Государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа с. Красноармейское муниципального района Красноармейский Самарской области

Секция математики и ИКТ

Шифры и математика

автор: Павлов Кирилл Алексеевич

ученик 5 "Б" класса

ГБОУ СОШ с.Красноармейское

Руководитель: Глазкова Г.Ю.

учитель математики высшей категории

ГБОУ СОШ с.Красноармейское

с. Красноармейское

2016г.

Оглавление

Введение

Мне очень понравились сериалы: "Приключения Шерлока Холмса и Доктора Ватсона", "Семнадцать мгновений весны", где использовались зашифрованные тайные сообщения. А ещё приключения ребят из повести Н. Рыбакова "Кортик" и таинственные знаки на рукоятке этого оружия, некогда принадлежавшего морскому офицеру. Прочитать зашифрованную надпись помогли только ножны, найденные в результате длительных поисков, - ключ к шифровке.

Я узнал, что к шифрованию прибегают довольно часто: в дневниковых записях, в военном деле, на дипломатической службе – вообще в тех случаях, когда нужно сохранить в тайне содержание письменного или устного сообщения.

Оказывается, существует много шифров. Есть и чисто профессиональные: шифры подстановки и замены, шифр RSA, разнообразные типы кодов и т.д. А есть и не на что не похожие шифры. В рассказе Артура Конан Дойля "Пляшущие человечки" Шерлок Холмс сумел понять, что изображенные пляшущие человечки не детские рисунки, а шифр. Знаменитый сыщик разгадал значение каждой фигурки-буквы и тем же самым шифром написал письмо преступнику. Мне захотелось больше узнать о науке криптографии, история которой полна загадок и "шпионских" сюжетов.

Для того чтобы подробно рассмотреть данную тему, я задал несколько вопросов своим одноклассникам:

1) Смотрели ли вы эти фильмы, чем они вам интересны?
2) Интересуетесь ли вы кодами и шифрами?
3) Знаете ли вы современные методы кодирования?
4) Пробовали ли вы когда-либо составлять собственные шифры?

Итак, вот результаты:

70 % учеников интересуются шифрами,

18 % - знают современные методы,

65 % - учеников пробовали зашифровывать свои фразы.

Исходя из полученной информации я решил более подробно рассмотреть этот вопрос, найти его практическое применение и научиться составлять свои шифры.

Цель работы: Рассмотреть различные виды шифрования и их математическое обоснование.

Задачи:

1. Рассмотреть различные виды шифрования
2. Найти их математическое обоснование.
3. Создать свой шифр.
4. Осуществить шифровку и дешифровку текста.

Актуальность этой темы в том интересно узнать с чего всё начиналось, зачем создавались шифры. Значимость для меня в том, что можно создать свой шифр и его будут понимать только те близкие люди, которые вы хотите.

Выводы из работы:

1. Изучив литературу по данной теме, я рассмотрел различные виды шифрования;
1. Я нашел математическое обоснование шифров;
2. На основе изученных шифров я создал свой шифр;
3. Применив полученные знания, я осуществил шифровку и дешифровку текста.

Основная часть
Обзор литературы

1. Мир математики: в 40 т. Т. 2; Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. Де Агостини, 2014.

В книге рассказывается история шифрования через призму развития математической мысли. В книге представлена история шифрования, рассказано о

шифрах перестановки, шифрах замены, шифровании с открытым ключом, рассказывается о шифровальных машинах.

1. Саймон Сингх. Книга шифров. АСТ, Астрель 2007 год.

В "Книге шифров" приводится много интереснейших фактов из истории. Ведь были и войны, в которых выигрывал тот кто знал больше; были секреты, которые нужно было тщательно скрывать от посторонних глаз; была зашифрованная информация, от которой зависели жизни людей. А уж в наше время, значение информации трудно переоценить. И не последнюю роль в развитии криптографии всегда играла математика, в частности, теория чисел. Саймон Сингх рассказывает о постоянной борьбе, которую ведут шифровальщики и взломщики кодов, о различных способах шифрования, которые когда-либо использовались, о способах дешифровки. Рассказывает он и о людях, которые развивали криптографию, о задачах, которые стоят перед криптографами сегодня. Приводятся и задачи, которые можно решить самостоятельно и почувствовать себя дешифровщиком, работающим над текстом.

2. Зубов А.Ю. «Совершенные шифры». Гелиос АРВ 2003 год.

Изложены свойства и конструкции безусловно стойких шифров, названных К. Шенноном совершенными по отношению к различным криптоатакам. Выделяются совершенные шифры с минимально возможным числом ключей, а также стойкие к попыткам обмана со стороны злоумышленника.

История развития шифров и криптографии

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. 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.

Изменение текста с целью сделать его понятным только избранным дало начало науке криптографии (греч. "тайное письмо"). Процесс преобразования текста, написанного общедоступным языком, в текст, понятный только адресату, называют шифрованием, а сам способ такого преобразования называют шифром.

Сначала шифрами пользовались пираты, отмечая расположение кладов, алхимики, купцы, заговорщики. Впоследствии – дипломаты, стремящиеся сохранить тайны переговоров, военачальники, скрывающие от противника отданные распоряжения, разведчики и другие.

Но если есть желающие скрыть смысл текста, то найдутся и те, кто захочет прочитать зашифрованный текст. Методы чтения таких текстов изучает наука криптоанализ.

Кодированием называют изменение исходного текста, цель которого – подготовка к передаче его с помощью каких-то технических устройств. Современные примеры кодирования – это телеграф или цифровая телефонная связь. В частности, все мобильные телефоны. Способ кодирования не является секретом, наоборот, он должен быть известен всем, кто использует данный способ связи.

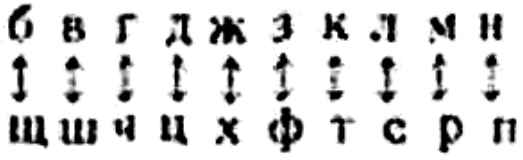
Хотя сами методы криптографии и криптоанализа до недавнего времени были не очень тесно связаны с математикой, но во все времена многие известные математики участвовали в расшифровке важных сообщений. И часто именно они добивались заметных успехов, ведь математики в своей работе постоянно имеют дело с разнообразными и сложными задачами, а каждый шифр — это серьезная логическая задача.

Еще в конце 16 века расшифровкой переписки между противниками французского короля Генриха III занимался один из создателей современной алгебры Франсуа Виет. Испанские инквизиторы изобрели очень сложную тайнопись (шифр), которая все время изменялась и дополнялась. Благодаря этому шифру воинствующая и сильная в то время Испания могла свободно

переписываться с противниками французского короля даже внутри Франции, и эта переписка оставалась неразгаданной. После бесплодных попыток найти ключ к шифру король обратился к Виету. Рассказывают, что Виет, две недели подряд дни и ночи просидев за работой, все же нашел ключ к испанскому шифру. После этого неожиданно для испанцев Франция стала выигрывать одно сражение за другим. Испанцы долго недоумевали. Наконец им стало известно, что шифр для французов уже не секрет и что виновник его расшифровки – Виет. Будучи уверенными, в невозможности разгадать способ тайнописи людьми, они обвинили Францию перед папой римским и инквизицией в кознях дьявола, а Виет был обвинен в союзе с дьяволом и приговорен к сожжению на костре. К счастью для науки, он не был выдан инквизиции.

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: как-то в уме извлек квадратный корень из 53-значного числа. Однако никакого математического образования он не получил, занимаясь самостоятельно. Он считал себя основателем новой науки – криптографии.

И во время второй мировой войны этой работой занимались лучшие математики воюющих стран. Например, одним из лучших дешифровальщиков в Англии был известный математик Алан Тьюринг. Он в 1943 г. с помощью первых вычислительных машин расшифровал германские послания, закодированные шифровальной машиной "Энигма".



Постепенно роль математических методов в криптографии стала возрастать, и за последнее столетие они существенно

изменили эту древнюю науку.

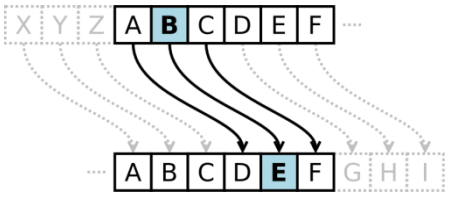
Первые шифры были очень несложными. Например, русские дипломаты XV—XVI веков применяли так называемую «тарабарскую грамоту», или, как ее еще называли "хитрую литорею", в которой все гласные буквы оставались неизменными, а согласные заменялись одна другой по следующей схеме: (в первой строке согласные идут в обычном порядке, а во второй строке — в обратном) Например, вместо «Великий государь» получал "Шеситий чолуцамь".

В рассказе А. Конан-Дойля "Пляшущие человечки" описан способ шифрования при помощи рисунков (буквы заменялись на изображения пляшущих человечков). Например, одна из шифровок, разгаданная неподражаемым Шерлоком Холмсом:

Фраза означала: "Никогда".

Код Цезаря

К шифрам замены относится и один из первых известных кодов в истории человечества – **код Цезаря**, применявшийся в древнем Риме. Суть этого кода состояла в том, что буква алфавита заменялась другой с помощью сдвига по алфавиту на одно и то же число позиций – на три места (понятно, что при этом последние буквы алфавита заменялись последовательно на первые).



Такой же шифр применял другой римский император – Август Октавиан, только он сдвигал буквы не на 3, а на 4 места.

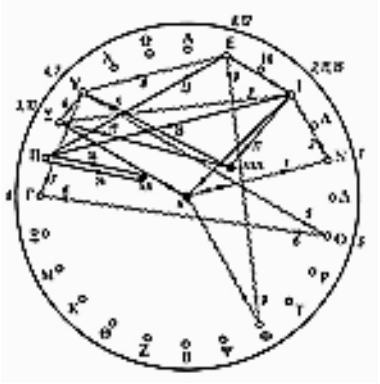
Несмотря на свою популярность, шифр может быть легко взломан, ведь алгоритм его незамысловат: каждая буква исходного текста заменяется символом, который располагается на X позиций левее или правее шифруемой буквы в

алфавите. Предположим, что диапазон, на который следует сдвигаться 3, а направление движения вправо (сдвиг, который использовал Цезарь).

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

Зашифруем слово "математика", получим "пгхипгхлнг". Величину сдвига можно рассматривать как ключ шифрования.

Диск Энея



Были и другие способы защиты информации, разработанные в античные времена. Древнегреческий полководец Эней Тактика в IV веке до н.э. предложил устройство, названное впоследствии "диском Энея". Принцип его был прост: на диске диаметром 10-15 см и толщиной 1-2 см высверливались отверстия по числу букв алфавита. В центре диска помещалась "катушка" с намотанной на ней ниткой достаточной длины. При шифровании нитка "вытягивалась" с катушки и последовательно протягивалась через отверстия, в соответствии с буквами шифруемого текста. Диск и являлся посланием. Получатель послания последовательно вытягивал нитку из отверстий, что позволяло ему получать передаваемое сообщение, но в обратном порядке следования букв. При перехвате диска недоброжелатель имел возможность прочитать сообщение тем же образом, что и получатель. Но Эней предусмотрел возможность легкого уничтожения передаваемого сообщения при угрозе захвата диска. Для этого было достаточно выдернуть "катушку" с закрепленным на ней концом нити до полного выхода всей нити из всех отверстий диска.

Квадрат Полибия

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

В Древнем Риме хорошо усвоили греческое наследие и придумали немало собственных способов шифрования. Например, квадрат Полибия изобретенный во II веке до н.э., не вышел из употребления до сих пор. Устроен он так: все или почти все буквы алфавита располагаются в квадрате или прямоугольнике соответствующего размера, - для латинского алфавита это 5x5, для русского – 5x6. В каждую клетку этого квадрата записывалась одна буква. (В греческом варианте одна клетка оставалась пустой, в латинском – в одну клетку помещали две буквы ***i*** и ***j***.) В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел.

Пример 1. 13 34 22 24 44 34 15 42 22 34 43 45 32

Это сообщение записано при использовании латинского варианта квадрата Полибия, в котором буквы расположены в алфавитном порядке.

("Cogito, ergo sum" – лат, "Я мыслю, следовательно, существую").

Каким должен быть шифр

При шифровании должны выполняться определенные условия. Во-первых, различные буквы должны обозначаться разными знаками: иначе получатель должен будет гадать, какую из нескольких букв обозначает тот или иной знак. Далее, шифр должен быть трудно разгадываем — легкие шифры можно применят лишь при условии, что у противника нет времени на разгадку. Наконец, секретность шифра должна сочетаться со сравнительной несложностью операции кодирования и раскодирования: иначе на них уйдет столько времени, что переданная информация устареет. А если раскодирование потребует слишком

много усилий, то можно оказаться в положении легендарного писца. Он писал за плату письма на восточном базаре, но при этом взимал плату еще и как гонец. Дело было в том, что написанное им никто, кроме него самого понять не мог.

Поскольку в каждом шифре применяют конечное число различных знаков, то их можно перенумеровать и вместо самих знаков использовать их номера. Будем для простоты рассматривать шифры, в которых нет избыточности. Тогда число знаков равно числу букв в алфавите плюс знаки, обозначающий пробел между словами, точку, запятую, тире. Для русского языка можно обойтись 35 знаками.

При шифровании каждая буква или знак заменяются иной буквой или знаком. Но вместо букв и знаков можно брать соответствующие им числа. Тогда шифрование сведет к тому, что вместо одних чисел, соответствующих исходной букве или знаку, надо взять другое число. Например, напишем такую таблицу:

1	А	7	8	Ж	19	15	Н	20	22	Ф	9	29	Ы	5
2	Б	11	9	З	12	16	О	13	23	Х	18	30	Ь	14
3	В	1	10	И	17	17	П	22	24	Ц	30	31	Э	25
4	Г	2	11	Й	32	18	Р	10	25	Ч	27	32	Ю	28
5	Д	35	12	К	6	19	С	31	26	Ш	29	33	Я	26
6	Е	33	13	Л	3	20	Т	4	27	Щ	8	34	.	21
7	Ё	24	14	М	15	21	У	16	28	Ъ	34	35	,	23

В таблице показано (красным цветом), каким числом заменяется каждое из 35 чисел. Зашифруем слово "математика". Сначала запишем слово цифрами 14,1,20,6, 14,1,20,10,12,1. А теперь смотрим в таблицу и видим, что числу 14 соответствует число 15, т.е. буква "н", числу 1 – число 7, т.е. буква "ё", числу 20 – число 4, т.е. буква "г", числу 6 – число 33, т.е. буква "я", числу 10 – число 17, т.е.

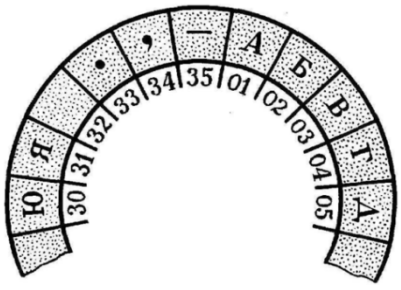
буква "п", числу 12 – число 6, т.е. буква "е". Получаем слово "нёгянёгпеё", т.е. "математика".

Используя шифр Цезаря, можно конструировать значительно более сложные шифры замены. Выберем какое-нибудь слово, например, "география". Если в нем есть повторяющиеся буквы, то оставим только первую из них, получим "георафия". Затем припишем к полученной последовательности букв справа все еще не использованные буквы алфавита в естественном порядке. В полученной последовательности каждая буква русского алфавита встречается точно один раз, поэтому если мы над ней запишем обычный алфавит в правильном порядке, получим правило замены букв, которое можно использовать для шифрования текстов:

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

Например, фраза " Я люблю математику" будет выглядеть "Ю жэежэ згпфзгпбдс". Для того чтобы еще сильнее усложнить расшифровку текста, слова в нем часто пишут слитно, без пробелов: "Южэежэзгпфзгпбдс".

Но запоминать наизусть такие таблицы, чтобы пользоваться ими при шифровании, очень трудно, а хранить их при себе по понятным причинам весьма нежелательно. Лучше иметь простое правило, позволяющее для каждого числа находить соответствующее ему число. А такие правила дают методы математики.



Шифры и арифметика остатков

Один из методов кодирования заключается в следующем. Разделим кольцо на 35 равных частей, занумеруем их и пометим каждую буквой или знаком препинания. А теперь выберем какое-нибудь число а ("ключевое число" шифра) и повернём кольцо вокруг центра по часовой стрелке так, чтобы каждая часть переместилась на а шагов. Это и задаёт шифр (на рисунке перед однозначными числами написан еще 0: иначе "15" можно прочитать как "пятнадцать" и как "один" и "пять").

Например, если а = 7, то часть, помеченная числом 01, перейдет в часть, помеченную числом 08, а это значит, что букве "А" при кодировании отвечает число 08 (буква "З"). И теперь слово "математика" = "20826132082616188".

Таким образом, каждая буква или знак записываются двузначным числом. Адресату для расшифровки надо разбить полученную последовательность цифр на двузначные числа, вычесть из каждого ключевое число и заменить полученное число буквой алфавита или знаком препинания. Например, 111322112408281603 – 11 13 22 11 24 08 28 16 03 = 04 06 14 04 17 01 21 09 31 = ГЕОГРАФИЯ.

Более сложный шифр получается, если заменить сложение умножением. Будем, например, умножать номера всех букв на 2. Конечно, если произведение окажется больше 35, надо заменять его остатком от деления на 35. Например, буква "ц" получит при шифровке номер 13, так как номер буквы "ц" равен 24, а при делении 24·2 = 48 на 35 получается остаток 13. Это преобразование сложнее, чем сложение и запутаннее.

Зашифруем слово "математика" : м – 14, а – 1, т – 20, е – 6, и – 10, к – 12.

- 14·2:35 = 0(ост.28) – ъ
- 1·2:35 = 0(ост.2) – б
- 20·2:35 = 1(ост.5) – д
- 6·2:35 = 0(ост.12) – к
- 10·2:35 = 0(ост.20) – т
- 12·2:35 = 0(ост.24) – ц

Получилось: **ъбдкъбдтцб**

Коды можно получить также, заменяя умножение возведением в степень.

Магический квадрат

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 ×3, если не принимать во внимание его повороты. Магических квадратов 4 × 4 насчитывается уже 880, а число магических квадратов размером 5 × 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был очень сложным. В квадрат размером 4 × 4 вписывались числа от 1 до 16. Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу — 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

Шифрование по магическому квадрату производилось следующим образом. Например, требуется зашифровать фразу: "Без наук как без рук". Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу.

В пустые клетки ставится точка. После этого шифрованный текст записывается в строку (считывание производится слева направо, построчно): кзезакбкаукенурБ

16 к	3 з	2 е	13 з
5 а	10 к	11 б	8 к
9 а	6 у	7 к	12 е
4 н	15 у	14 р	1 Б

При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел "магического квадрата".

Матричный способ

Познакомимся с одним очень простым способом шифрования. Чтобы воспользоваться им для шифровки и расшифровки (кодирования и декодирования), достаточно знать лишь простейшую арифметику, порядок букв в алфавите и помнить всего… четыре числа. А расшифровать ваш текст непосвященному человеку будет абсолютно не под силу.

Для кодирования текста на русском языке занумеруем все буквы по месту их расположения в алфавите – от 1 до 33, добавив 34-ю – знак " (пробел, тире, точка, в общем знак, означающий все, что угодно, исходя из смысла послания).

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	"
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

Зашифрую свою фамилию – К. Павлов и каждую букву заменю соответствующей цифрой. Получим последовательность: 12, 34, 17, 1, 3, 13, 16, 3. Построим из этой последовательности две матрицы: $\begin{pmatrix} 12 & 34 \\ 17 & 1 \end{pmatrix}$ и $\begin{pmatrix} 3 & 13 \\ 16 & 3 \end{pmatrix}$ Зашифруем это сообщение с помощью еще одной матрицы $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ - назовем ее

кодирующей матрицей, - по следующему правилу:

$$\begin{pmatrix} X & Y \\ Z & T \end{pmatrix} \cdot \begin{pmatrix} P & Q \\ R & S \end{pmatrix} = \begin{pmatrix} X \cdot P + Y \cdot R & X \cdot Q + Y \cdot S \\ Z \cdot P + T \cdot R & Z \cdot Q + T \cdot S \end{pmatrix}$$

Зашифруем:

$$\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 12 & 34 \\ 17 & 1 \end{pmatrix} = \begin{pmatrix} 2 \cdot 12 + 3 \cdot 17 & 2 \cdot 34 + 3 \cdot 1 \\ 1 \cdot 12 + 2 \cdot 17 & 1 \cdot 34 + 2 \cdot 1 \end{pmatrix} = \begin{pmatrix} 75 & 71 \\ 46 & 36 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 13 \\ 16 & 3 \end{pmatrix} = \begin{pmatrix} 2 \cdot 3 + 3 \cdot 16 & 2 \cdot 13 + 3 \cdot 3 \\ 1 \cdot 3 + 2 \cdot 16 & 1 \cdot 13 + 2 \cdot 3 \end{pmatrix} = \begin{pmatrix} 54 & 35 \\ 35 & 19 \end{pmatrix}$$

Теперь можно передать адресату следующий набор чисел: 75, 71, 46, 36, 54, 35, 35, 19. Мы знаем и более сложный способ передачи: 7571463654353519. Для того чтобы прочесть сообщение, нужно знать декодирующую матрицу $\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ и проделать с полученным текстом следующее:

$$\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 75 & 71 \\ 46 & 36 \end{pmatrix} = \begin{pmatrix} 2 \cdot 75 - 3 \cdot 46 & 2 \cdot 71 - 3 \cdot 36 \\ -1 \cdot 75 + 2 \cdot 46 & -1 \cdot 71 + 2 \cdot 36 \end{pmatrix} = \begin{pmatrix} 12 & 34 \\ 17 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 54 & 45 \\ 35 & 19 \end{pmatrix} = \begin{pmatrix} 2 \cdot 54 - 3 \cdot 35 & 2 \cdot 35 - 3 \cdot 19 \\ -1 \cdot 54 + 2 \cdot 35 & -1 \cdot 35 + 2 \cdot 19 \end{pmatrix} = \begin{pmatrix} 3 & 13 \\ 16 & 3 \end{pmatrix}$$

Получим 12, 34, 17, 1, 3, 13, 16, 3, что после перевода в буквы будет означать К. Павлов, то есть исходный текст.

Ясно, что никто посторонний, не знающий ни кодирующей, ни декодирующей матрицы, получить этот текст не сможет.

Однако матричный способ шифрования не смог бы существовать, если бы в качестве кодирующей можно было брать только матрицу $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$

На самом деле таких матриц бесконечно много, придумывать их очень легко. И вообще вы можете менять свою систему «тайнописи» каждый день. Для этого

нужно знать очень немного – уметь любые две матрицы «перемножать», т.е. по определенному правилу составлять из них третью.

Практическая часть

ЗАДАЧА №1"КВАДРАТ ПОЛИБИЯ"

Буквы русского алфавита я расположил в квадрате 6х6 в своем порядке

	1	2	3	4	5	6
1	А	К	У	Ъ	Я	
2	Ё	Б	Л	Ф	Ы	"
3	П	Ж	В	М	Х	Ь
4	Ч	Р	З	Г	Н	Ц
5	Э	Ш	С	И	Д	О
6		Ю	Щ	Т	Й	Е

Сначала я зашифровал простые слова:

Г	Е	О	М	Е	Т	Р	И	Я
44	66	56	34	66	64	42	54	15

ШИФР: 446656346664425415

Ф	У	Н	К	Ц	И	Я
24	13	45	12	46	54	15

ШИФР: 24134512465415

Я решил зашифровать более сложную фразу – М.В. Ломоносова "Математику уже за то любить следует, что она ум в порядок приводит".

Мне понадобился знак " (знаки препинания, его я тоже внес в таблицу). Получилось:

2634116466341164541213133366431164562362225464365323665513666426416456564511133433315642155556123142543356555464 26

ЗАДАЧА №2 "ШИФР ЦЕЗАРЯ"

Я опять решил зашифровать всем известное высказывание о математике Г. Галилея "Математика – это язык, на котором написана книга природы".

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

Получилось: ж ь м я ж ь м в д ь ч м и щ б х д з ь д и м и к ж з ь й в л ь з ь д з в э ь й к в к и ю х

ЗАДАЧА №3"МАТРИЧНЫЙ СПОСОБ"

Возьмем высказывание о математике В. Чкалова "Полет – это математика ".

Составим таблицу, в которой каждой букве русского алфавита будут соответствовать числа, взятые по порядку от 1 до 33(34 - символ пробела ␣)

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	␣
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

Заменим каждый символ этого сообщения соответствующим числом из таблицы 17 16 13 6 20 34 31 20 16 34 14 1 20 6 14 1 20 10 12 1

Построим из этой последовательности матрицы: $\begin{pmatrix}17 & 16\\13 & 6\end{pmatrix}, \begin{pmatrix}20 & 34\\31 & 20\end{pmatrix}, \begin{pmatrix}16 & 34\\14 & 1\end{pmatrix}, \begin{pmatrix}20 & 6\\14 & 1\end{pmatrix}, \begin{pmatrix}20 & 10\\12 & 1\end{pmatrix}$

Кодирующую матрицу я придумал свою: $\begin{pmatrix}3 & 2\\4 & 3\end{pmatrix}$

Получим:

$$\begin{pmatrix}17 & 16\\13 & 6\end{pmatrix}\cdot\begin{pmatrix}4 & 5\\3 & 4\end{pmatrix} = \begin{pmatrix}116 & 149\\70 & 89\end{pmatrix}, \quad \begin{pmatrix}20 & 34\\31 & 20\end{pmatrix}\cdot\begin{pmatrix}4 & 5\\3 & 4\end{pmatrix} = \begin{pmatrix}182 & 236\\184 & 235\end{pmatrix},$$

$\begin{pmatrix}16 & 34\\14 & 1\end{pmatrix}\cdot\begin{pmatrix}4 & 5\\3 & 4\end{pmatrix}=\begin{pmatrix}166 & 216\\59 & 74\end{pmatrix}$, $\begin{pmatrix}20 & 6\\14 & 1\end{pmatrix}\cdot\begin{pmatrix}4 & 5\\3 & 4\end{pmatrix}=\begin{pmatrix}98 & 124\\59 & 74\end{pmatrix}$,

$\begin{pmatrix}20 & 10\\12 & 1\end{pmatrix}\cdot\begin{pmatrix}4 & 5\\3 & 4\end{pmatrix}=\begin{pmatrix}110 & 140\\51 & 64\end{pmatrix}$

Теперь можно передать адресату следующий набор чисел:116 149 70 89 182 236 184 235 166 216 59 74 98 124 59 74 110 140 51 64

Или более сложный способ передачи: 116149708918223618423516621659749812459741101405164.

При получении необходимо расшифровать:

$\begin{pmatrix}116 & 149\\70 & 89\end{pmatrix}\cdot\begin{pmatrix}4 & -5\\-3 & 4\end{pmatrix}=\begin{pmatrix}17 & 16\\13 & 6\end{pmatrix}$, $\begin{pmatrix}182 & 236\\184 & 235\end{pmatrix}\cdot\begin{pmatrix}4 & -5\\-3 & 4\end{pmatrix}=\begin{pmatrix}20 & 34\\31 & 20\end{pmatrix}$,

$\begin{pmatrix}166 & 216\\59 & 74\end{pmatrix}\cdot\begin{pmatrix}4 & -5\\-3 & 4\end{pmatrix}=\begin{pmatrix}16 & 34\\14 & 1\end{pmatrix}$, $\begin{pmatrix}98 & 124\\59 & 74\end{pmatrix}\cdot\begin{pmatrix}4 & -5\\-3 & 4\end{pmatrix}=\begin{pmatrix}20 & 6\\14 & 1\end{pmatrix}$,

$\begin{pmatrix}110 & 140\\51 & 64\end{pmatrix}\cdot\begin{pmatrix}4 & -5\\-3 & 4\end{pmatrix}=\begin{pmatrix}20 & 10\\12 & 1\end{pmatrix}$.

Получим: 17 16 13 6 20 34 31 20 16 34 14 1 20 6 14 1 20 10 12 1, что после перевода в буквы будет означать "Полет – это математика ".

ЗАДАЧА №4 "МАГИЧЕСКИЙ КВАДРАТ"

Я зашифрую слова А.В. Суворова " Математика - гимнастика ума".

11	**24**	**7**	**20**	**3**
4	**12**	**25**	**8**	**16**
17	**5**	**13**	**21**	**9**
10	**18**	**1**	**14**	**22**
23	**6**	**19**	**2**	**15**

Буквы этой фразы впишу последовательно в квадрат согласно записанным в них числам: позиция буквы в предложении соответствует порядковому числу.

В пустые клетки ставим точку. После этого шифрованный текст записывается в строку (считывание производится слева направо, построчно):

11 **г**	24 **.**	7 **т**	20 **а**	3 **т**
4 **е**	12 **и**	25 **.**	8 **и**	16 **с**
17 **т**	5 **м**	13 **м**	21 **у**	9 **к**
10 **а**	18 **и**	1 **М**	14 **н**	22 **м**
23 **а**	6 **а**	19 **к**	2 **а**	15 **а**

Получаем: г.татеи.истммукаиМнмаакаа

ЗАДАЧА №5"СВОЙ ШИФР"

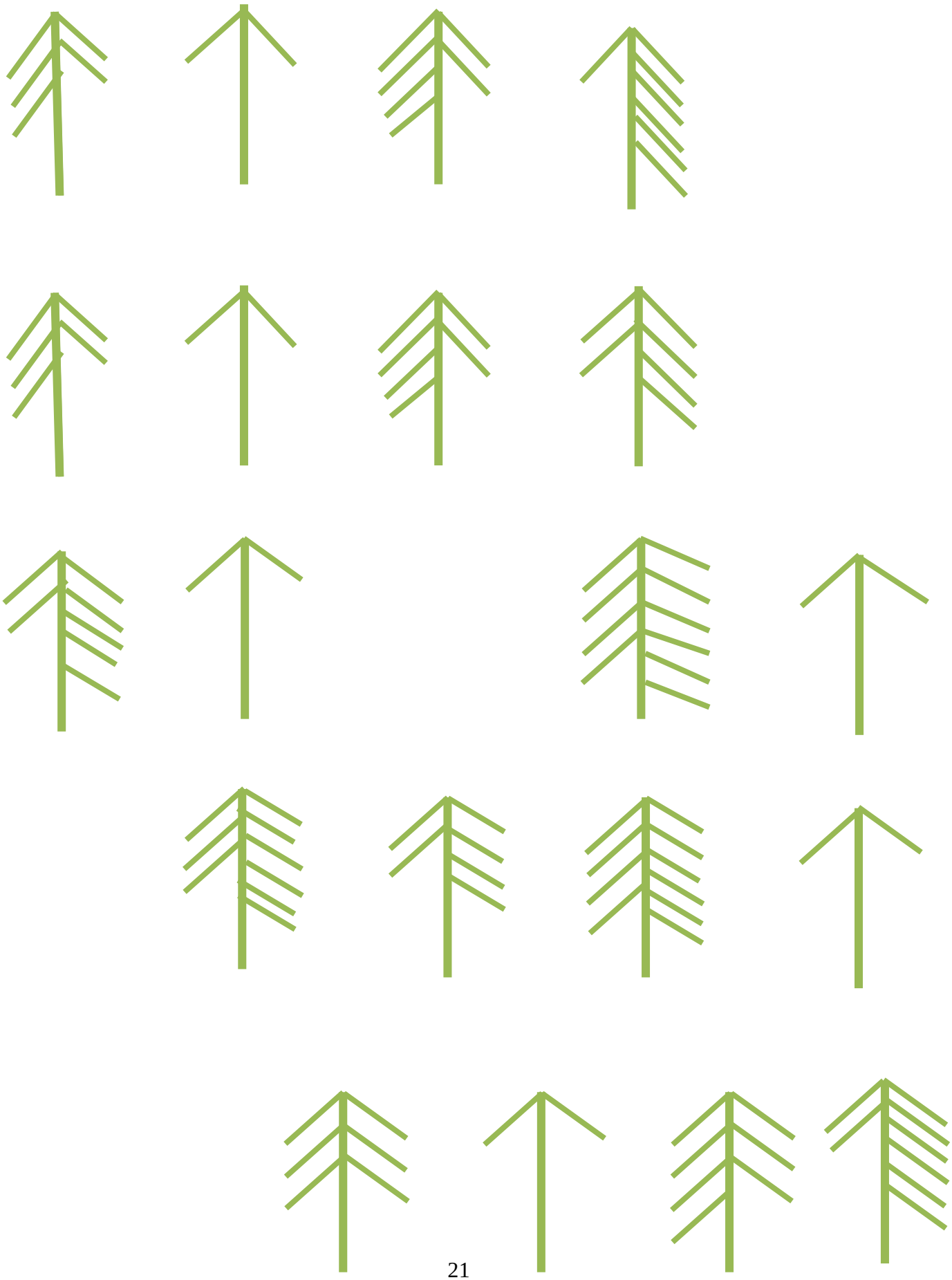
Я придумал свой шифр и назвал его "Ёлки".

–	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	–	–	-

Примеры обозначения

Р **О** **Т** **А**

Зашифрую фразу: "Математика – царица наук".



ЗАДАЧА №6"ШТАКЕТНИК"

Мне очень понравился шифр "штакетник". Запишем два слова: "геометрия и география". Первая буква пишется сверху, вторая снизу, и так по очереди. Получается две линии из букв. А потом они просто записываются в строку, как будто две перекладины у штакетника выстроили в одну палку.

Г О Е Р Я Е Г А И
Е М Т И Г О Р Ф Я

Получится:
ГОЕРЯЕГАИЕМТИГОРФЯ

Надо расшифровать: МТМТК – ООЕАСУАКНУАЕАИАКРЛВИЛЖНААК

Чтобы прочесть, нужно разделить текст на две части и из каждой поочередно выписывать по букве. Зашифрованная фраза: "Математика - королева и служанка наук". (Э. Т. Белл)

Дидактическая игра "РАСШИФРУЙКА"

В рамках недели математики на классном часе мною была проведена игра "РАСШИФРУЙКА".

Правила игры.

Учащиеся делятся на группы по 2-3 человека. Распределяются обязанности. Например, в каждой должен быть руководитель группы, главный шифровальщик, оформитель – докладчик.

Каждая группа получает одинаковые задания. Группа, выполнившая задание первой, показывает ответ и проверяет качество выполнения работы другими группами.

Группа ребят, выполнившая все задания первой, выиграла.

Приведу задания для групп.

1. Используя в качестве декодирующей матрицу $\begin{pmatrix} -1 & 3 \\ 1 & -2 \end{pmatrix}$

расшифруйте сообщение: 72, 11О, 31, 45, 159, 80, 63, 33, 776431,

24, 79, 122, 33, 46, 33, 50, 15, 22, 77, 60, 32, 22, 170, 68, 68, 23,81,59,33,20.

Ответ: "Учиться можно только весело..." (А. Франс).

2. Название какого литературного произведения зашифровано числом, если каждая буква заменена ее номером в алфавите:

а)171810121333225615103320161411916116181

("Приключения Тома Сойера")

б)191733202119201329610418212612 10

("Спят усталые игрушки")

3. Расшифруем стихотворение:

Йков пж ёвтро йнкфуб,

Стрънв хз сртв -

Джупв д рмпр уфхщкфуб.

К ерпкф Ур ёдртв.

Принцип решения: все буквы сдвинуты на 2, то есть В ⟹ А, Г ⟹ Б и т. д.

Ответ: Зима не даром злится,

Прошла ее пора -

Весна в окно стучится

И гонит со двора.

4. Шифровичок-тренировичок:

Расшифруйте послание, используя таблицу – кодификатор.

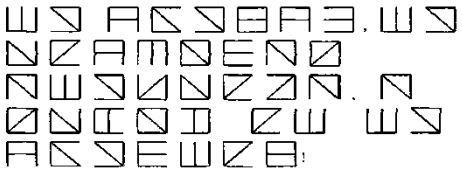
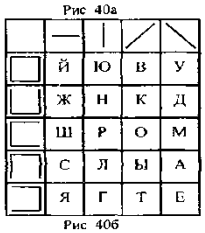


Рис 40а

Ответ: «Не смейся, не дослушав анекдота, а вдруг он не смешной!»



	—	|	／	＼
	Й	Ю	В	У
	Ж	Н	К	Д
	Ш	Р	О	М
	С	Л	Ы	А
	Я	Г	Т	Е

Рис 40б

Заключение

Я считаю, что шифры – это одна из самых интересных и актуальных тем. Шифры использовались, используются и будут использоваться, т.к. они необходимы во многих областях и помогают людям решить те или иные логические задачи. Благодаря своей работе я узнал о связи шифров и математики. И о том, что с помощью различных математических методов можно зашифровать информацию. В работе я познакомился с шифрами древности, рассмотрел шифры подстановки (замены), шифры перестановки, матричный способ кодирования. При работе с этими шифрами не обойтись без математических методов (поиск закономерностей, сравнение, комбинаторика, частотный анализ). На их основе придуманы свои простые шифры и зашифрованы известные высказывания о математике.

Я научился шифровать и дешифровать текст при помощи некоторых видов шифров. Особенно мне понравились математические шифры. Я думаю, что каждый сможет составить собственный шифр, кто-то сложнее, кто-то проще, придумав просто любые обозначения для каждой буквы алфавита.

Я планирую на следующий год рассмотреть и изучить более сложные шифры, а также подумать придумать небольшую программу для их написания.

Работа по данной теме была интересной и увлекательной.

Список используемой литературы

1Гатчин Ю.А., Коробейников А.Г. «Основы криптографических алгоритмов». Учебное пособие. Санкт-Петербургский государственный университет информационных технологий, механики и оптики 2002 год.

2. Зубов А.Ю. «Совершенные шифры». Гелиос АРВ 2003 год.
3. Мир математики: в 40 т. Т. 2; Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. Де Агостини, 2014.
4. Депман И.Я. «За страницами учебника математики» - Просвещение. 1989 г.
5. Каратаева Т.А. «Час занимательной математики» - Москва 2003 г.
6. Карпенко А.Г. «Занимательные шифры-головоломки» Журнал «Квант» №5 1977 г.
7. Козина М.Е. «Сборник элективных курсов по математике"Волгоград 2006 г
8. Шеврин Л.Н. «Учебник-собеседник по математике» - Просвещение. 1989 г.
9. Виленкин Н.Я Математика и шифры. – Квант, № 8, 1997.
10. Аршинов М.Н., Садовский Л.Е. Коды и математика. – М.: Наука, 1983.
11. Гонина Е.Е. Шифры, коды, тайны. – Живая математика, № 1, 2008.
12. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах: Популярно о современной криптографии — М.: Теис, 1994.
13. Ященко В.В., ред. Введение в криптографию. – М: МЦНМО, 2000.
14. http://ru.wikipedia.org
15. http://citforum.ru/security/cryptography/yaschenko/78.html
16. http://www.wikiznanie.ru/ru-wz/index.php/Шифр

Приложение

Шифр Цезаря

Шифр Цезаря называют в честь Юлия Цезаря, который согласно «Жизни двенадцати цезарей» Светония использовал его со сдвигом 3, чтобы защищать военные сообщения. **Гай Ю́лий Це́зарь** (100 или 102до н. э. – 44 до н. э.) – древнеримский государственный и политический деятель, диктатор, полководец, писатель. Хотя Цезарь был первым зафиксированным человеком использующим эту схему, другие шифры подстановки, как известно, использовались и ранее. Его племянник, Август, также использовал этот шифр, но со сдвигом вправо на один, и он не повторялся к началу алфавита. Есть доказательства, что Юлий Цезарь использовал также и более сложные схемы. Часто для удобства использования шифра Цезаря используют два диска разного диаметра с нарисованными по краям дисков алфавитами, насаженных на общую ось. Изначально диски поворачиваются так, чтобы напротив каждой буквы алфавита внешнего диска находилась также буква алфавита малого диска. Если теперь повернуть внутренний диск на несколько символов, то мы получим соответствие между

символами внешнего диска и внутреннего - шифр Цезаря. Получившийся диск можно использовать как для шифрования, так и для расшифровки. Например, если внутреннее колесо повернуть так, чтобы символу A внешнего диска соответствовал символ D внутреннего диска, то мы получим шифр со сдвигом 3 влево.

Естественным развитием шифра Цезаря стал **шифр Виженера.** Этот шифр удобнее всего представлять себе как

шифр Цезаря с переменной величиной сдвига. Чтобы знать, насколько сдвигать очередную букву открытого текста, заранее договариваются о способе запоминания сдвигов. Сам Виженер предлагал запоминать ключевое слово, каждая буква которого своим номером в алфавите указывает величину сдвига. Ключевое слово повторяется столько раз, сколько нужно для замены всех букв открытого текста. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв открытого текста: 3191319131913191... Например, открытый текст КРИПТОГРАФИЯ при таком способе шифрования преобразуется в шифртекст НССРХПЛСГХСА. **Блез де Виженер** (1523-1596) был французским дипломатом и криптографом. Виженер родился в деревне Saint-Pourçain (англ.). В возрасте 17 лет он поступил младшим секретарем на дипломатическую службу к Вормсский эдикт. В возрасте 24 он поступил на службу к герцогу Невер. В 1954 и 1966 он посетил Рим с двухгодичной дипломатической миссией. В этих поездках, он познакомился с книгами о криптографии и самой криптографией. Умер в 1596 от рака горла.

Первое точное документированное описание многоалфавитного шифра было сформулировано Леоном Баттиста Альберти в 1467 году. Для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, Иоганн Трисемус в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера. То, что сейчас известно под шифром Виженера, впервые описал Джованни Батиста Беллазо в своей книге La cifra del. Sig. Giovan Battista Bellaso. Он использовал идею Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую

букву. Блез Виженер представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему. Давид Кан в своей книге "Взломщики кодов" отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания». Шифр Виженера имел репутацию исключительно стойкого к "ручному" взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера невзламываемым в своей статье "Алфавитный шифр», опубликованной в детском журнале в 1868 году. Это представление было опровергнуто после того, как Казиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

Шифр "Сциталь"

Этот шифр известен со времен войны Спарты и Персии против Афин. Спартанский полководец Лисандр подозревал персов в возможной измене, но не знал их тайных планов. Его агент в стане персов прислал шифрованное сообщение, которое позволило Лисандру опередить персов и разгромить их. Шифрованное сообщение было написано на поясе официального гонца от персов следующим образом: агент намотал пояс на сциталь (деревянный цилиндр определенного диаметра) и написал на поясе сообщение вдоль сциталя; потом он размотал пояс, и получилось, что поперек пояса в беспорядке написаны буквы. Гонец не догадывался, что узор на его красивом поясе на самом деле содержит зашифрованную информацию. Лисандр взял сциталь такого же диаметра, аккуратно намотал на него пояс и вдоль сциталя прочитал сообщение от своего агента. Например, если роль сциталя выполняет карандаш с шестью гранями, то открытый текст КРИПТОГРАФИЯ может быть преобразован в шифр текст

РПОРФЯКИТГАИ. Шифр текст может быть и другим, так как он зависит не только от диаметра карандаша.

Джероламо Кардано (24 сентября 1501 – 21 сентября 1576) — итальянский

математик, механик, астролог, философ и медик. Учился в университетах Павии и Падуи. Занимался сначала исключительно медициной, а с 1534 был профессором математики в Милане и Болонье; однако для увеличения скромных доходов профессоров того времени продолжал заниматься врачеванием, а также составлял альманахи. Кардано внёс значительный вклад в развитие алгебры: его имя носит формула Кардано для нахождения корней кубического неполного уравнения вида

$\mathbf{x^3 + ax + b = 0}$. Он же первым в Европе стал использовать отрицательные корни уравнений. Кардано также занимался механикой: изобретенные им карданный подвес и карданная передача до сих пор широко применяются в технике. В 1550 году предложил простую решётку для шифрования сообщений. Он планировал маскировать сообщения под обычное послание, так что в целом они не были полностью похожи на шифрованные. Такое замаскированное сообщение считается примером стеганографии. Но имя Кардано относилось к решёткам, которые могли и не быть изобретением Кардано, тем не менее, шифры, реализованные с использованием картонных решеток, принято называть решётками Кардано. Известно, что Кардинал Ришелье (1585—1642) был приверженцем решётки Кардано и использовал её в личной и деловой переписке. К концу XVII века первые решётки Кардано уже почти не использовались, но иногда они всё же появлялись в виде зашифрованных посланий и в качестве литературных диковинок. Например, Джордж Гордон Байрон пользовался решёткой Кардано, но скорее для демонстрации литературных навыков, чем для серьёзного шифрования. Из сочинений

Кардано интересны: «Ars magna, sive de regulis Algebrae»; «Ars magna Arithmeticae»; «Exaereton mathematicorum», «De subtilitate» и «De varietate rerum». Им оставлена также любопытная автобиография под заглавием «De vita propria». Несмотря на многочисленность сочинений Кардано, в науке сохранились лишь формулы, данные им для решения уравнений третьей степени и носящие имя Кардано. Занимаясь составлением гороскопов Кардано, помимо прочего, предсказал день своей смерти и, как говорит предание, чтобы оправдать своё предсказание, сам уморил себя голодом.