти записок, показанных на рис. 2. Шерлок Холмс анализировал их и смог понять отдельные буквы. Зная отдельные буквы, он по смыслу восстановил все остальные буквы сообщения.

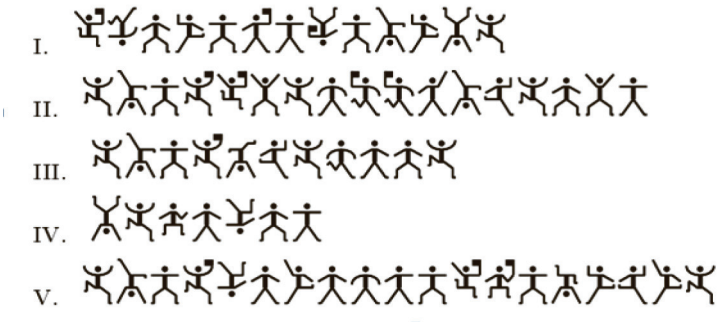


Рис. 2. «Пляшущие человечки»

Рассказ так понравился мне, что я решил сделать свой собственный шифр с «Пляшущими человечками». Это оказалось не так просто – придумать 33 разных человечка. Но в итоге у меня получилось!!! На рис. 3а фотография, мама сфотографировала меня, пока я придумывал человечков. А на рис. 3б – то, что получилось у меня в итоге.

Я зашифровал сообщение «Папа я тебя люблю!» и отнес его папе (рис. 4). Я засек время – папе понадобилось всего 20 минут, чтобы расшифровать сообщение! Я очень удивился, как он смог это сделать. Но папа объяснил, что в сообщение первые две буквы повторяются, а так как сообщение было для него, для папы, то он и подумал, что это буквы П и А. Дальше он предположил, что отдельный человечек – это буква Я. А таких букв в сообщении сразу три! Остальные буквы папа угадал по смыслу. Он очень быстро смогу узнать, что я ему написал!

а *б*

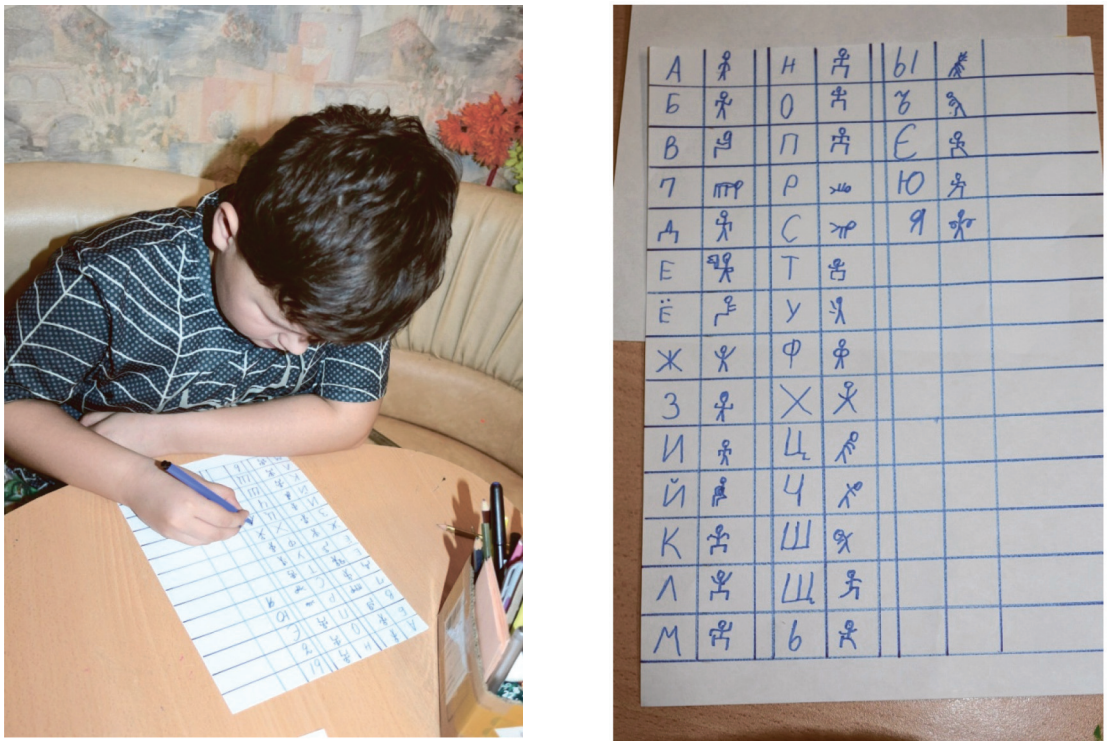


Рис 3:
а – я составляю алфавит со своими пляшущими человечками; б – мои пляшущие человечки

Рис. 4. Зашифрованное сообщение для папы

Тогда я решил проверить, смогут ли ребята из нашей школы угадать мое сообщение. Мы с учителем провели анкетирование. Вопрос звучал так: «Сможешь ли ты угадать, какое сообщение я написал папе?» Слово «папа» в вопросе было небольшой подсказкой. На вопросы анкеты отвечали ученики 2 и 6 класса МОБУ СОШ №8 им. А.Г. Ломакина. Всего было опрошено 44 ученика. Всю фразу угадали 10 человек. Интересно, что из этих 10 человек только один учится в 6 классе, а остальные во 2. Я думаю это потому, что ученики 2 класса обратились за помощью к родителям. Еще два человека смогли угадать только первое слово «папа». Остальные не смогли расшифровать шифр. Результаты представлены на рис. 5. В этот раз моя гипотеза оказалась верной.

Рис. 5. Результаты дешифрования шифра с пляшущими человечками учениками школы МОБУ СОШ №8 им. А.Г. Ломакина

3. Шифр «поворотная решетка»

Шифр «поворотная решетка» принадлежит Джероламо Кардано [1]. Решетки для шифрования сообщений использовались еще раньше, например кардиналом Ришелье. В качестве решетки использовался плотный лист бумаги, в котором было обозначено m строк и n столбцов. В некоторых позициях листа были сделаны прорези. Лист с прорезями накладывался на лист бумаги, после чего текст шифруемого сообщения записывался в прорези. В самом простом случае после этого можно было убрать решетку и заполнить пустые места произвольными буквами и символами. Кардано усовершенствовал применение таких решеток. Его решетку необходимо было использовать 4 раза, каждый раз поворачивая вправо на 90 градусов. После такого использования все свободные позиции листа оказывались заполненными передаваемым сообщением.

Мама помогла мне сделать свою решетку Кардано. Она состояла из 6 строк и 6 столбцов (рис. 6а). С ее помощью я зашифровал сообщение «Теперь я знаю криптографию Ура» (рис. 6б). Я дал это сообщение папе, но он не смог его прочитать. Тогда я дал папе саму решетку. Через несколько секунд папа сказал мне ответ. Это значит, что данный шифр может прочитать только тот, кто знает, какая именно была использована решетка!

а *б*

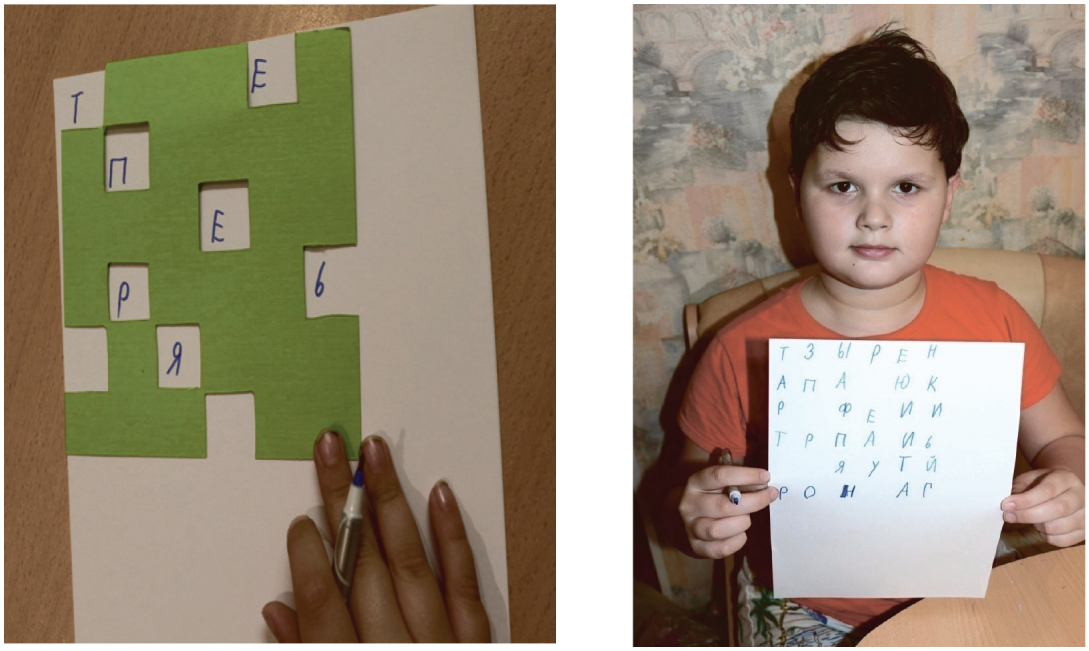


Рис. 6:
а – мой вариант решетки Кардано;
б – текст, зашифрованный с помощью моей решетки Кардано

4. Шифр Скитала

Известно, что в Древней Греции, относящийся к V в. до н. э., во время войн для передачи военных донесений использовалось одно из первых шифровальных приспособлений – «Скитала». «Скитала» представляла собой цилиндрический жезл, на который без нахлестов и разрывов наматывалась узкая полоска папируса или пергамента [4]. Кроме жезла могли использоваться любые другие цилиндрические предметы, например, рукоятки мечей, кинжалов, копий и т.д. Текст записывался построчно вдоль оси «Скиталы», а затем лента снималась с жезла. В результате получались беспорядочно написанные буквы, то есть своего рода шифр перестановки. Ключом к шифру служил диаметр Скиталы. На рис. 7а показан пример написания шифровки с использованием Скиталы.

В качестве основы мы с мамой взяли рулон бумаги, намотали на него полоску бумаги. Я написал сообщение «Спасите». А остальные буквы написал в произвольном порядке (рис. 7б).

Я отнес шифр брату. Он долго его крутил, но так и не смог прочитать. Тогда я показал ему свое устройство, и он смог прочитать сообщение. Мама рассказала, что метод вскрытия такого шифра приписывается Аристотелю. Для того, чтобы прочитать сообщение необходимо было заточить на конус длинный брус. После чего ленту с шифрованным сообщением необходимо было обернуть вокруг самого узкого места конуса и начать сдвигать ее по направлению к основанию конуса. В том месте, где диаметр конуса совпадал с диаметром Скиталы, буквы текста складывались в понятные слова или слоги. Таким образом, оставалось выточить (или найти) цилиндр нужного диаметра, чтобы прочитать сообщение.

а *б*

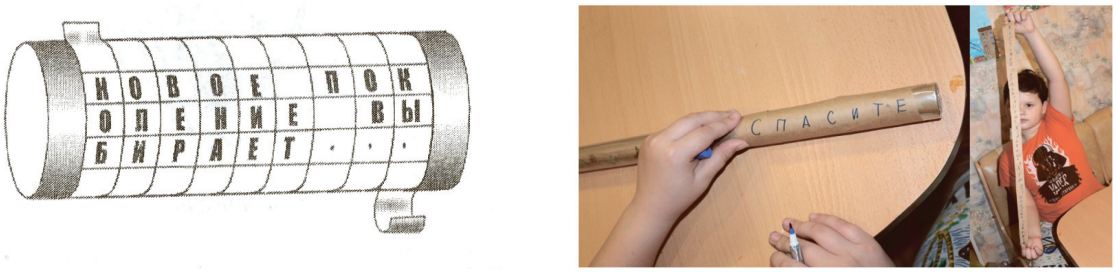


Рис. 7:
а – пример написания шифровки с использованием Скиталы; б – моя шифровка по принципу «Скитала»

5. Диск Энея

Помимо устройства Скитала в Древней Греции использовался еще один шифровальный прибор, который назывался таблица Энея. На небольшой таблице горизонтально располагался алфавит, а по ее боковым сторонам имелись выемки для наматывания нити. При зашифровании нить закреплялась у одной из сторон таблицы и наматывалась на нее. На нити делались отметки (например, узелки) в местах, которые находились напротив букв данного текста. По алфавиту можно было двигаться лишь в одну сторону, то есть делать по одной отметке на каждом витке. После зашифрования нить сматывалась и передавалась адресату. Этот шифр представлял собой шифр замены букв открытого текста знаками, которые означали расстояния между отметками нити. Ключом являлись геометрические размеры таблицы и порядок расположения букв алфавита.

Диск Энея является разновидностью таблицы Энея. Он представлял собой диск диаметром 10–15 см с отверстиями по числу букв алфавита. Каждому отверстию ставилась в соответствие конкретная буква. В центре диска находилась катушка с намотанной на неё ниткой. Для записи сообщения нитка протягивалась через отверстия в диске, соответствующим буквам сообщения. При чтении получатель вытягивал нитку, и получал буквы, правда, в обратном порядке. Хотя недоброжелатель мог прочитать сообщение, если перехватит диск, Эней предусмотрел способ быстрого уничтожения сообщения – для этого было достаточно выдернуть нить, закреплённую на катушке в центре диска [5].

Я зашифровал сообщение «Мы поедем в путешествие по России». И папа, и брат его легко прочитали, вытягивая нитку и составляя буквы (рис. 8).

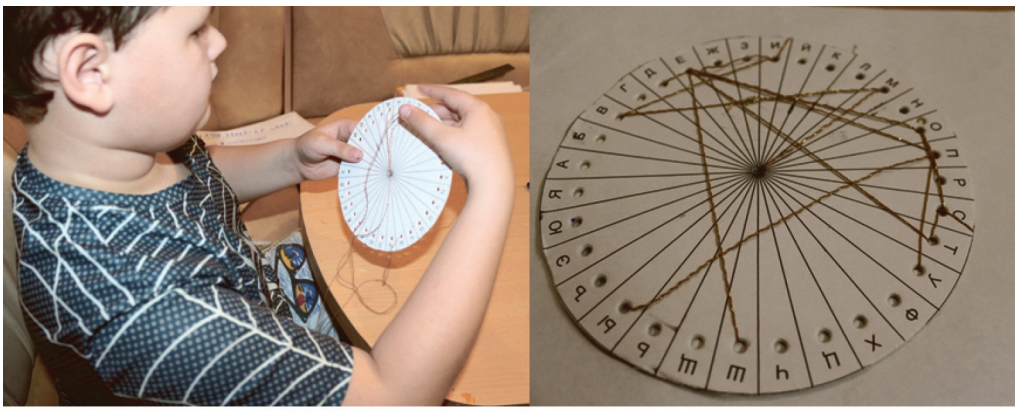


Рис. 8. Зашифрованное сообщение

6. Шифр Полибия

Греческий писатель Полибий использовал систему сигнализации, которая была широко принята как метод шифрования [6]. Он записывал буквы алфавита в квадратную таблицу и заменял их парой чисел, которые указывали соответственно на номер строки и номер столбца, на пересечении которых находилась зашифровываемая буква. Для латинского языка Полибий использовал квадратную таблицу размером 5x5 (буквы i и j считались сходными и заменялись на одно и то же значение). Для кириллицы можно было бы опустить буквы ё, й и ъ – в этом случае квадрат Полибия мог бы иметь размер 5x6 или 6x5.

При передаче сообщений между сторожевыми вышками тех времен использовались факелы. Так, чтобы передать букву R необходимо было взять 4 факела в правую руку и 2 – в левую. Полибий использовал это для шифрования сообщений и стал записывать каждую букву парой координат.

В нашей стране принцип использования таблицы Полибия нашел широкое применение в 19 веке в среде революционеров, находящихся в тюремном заключении. Революционерами использовались различные наборы алфавитов (то есть опускалось различное число редко встречающихся букв русского языка) и различные размеры таблиц для перестукивания друг с другом через стены камер. Такие системы получили название «тюремных шифров».

Я сделал свой квадрат и зашифровал сообщение «Мне восемь лет» (рис. 9а). Без квадрата папе и старшему брату было сложно его отгадать – они не смогли. Зато с квадратом они быстро справились с заданием! (рис. 9б). Я решил проверить, смогут ли ребята из нашей школы угадать мое сообщение. Они получили задание так, как показано на рис. 9б. Всего было опрошено 44 ученика. Из них 36 человек успешно справились с заданием.

а *б*

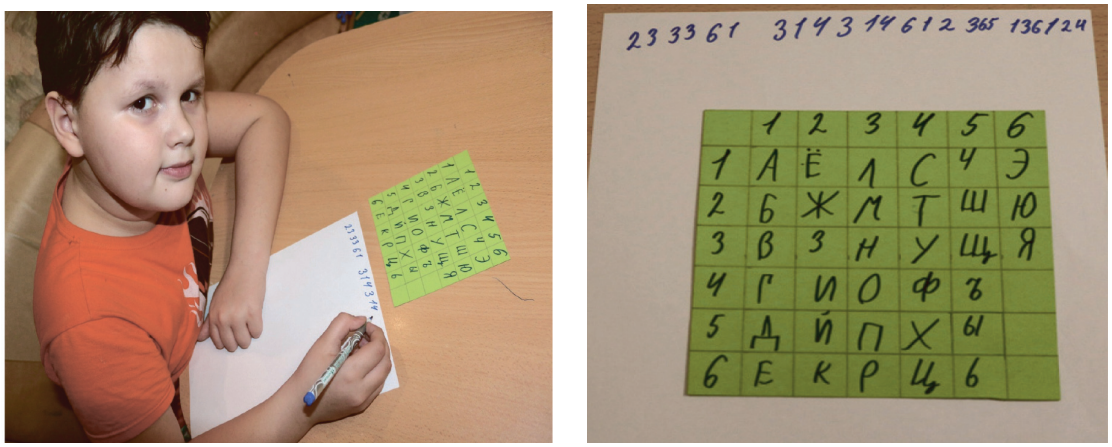


Рис. 9:
а – создаю шифрованное послание с помощью квадрата Полибия; б – текст, зашифрованный с помощью квадрата Полибия

7. Шифр Цезаря

Широко известна система шифрования, предложенная Юлием Цезарем и описанная им в «Записках о галльской войне» (I век до н.э.). Принцип шифрования был весьма прост. Шифруемую букву сообщения необходимо было заменить на букву алфавита, отстоящую от нее на 3 позиции правее. Для удобства шифрования можно переписать алфавит так, как показано на рис. 10.

8. Диск Альберти

Большой шаг вперед криптография совершила с помощью трудов известного философа Леона Альберти, который помимо описания математической модели криптографии ввел в использование механическое устройство, которое получило название «Диск Альберти» и широко использовалось вплоть до начала 19 века, а затем легло в основу многих механических шифровальных устройств [8].

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	Ь	Ы	Ъ	Э	Ю	Я
Э	Ю	Я	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	Ь	Ы	Ъ

Рис. 10. Шифр Юлия Цезаря

Так, с использованием шифра Цезаря фраза «Жизнь коротка» превратится в фразу «Йлкрэ нснсхнг».

Я зашифровал сообщение «Это шифр Юлия Цезаря» (рис. 11). Папа смог прочитать шифр. Он объяснил мне, что шифр похож на пляшущих человечков. Одинаковые буквы заменяются одинаково. Так, буква Р заменилась оба раза на букву У, а буква И – на букву Л.

«Диск Альберти» представлял собой пару дисков. Первый диск большего диаметра был неподвижным. Второй диск меньшего диаметра был соотнесен с первым и вращался в любом направлении. Оба диска были разделены на 24 сектора. В сектора большого диска вписывались 20 букв латинского алфавита (Альберти исключил буквы h, j, k, u, w, y) и четыре цифры от 1 до 4. В меньший диск были вписаны все

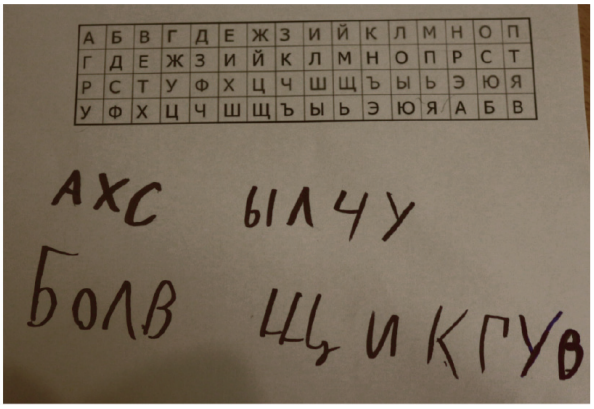


Рис. 11. Моя шифровка для папы с использованием шифра Цезаря

буквы латинского алфавита, но не по порядку, а вперемешку (рис. 12а).

таблицы Тритемия были применены в пер-

а *б*

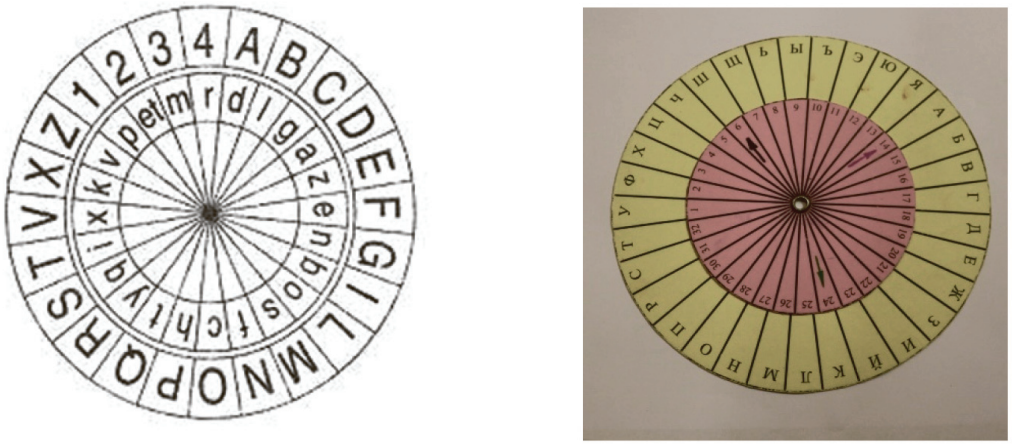


Рис. 12:
а – Диск Альберти; б – мой вариант Диска Альберти

Для успешного осуществления шифрования, необходимо было иметь два таких устройства на приемной и передающей сторонах. Кроме того, необходимо было договориться о начальной установке малого диска относительно большого и о частоте смещения малого диска относительно большого. После этого очередная буква шифруемого сообщения отыскивалась на неподвижном большом диске, а стоящая против нее буква малого диска являлась результатом зашифрования. После того, как условленное число букв было зашифровано, малый диск сдвигался вправо или влево на оговоренное число позиций и шифрование продолжалось. Получалось, что с помощью дисков можно было использовать не один, а несколько алфавитов для зашифрования. Такого рода криптосистемы получили название многоалфавитных. Кроме того, наиболее встречающиеся в сообщениях фразы и названия можно было представить в виде кодов из четырех цифр, после чего зашифровать их с помощью дисков. Такие шифры были названы кодами с перешифрованием, и получили широкое распространение в конце 19 века.

Мама помогла мне сделать диск Альберти для русского алфавита (рис. 12б). Во внутреннем диске мы использовали только цифры. С его помощью я зашифровал сообщение «Я закончу школу с золотой медалью» (рис. 13). Я дал шифр папе. Он не смог его прочитать. Тогда я отдал ему Диск. С Диском папа справился с заданием!

Рис. 13. Шифрую сообщение с помощью диска Альберти

9. Шифр Виженера

Богатым на криптографичекие новшества оказался 16 век. В 1518 году появилась работа Иоганнеса Тритемия, которая называлась «Полиграфия» [9]. Тритемий впервые предложил использовать для шифрования квадратные таблицы. Алфавиты для шифрования записывались в строки таблицы один под другим, каждый со сдвигом на одну позицию влево. Естественно,

вую очередь к латинскому алфавиту. Мы же представим их применительно к русскому. Тритемий предлагал использовать свою таблицу следующим образом: первая буква текста шифруется первым алфавитом, вторая – вторым и так далее.

В 1553 году Джованни Батиста Беллазо предложил использовать для многоалфавитного шифра буквенный, легко запоминаемый ключ, который он назвал паролем. Это могло быть какое-либо слово или фраза, которая записывалась над открытым текстом. Буква пароля, расположенная над буквой открытого текста, указывала на алфавит таблицы, который использовался для зашифрования этой буквы. Однако на некоторое время работы Тритемия и Беллазо были забыты и получили свое развитие в работе Блеза де Виженера «Трактат о шифрах». Вижинер добавил к таблице Тритемия еще одну строку (верхнюю) и еще один столбец (самый левый) как показано в таблице 1.

В верхней строке отыскивалась очередная буква пароля, а в левом столбце – буква шифруемого сообщения. На пересечении найденных строки и столбца находилась очередная буква шифрованного сообщения. Широкое использование шифра, предложенного Виженером, несколько оттеснило на второй план первоначального изобретателя многоалфавитных шифров Тритемия. Именно поэтому в литературе наиболее часто можно встретить название таблица Виженера, а не таблица Тритемия. Кроме того, Виженер предложил использовать в таких таблицах не только упорядоченные алфавиты, но и алфавиты, составленные произвольным образом.

Таблица 1

Таблица Виженера

	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
А	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
Б	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А
В	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б
Г	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В
Д	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г
Е	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д
Ж	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е
З	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ь	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Э	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы
Ю	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э
Я	Я	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	

Я зашифровал фразу «Я люблю рисовать картины» (рис. 14). В качестве пароля я использовал фразу «Шифр Виженера». В табл. 2 показано как соотносятся буквы ключа и шифра. В первом столбце обозначено содержимое строк. Буква «Т» обозначает исходный текст, «П» – парольную фразу, «Ш» – полученный шифр. Парольная фраза короче текста, который надо зашифровать, поэтому я повторяю ее заново. Я отдал папе шифр и таблицу, но он не смог прочитать шифровку. Тогда я сказал ему пароль и он легко смог расшифровать, что я написал.

Мама рассказала мне, что существует множество способов сделать невидимые надписи. Есть сложные, когда надо использовать специальные химические вещества. А есть более простые, когда можно использовать то, что есть у нас на кухне. В интернете я прочитал, что самые известные невидимые чернила – это лимонный сок и молоко. Также можно использовать яблочный сок, луковый или свекольный отвар, растворы соды или крахмала. Проявить надписи, сделанные при помощи этих веществ, легко под воздействием тепла: следует использовать утюг, лампочку накаливания, либо открытый огонь (свечку) [11]. В случае же с крахмалом листок надо поместить в слабый йодный раствор – вскоре появятся посиневшие символы. Вместо крахмала можно использовать рисовый отвар.

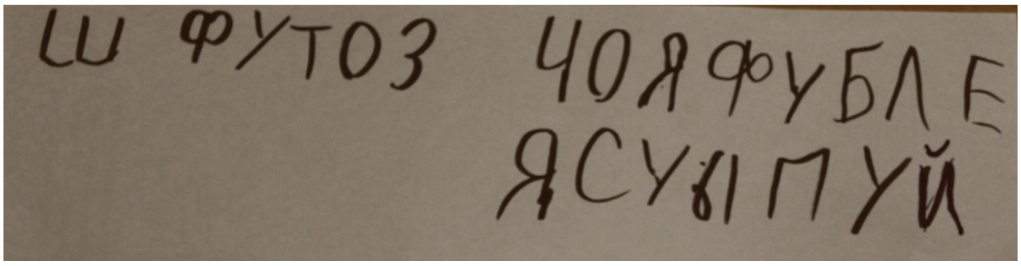


Рис. 14. Моя шифровка

Таблица 2

Текст, пароль и шифр для таблицы Виженера

Т	Я	Л	Ю	Б	Л	Ю	Р	И	С	О	В	А	Т	Ь	К	А	Р	Т	И	Н	Ы
П	Ш	И	Ф	Р	В	И	Ж	Е	Н	Е	Р	А	Ш	И	Ф	Р	В	И	Ж	Е	Н
Ш	Ш	Ф	У	Т	О	З	Ч	О	Я	Ф	У	Б	Л	Е	Я	С	У	Ы	П	У	Й

10. Скрытые послания

Помимо шифрования для защиты сообщений от перехвата использовались различные способы сокрытия самого факта передачи информации. Такие способы в наши дни получили название стеганографические.

Первое послание я написал соком лимона (рис. 15), второе – молоком (рис. 16).

Рис. 15. Тайное сообщение, написанное соком лимона

Рис. 16. Тайное сообщение, написанное молоком

После того, как молоко и сок лимона окончательно высохли, наступил самый интересный момент – выявление тайного. Для того, чтобы проявить надписи, я выбрал утюг, как самое безопасное средство. Процесс проявления письмен оказался безумно увлекателен. Действительно, при нагреве абсолютно казалось бы чистой страницы начинают выступать невидимые ранее буквы.

11. Игры со словами

В 20 веке интерес к сокрытию информации значительно возрастает. Широкое распространение получили так называемые акростихи, в которых «секретное» послание скрывается за начальными буквами строк. Хороший пример в этом плане представляет стихотворение, написанное русским поэтом Н. Гумилевым в 1913 году и адресованное любимой женщине:

«АННА АХМАТОВА»
Ангел лег у края небосклона,
Наклонившись, удивлялся бездне;
Новый мир был синим и беззвездным.
Ад молчал, не слышалось ни стона.
Алой крови робкое биение,
Хрупких рук испуг и содроганье
Миру снов досталось в обладанье
Ангела святое отраженье.
Тесно в мире, пусть живет, мечтая
О любви, о свете и о тени,
В ужасе предвечном открывая
Азбуку своих же откровений».

Мне очень понравилась идея акростиха. И я предложил маме сочинить акростих про меня. Вот что у нас получилось:

«ИЩУКОВ ИВАН»
Иду по жизни я смеясь,
Щекочет жизнь меня.
Учу уроки не ленясь,
Кто первый? Это я!
Опаздываю иногда,
Вот это про меня.
И непослушный иногда,
Ведь не девчонка я
А так хочу я все узнать,
Найти, понять, не опоздать!

12. Шифратор Энигма

В 18 веке стали появляться первые шифрующие машины [9] (рис. 17). Самая известная машина – это машина 20 века, которая называлась «Энигма». Энигму немцы использовали во время Второй мировой войны.

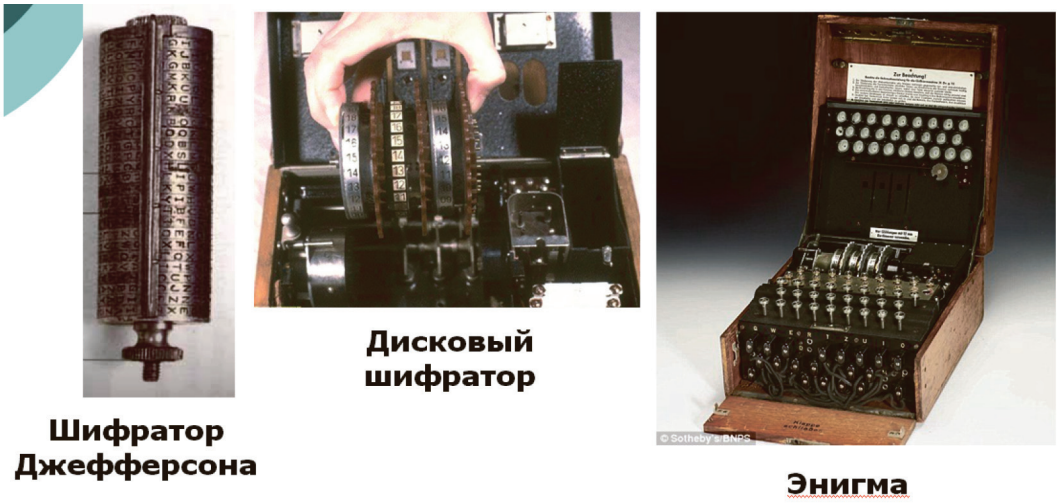


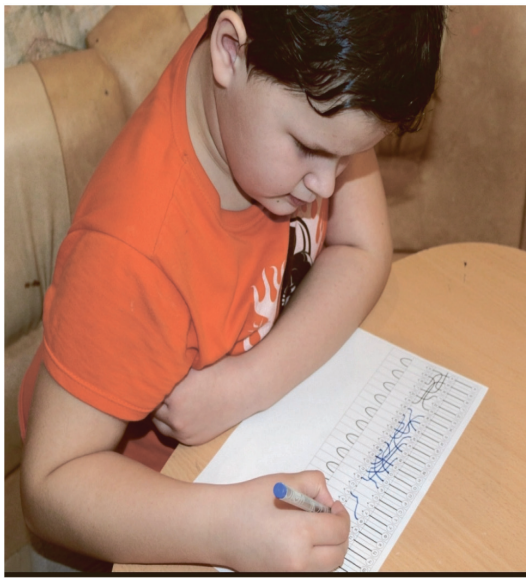
Рис. 17. Шифрующие устройства

Мама рассказала мне про то, как была устроена машина Энигма. И мы приступили к созданию собственного шифратора. Мама распечатала схему, и я соединил буквы разных рядов в произвольном порядке (рис. 18а и 18б). Из каждого буквенного ряда мы склеили цилиндры (рис. 18в), которые надели на ось (рис. 19а).

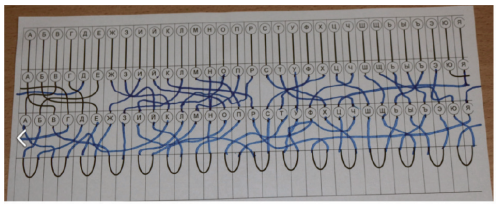
Мама объяснила мне, как работают шифраторы. И сказала, что для того, чтобы сообщение оставалось стойким надо использовать некоторые правила. Например, каждый раз надо использовать новое расположение дисков относительно друг друга.

Я зашифровал сообщение «Так работала машина Энигма» (рис. 19б).

а



б



в

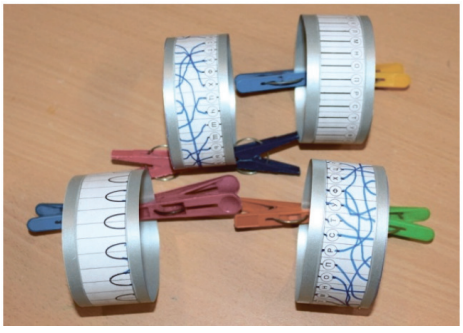


Рис. 18:
а – я соединяю между собой буквы шифратора; б – все буквы соединены;
в – в процессе создания цилиндров

Я отдал папе шифровку (рис. 20) и сам шифратор. Но папа так и не смог прочитать сообщение, сколько он не крутил шифратор.

Заключение

В результате работы над проектом я узнал много новой, интересной информа-

а *б*

Рис. 19:
а – готовый шифратор; б – составляю шифр с помощью своего устройства

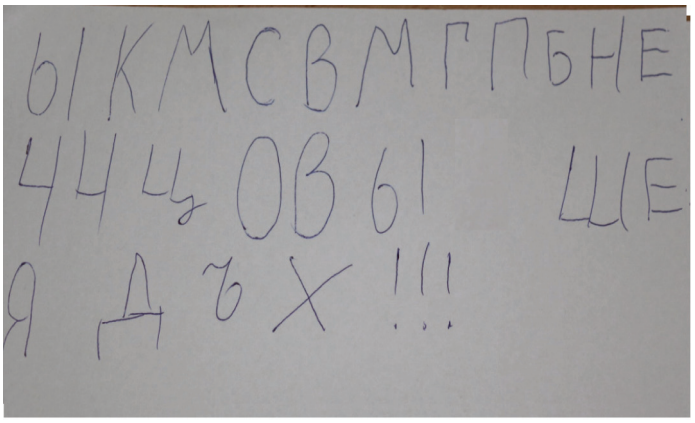


Рис. 20. Зашифрованное сообщение

ции. С помощью мамы я создал различные устройства для шифрования, использовал разные шифры и даже сделал свой шифр из пляшущих человечков. Моя гипотеза была такая: если известно, какой был использован шифр, то можно расшифровать сообщение. Она оказалась частично правильной. Для древних шифров, таких как квадрат Полибия, таблица Энея, шифр Цезаря человеку достаточно знать шифр, чтобы расшифровать сообщение. Это подтвердил и мой эксперимент: и папа, и большинство учеников смогли расшифровать загаданные шифры. Те шифры, которые имеют более сложное устройство, расшифровывать труднее. Так, чтобы расшифровать шифр по таблице Виженера надо знать еще парольную фразу. А чтобы расшифровать шифр, составленный с помощью шифратора наподобие Энигмы, надо знать начальное расположение дисков устройства, а также как они крутятся после каждой зашифрованной буквы. Так что сложные шифры затрудняют прочтение сообщения.

Мама мне объяснила, что сейчас в компьютерах используются совсем другие шифры. Потому что в компьютере информация представляется в двоичном виде – в виде ноликов и единичек. Современные шифры – сложные. Они основаны на использовании сложных математических функций. И они разрабатываются так, чтобы человек не смог расшифровать информацию, даже если ему известен шифр. Поэтому для современных шифров моя гипотеза не верна.

Когда я вырасту, я хочу узнать о таких шифрах побольше. В старших классах я обязательно сделаю исследовательский проект на эту тему!

Опрос учеников из моей школы показал, что эта тема им очень интересна, поэтому я с удовольствием представлю свой доклад на тему «Загадки древних шифров» своим одноклассникам.

Список литературы

1. Кан Д. Взломщики кодов. – https://www.livelib.ru/book/137428/readpart-vzlomschiki-kodov-devid-kan/~3.

2. Жельников В. Криптография от папируса до компьютера. – http://bezopasnik.org/article/book/zhelnikov_-_Cryptography.pdf.

3. Дойл А.К. Пляшущие человечки. – http://www.lib.ru/AKONANDOJL/sh_dancm.txt_with-big-pictures.html.

4. Сведения из истории криптографии. – http://toptodoc.ru/svedeniya-iz-istorii-kriptografii.html.

5. Диск Энея, линейка Энея, книжный шифр. – http://poznayka.org/s87373t1.html

6. Семенова Е. Простейшие методы шифрования текста. – http://xn--i1abbnckbmcl9fb.xn--p1ai/%D1%81%D1%82%D0%B0%D1%82%D1%8C%D0%B8/598604/

7. История Криптографии – http://www.cryptographer.ru/article1.php.

8. Трактат о шифрах // Википедия. – https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BA%D1%82%D0%B0%D1%82_%D0%BE_%D1%88%D0%B8%D1%84%D1%80%D0%B0%D1%85.

9. История криптографии: Учебное пособие. – https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema2.

10. Как сделать невидимые чернила своими руками. Исчезающие чернила. – http://zadachi-po-khimii.ru/zanimatelnaya-khimiya/kak-sdelat-nevidimye-chernila.html.

11. Научные забавы: Что написано молоком… -https://letidor.ru/univit/article/434_nauchnyie_zabavyi_chto_napisano_molokom_24332/

12. Бабаш А.В., Шанкин Г.П. Средневековая криптография. – http://cccp.narod.ru/work/book/kgb/babash_02.html.