Образовательный Центр "Лучшее Решение"
www.лучшеерешение.рф www.lureshenie.ru www.высшийуровень.рф
www.лучшийпедагог.рф www.publ-online.ru www.t-obr.ru

Мой универсальный шифр

Автор: Чернигов Егор
ученик 8 «А» класса
МБОУ г. Иркутска "СОШ № 14"

Руководитель:
Боннет Светлана Александровна
учитель математики
МБОУ г. Иркутска "СОШ № 14"

Введение.

Тайны, заговоры, попытки перевернуть ход истории и быть в центре этих событий, управлять государствами и народами - мечта многих с древнейших времён. Люди придумывали много способов, чтобы всего достичь и в первую очередь, все понимали, что нужна информация. Не зря мы часто слышим высказывание: «владеешь информацией – владеешь миром». Но эта же самая информация очень нуждается в защите. Всё это привело к развитию криптографии и шифров, к увеличению интереса к вопросу, как защитить нужную тебе информацию, а также, как передать её, чтобы твои недруги не прочитали послание. Во все времена это было более чем актуально.

Сейчас, с развитием компьютерных технологий, с развитием миллиона вариантов передачи информационных потоков, вопрос о безопасности и кибербезопасности становится на одно из первых мест. Современные методы шифрования требуют практически абсолютную защиту данных. Часто от этого зависит судьба не только отдельных личностей, но и целых государств. Именно актуальность, загадочность этой темы и вызвала большой интерес у меня и подвигла начать детально разбираться в этой проблеме. И основываясь на некоторых знаниях, попробовать создать свой универсальный шифр.

В связи со всем вышеперечисленным я определил цель и задачи моей работы.

Цель моей работы – проанализировать роль шифра на протяжении всей истории человечества и создать свой отличительный шифр. В этом мне помогут шрифт Брайля и мой любимый кубик Рубика, с которым я знаком с самого детства.

Исходя из цели, поставлены задачи:

1. Изучить историю развития стенографии и криптографии;
2. Понять, что такое шифры, как они возникали, выяснить их виды, разновидности, классификации и как находили ключ к ним;
3. Выяснить, как на современном этапе используется шифрование информации;
4. Определить роль криптографии в шифровке данных;
5. После анализа различных шифров попробовать создать свой уникальный шифр для передачи информации на основе шрифта Брайля и кубика Рубика;
6. Познакомить всех с шрифтом Брайля и кубиком Рубиком;
7. Опробовать созданный шифр в конкретных условиях;
8. Представить полученные результаты в форме презентации.

Гипотеза: По-моему мнению, шифровка данных – одна из самых востребованных и интересных видов деятельности, как в прошлом, так и в настоящем. Считаю, что каждый, если немного постарается в силах сделать свой универсальный шифр. Требуется лишь немного труда, усердия, знаний!

Я готов это доказать данной работой.

1.Теоретическая часть.

1.1. Актуальность темы.

Тысячи лет короли, королевы и полководцы управляли своими странами и командовали своими армиями, опираясь на надежно и эффективно действующую связь. В то же время все они осознавали последствия того, что произойдет, если их сообщения попадут не в те руки, если вражескому государству будут выданы ценные секреты, а жизненно важная информация окажется у противника. И именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров — способов скрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано[1]. Непрекращающаяся борьба между создателями и взломщиками шифров содействовала появлению целого ряда замечательных научных открытий. Создатели шифров постоянно прилагали усилия для создания все более стойких шифров по защите систем и средств связи, в то время как дешифровальщики непрерывно изобретали все более мощные методы их атаки. В своих усилиях разрушения и сохранения секретности обе стороны привлекали самые разнообразные научные дисциплины и методы: от математики до лингвистики, от теории информации до квантовой теории. Взамен шифровальщики и дешифровальщики обогатили эти предметы, а их профессиональная деятельность ускорила научно-технический прогресс, причем наиболее заметно это проявилось в развитии современных компьютеров.

И сегодня шифры сегодня имеют гораздо большее значение, чем когда бы то ни было раньше. Поскольку информация становится все более и более ценным товаром, а революция в сфере коммуникаций изменяет общество, процесс зашифровывания сообщений, или иначе, шифрование, начинает играть все большую роль в повседневной жизни. Сегодня наши телефонные разговоры передаются по спутниковым каналам, а наши электронные письма проходят через различные компьютеры, и можно с легкостью осуществить перехват передаваемой информации по обеим этим видам связи, что ставит под угрозу нашу частную жизнь. Точно также, поскольку коммерческая деятельность во все большей степени осуществляется через Интернет, следует вводить меры безопасности, чтобы защитить компании и их клиентов.

Шифрование — единственный способ защитить нашу частную жизнь и гарантировать успешное функционирование электронного рынка. Искусство секретной связи, иначе известное как криптография, даст вам замки и ключи информационного века.

Хотя в настоящее время криптография оказывает значительное влияние на действия гражданских лиц, следует отметить, что военная криптография остается важным вопросом. Говорят, что Первая мировая война была войной

[1] С. Сингх. Тайная история шифров и их расшифровки.

химиков, потому что в ней впервые были применены иприт и хлор, а Вторая мировая война — войной физиков, поскольку в ней была взорвана атомная бомба. Подобным же образом утверждают, что третья мировая война станет войной математиков и информатиков, потому что математики будут обладать контролем над очередным величайшим оружием — информацией. Математики отвечали за создание шифров, которые в настоящее время используются для защиты военной информации. Не удивительно, что они же находятся на передовой линии, взламывая эти шифры.

Однако растущая потребность общества в криптографии вступает в противоречие с требованиями правоприменяющих органов и национальной безопасности. Десятилетиями полиция и разведывательные службы прослушивали телефонные переговоры для сбора улик против террористов и организованных преступных синдикатов, но создание в наше время сверхстойких шифров угрожает свести на нет их ценность. Ввиду того, что мы вступили в двадцать первый век, борцы за гражданские права добиваются широкого использования криптографии для защиты права каждого на личную жизнь. Вместе с ними выступают и представители бизнеса, которым требуется стойкая криптография для обеспечения безопасности сделок, осуществляемых в быстро развивающемся мире электронной коммерции. Представители же сил правопорядка оказывают давление на правительства, чтобы ограничить пользование криптографией. Вопрос состоит в том, что для нас важнее: наше право на частную жизнь или эффективно действующая полиция? Или все же существует компромисс? Истина, как всегда где-то посередине. [2]

1.2. Зарождение стенографии и криптографии.

Тайнопись зародилась в далёком прошлом. Некоторые из наиболее ранних упоминаний о тайнописи восходят еще к Геродоту, «отцу истории», как называл его римский философ и политический деятель Цицерон.

В своей «Истории» Геродот повествовал о вооруженных столкновениях между Грецией и Персией в пятом веке до н. э., которые он рассматривал как противоборство между свободой и рабством, между независимыми греческими государствами и тиранической Персией. Согласно Геродоту, именно искусство тайнописи спасло Грецию от порабощения Ксерксом, царем царей, деспотичным правителем Персии.

Секретная переписка, осуществляемая путем сокрытия имеющегося сообщения, носит название стеганография, которое происходит из греческих слов *steganos* — «покрытый» и *graphein* — «писать». В течение двух тысячелений после Геродота во всем мире применялись различные виды стеганографии. Например, древние китайцы писали сообщения на тонкой шелковой ткани, которая затем сворачивалась в крохотный шарик и покрывалась воском, после чего посланец проглатывал этот восковой шарик.

---

[2] Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М, 2005.

То, что стеганография смогла просуществовать столь длительное время, показывает, что она, несомненно, обеспечивает определенную секретность, но ей присущ один принципиальный недостаток. Если курьер будет обыскан и у него обнаружат сообщение, то сразу же станет известно и его содержание. Перехват сообщения мгновенно ставит под угрозу всю безопасность. Бдительная стража может тщательно обыскивать всех, кто пересекает границу, счищая с дощечек весь воск, нагревая чистые листы бумаги, очищая сваренные яйца от скорлупы, брея людям головы и т. п., так что случаи обнаружения сообщения будут неизбежны.

Поэтому, наряду с усовершенствованием стеганографии, происходило развитие криптографии, которая берет начало от греческого слова kryptos, означающего «тайный». Цель криптографии состоит не в том, чтобы скрыть наличие сообщения, а в том, чтобы скрыть его смысл, — процесс, известный как шифрование.

Так процесс стенографии плавно перерос в процесс шифрования.
Криптография сама может быть разделена на два направления, известные как перестановка и замена. [3]

1.3.Виды криптографии: перестановка и замена.

При перестановке буквы сообщения просто переставляются, образуя анаграмму. Для очень короткого сообщения, состоящего, например, из одного слова, такой способ весьма ненадежен, поскольку существует крайне ограниченное число возможных способов перестановки горстки букв.

Однако по мере увеличения количества букв число возможных перестановок стремительно растет, и восстановить исходное сообщение становится невозможным. Но здесь есть отрицательный момент. При перестановке образуется невероятно сложная анаграмма, и если буквы случайно, ни с того ни с сего, перепутаются, то ни получатель, ни перехвативший ее противник не смогут ее расшифровать. Для обеспечения эффективности способ перестановки букв должен быть заранее оговорен отправителем сообщения и его получателем, но он должен храниться в секрете от противника.

Один из способов перестановки был реализован в самом первом из известных шифровальных устройств, предназначенных для военных целей, — спартанской *скитале.* Упоминание о ней восходит к пятому веку до н. э. Скитала представляла собой деревянный цилиндр, вокруг которого наматывалась полоска кожи или пергамента. Отправитель писал сообщение по всей длине скиталы, а затем разматывал полоску, на которой после этого оставался бессмысленный набор букв. Сообщение оказывалось зашифрованным. Вестник брал кожаную полоску и обычно прятал сообщение, используя полоску как пояс, буквами внутрь, то есть кроме зашифровывания применял также и стеганографию. Чтобы получить исходное сообщение,

[3] С. Сингх. Тайная история шифров и их расшифровки.

адресат просто наматывал полоску кожи вокруг скиталы того же диаметра, что и скитала, которой пользовался отправитель.

Альтернативой перестановке является замена.

Способ заключается в том, чтобы расположить попарно буквы алфавита случайным образом, а затем заменять каждую букву в исходном сообщении ее парной. Такой вид тайнописи называется шифром замены, поскольку каждая буква в исходном тексте заменяется другой буквой, так что этот шифр диаметрально противоположен шифру перестановки. При перестановке каждая буква остается сама собой, но меняет свое местоположение, в то время как при замене каждая буква меняется на другую, но остается на своем месте.

Первое документально подтвержденное использование шифра замены в военных целях появилось в «Галльских войнах» Юлия Цезаря. Цезарь описывает, как он послал сообщение Цицерону, находившемуся в осаде и бывшему на грани капитуляции.

В качестве замены Цезарь часто заменял каждую букву в послании буквой, стоящей в алфавите на две, три, четыре и т.д. позиции дальше. Шифр Цезаря основан на шифралфавите, который сдвинут на определенное число позиций относительно алфавита открытого текста.

К каждому отдельному шифру применимы понятия общего метода шифрования, известные как алгоритм и ключ, которые определяют детали конкретного способа шифрования. В этом случае алгоритм заключается в замене каждой буквы в алфавите открытого текста буквой из шифралфавита, причем шифралфавит может представлять собой любую возможную перестановку алфавита открытого текста. Ключ же определяет, какой именно шифралфавит используется для конкретного способа шифрования. В приложении 1 рассмотрен пример со сдвигом на три буквы.

Помимо того, что ключ должен храниться в секрете, стойкая система шифрования должна также обладать широким набором возможных ключей. Например, если для зашифровывания сообщения отправитель применяет шифр сдвига Цезаря, то такое шифрование является сравнительно слабым, так как существует всего 33 возможных ключей. С точки зрения противника, если он перехватит сообщение и подозревает, что применялся алгоритм сдвига Цезаря, то ему следует просто проверить 33 возможных вариантов. Однако если отправитель использует более общий алгоритм замены, благодаря которому шифралфавит будет представлять собой любую возможную перестановку букв алфавита открытого текста, тогда ключ найти становится наисложнейшей задачей.

Прелесть этого вида шифра состоит в том, что он прост в применении, но обеспечивает высокую степень защиты. Отправитель без труда может задать ключ, который просто определяет порядок следования букв в шифралфавите, однако для противника по-прежнему практически невыполнимо проверить все возможные ключи с помощью, так называемого, метода прямого перебора всех возможных вариантов.

1.4. Частотный анализ.

Большое развитие криптография получила в мусульманских странах. Большое развитие многих наук дало большой толчок к этому развитию. И одним из огромных достижений было изобретение частотного анализа. Вот в чем его смысл.

Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, — это взять другой незашифрованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву «первой», букву, которая по частоте появления стоит на втором месте, назовем «вторая», букву, которая по частоте появления стоит на третьем месте, назовем «третья» и так далее, пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдем наиболее часто встречающийся символ и заменим его «первой» буквой незашифрованного текста, второй по частоте появления символ заменим «второй» буквой, третий по частоте появления символ заменим «третьей» буквой и так далее, пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать. Так в русском языке, если мы сделаем такой же анализ мы убедимся, что самой популярной буквой нашего языка будет буква «О», «Ё» - самая редкая буква.

Буква	Частота появления
О	18%
А	16%
Ё	Самая редкая 0,1%

Поэтому из зашифрованных какими-то значками текст самые распространённые с большей долей вероятностью будет буква русского алфавита «О». И чем больше текст, чем доля вероятности возрастает.
Такой способ дешифрования называется частотным. [4]

1.5. Код и кодовые слова

К попыткам усилить шифр замены относится и введение кодовых слов. Термин *код* имеет очень широкое значение в обыденной речи, и он часто употребляется для описания любых способов, используемых для тайной передачи информации. Мы рассматривали шифр замены, посредством которого каждая буква заменяется на другую букву, число или символ.

[4] Введение в криптографию; Под редакцией В. В. Ященко, Издание четвертое, дополнительное.- Москва МЦНМО 2012.

Однако замену можно осуществлять на гораздо более высоком уровне, когда каждое слово представляется другим словом или символом — это и будет код.

Формально код определяется как замена, выполняемая на уровне слов или фраз, в то время как шифр определяется как замена на уровне букв. Поэтому термин зашифровать означает «сделать сообщение секретным с помощью шифра», в то время как закодировать означает «сделать сообщение секретным с помощью кода». Аналогично термин расшифровать/дешифровать применяется для рассекречивания зашифрованного сообщения, а раскодировать/декодировать — для рассекречивания закодированного сообщения. Термины зашифровать и расшифровать/дешифровать более общие и охватывают засекречивание и рассекречивание, выполняемое как с помощью кодов, так и с помощью шифров.

На первый взгляд представляется, что коды обеспечивают более высокую степень стойкости, чем шифры, так как слова гораздо менее уязвимы для частотного анализа, чем буквы. Чтобы дешифровать одноалфавитный шифр, вам потребуется установить точные значения каждой из всего лишь 26 букв, а чтобы взломать код, вам потребуется определить точные значения сотен и даже тысяч кодовых слов. Однако если мы более внимательно рассмотрим коды, мы увидим, что они, по сравнению с шифрами, обладают двумя существенными с практической точки зрения недостатками. Во-первых, после того как отправитель и получатель согласуют 26 букв в шифралфавите (ключ), они смогут зашифровать любое сообщение, но чтобы добиться той же гибкости при применении кода, им придется проделать кропотливую работу по заданию кодового слова для каждого из тысяч возможных слов незашифрованного текста. Кодовая книга будет состоять из сотен страниц, и напоминать словарь. Другими словами, составление кодовой книги — это изрядная задача, держать же ее при себе представляет значительное неудобство.

Во-вторых, последствия того, что противник завладеет кодовой книгой, поистине ужасающи. Все закодированные сообщения сразу же станут известны противнику. Отправители и получатели должны будут заново пройти через кропотливый процесс создания совершенно новой кодовой книги, а затем этот объемистый новый том необходимо будет передать всем в коммуникационной сети, то есть секретно доставить его всем послам во всех странах. Сравните: если противнику удастся завладеть ключом шифра, то сравнительно несложно составить новый шифралфавит из 26 букв, который можно запомнить и легко передать.

1.6. Код Блез де Виженера.

Никогда влияние криптоанализа не проявилось так драматично, как в случае Марии Стюарт, королевы Шотландии. Исход судебного процесса над ней всецело зависел от поединка между ее шифровальщиками и дешифровальщиками королевы Елизаветы. Мария была одной из наиболее заметных фигур шестнадцатого столетия — королева Шотландии, королева Франции, претендент на английский трон — и все же ее судьба зависела от

листочка бумаги, содержавшегося на нем сообщения и от того, будет или нет оно дешифровано.

Увы, в истории Марии Стюарт дешифровальщики оказались сильнее, чем шифровальщики и Мария Стюарт предстала перед судом и была приговорена к казни. 8 февраля 1587 года Мария Стюарт была обезглавлена в замке Фотерингей. Об этой детективной исторической истории подробно описано в книге Сингха Саймона «Книга шифров».[5]

В течение столетий использование простого одноалфавитного шифра замены было достаточным, чтобы обеспечить секретность. Последующее развитие частотного анализа, вначале арабами, а затем в Европе, разрушило его стойкость. Трагическая казнь Марии Стюарт, королевы Шотландии, явилась драматической иллюстрацией слабостей одноалфавитной замены; очевидно, что в поединке между криптографами и криптоаналитиками последние одержали верх. Любой, кто отправлял зашифрованное сообщение, должен был отдавать себе отчет, что опытный дешифровальщик противника может перехватить и раскрыть самые ценные секреты.

Таким образом, криптографы должны были придумать новый, более стойкий шифр, с помощью которого смогли бы перехитрить криптоаналитиков. Но перед тем, как перейти в 16 век в Европу посмотрим, как развивалась криптография до этого момента именно в Европе. При этом мы хорошо знаем, что пока наибольший расцвет криптография достигла в мусульманских странах.

Если между 800 и 1200 годами н. э., когда для арабских ученых наступил период выдающихся интеллектуальных достижений, то Европа прочно увязла в Темных веках. В то время как аль-Кинди описывал изобретение криптоанализа, европейцы все еще постигали основы криптографии. Единственными в Европе институтами, в которых поощрялось изучение тайнописи, были монастыри, где монахи исследовали Библию в поисках скрытого в ней значения; заманчивость этих поисков была такова, что они продолжаются и по сей день.

Средневековые монахи были заинтригованы тем фактом, что в Ветхом Завете имелись явные признаки использования криптографии. В нем, к примеру, встречаются куски текста, зашифрованного с помощью *атбаша*, — традиционной формы шифра замены в иврите. Принцип зашифровывания здесь следующий: берется буква, определяется, какой она является по счету от начала алфавита, после чего заменяется буквой, которая стоит на том же самом месте, но только считая от конца алфавита. Именно это считается началом развития науки криптографии в Европе. Как видим это опять связано с древнейшими религиозными писаниями, учениями, верой (Иудаизмом, Христианством).

К четырнадцатому веку криптографией стали пользоваться повсеместно; алхимики и ученые использовали ее, чтобы хранить свои открытия в секрете. К пятнадцатому веку европейская криптография превратилась в целую отрасль, развивающуюся стремительными темпами. Возрождение искусства и науки в

[5] С. Сингх. Тайная история шифров и их расшифровки.

эпоху Ренессанса «вскормило» криптографию, а бурный рост политических интриг вынуждал обеспечивать секретность переписки. Идеальной средой для криптографии была, в частности, Италия. Она, наряду с тем, что являлась душой Возрождения, состояла из независимых городов-государств, каждый из которых старался перехитрить другие и добиться над ними преимущества. Был расцвет дипломатии; от каждого государства ко дворам других направлялись послы. Каждый посол получал указания от своего правителя о том, какую внешнюю политику он должен проводить. В свою очередь послы отсылали своим правителям все сведения, которые они собирали. Ясно, что имелась веская причина для зашифровывания посланий, идущих в обоих направлениях. В связи с этим в каждом государстве были учреждены шифровальные ведомства, а при каждом после находился секретарь-шифровальщик.

В 16 веке был совершен прорыв в области криптографии. Появился шифр Блез де Виженера, французского дипломата, хотя начало развития такого вида шифрования принадлежит флорентийскому энциклопедисту Леону Баттиста Альберти.

До этого времени все шифры замены требовали отдельного одного шифралфавита для зашифровывания каждого сообщения.

Виженер же предложил использовать два или более шифралфавитов, переходя от одного к другому в процессе зашифровывания и сбивая этим с толку возможных криптоаналитиков.

Стойкость шифра Виженера состоит в том, что для зашифровывания сообщения в нем используется не один, а 33 различных шифралфавитов. Шифрование начинается с построения так называемого квадрата Виженера, показанного в таблице : алфавит открытого текста с последующими 33 шифралфавитами, каждый из которых сдвинут на одну букву относительно предыдущего алфавита. Для наглядности я привел пример в приложении № 2.

1.7. Бэббидж против шифра Виженера

Наиболее любопытной фигурой в криптоанализе девятнадцатого века был Чарльз Бэббидж, эксцентричный английский гений, более всего известный разработкой прототипа современного компьютера. Чарльз Бэббидж родился в 1791 году в семье Бенджамина Бэббиджа, богатого лондонского банкира. Ему удалось взломать шифр Виженера, и это стало величайшим достижением в криптоанализе с тех пор, как арабские ученые в девятом веке взломали одноалфавитный шифр, изобретя частотный анализ. Для этого Бэббиджу не потребовалось проводить никаких вычислений или сложных выкладок. Единственное, что оказалось необходимым, это сообразительность. Взламывание сложного шифра напоминает восхождение по обрывистой отвесной скале. Криптоаналитик стремится отыскать любую трещинку или выступ, которые могли бы дать хоть сколь-нибудь мельчайшую зацепку. В одноалфавитном шифре криптоаналитик будет отталкиваться от частотности появления букв, потому что чаще всего встречающиеся буквы. В многоалфавитном же шифре Виженера буквы появляются более равномерно,

поскольку для перехода от одного шифралфавита к другому применяется ключевое слово. Поэтому здесь появляется приём повторения.

Бэббидж понял, что такой характер повторения дает ему точку опоры, которая необходима, чтобы раскрыть шифр Виженера. Он сумел определить ряд сравнительно простых действий, следуя которым любой криптоаналитик сможет взломать до того момента нераскрываемый шифр. Первый этап криптоанализа Бэббиджа заключался в том, чтобы отыскать последовательности букв, которые появляются в шифртексте более одного раза. Существуют две причины, почему могут возникнуть такие повторения. Первая, и наиболее вероятная, состоит в том, что одна и та же последовательность букв в открытом тексте была зашифрована с помощью одной и той же части ключа. Но есть также определенная, хотя и незначительная, вероятность того, что две разных последовательности букв в открытом тексте, зашифрованных различными частями ключа, случайно образуют идентичные последовательности в шифртексте. Конечно, при разгадки кода Виженера дешифровальщик должен обладать логичностью, сообразительностью, усидчивостью, недюженным терпением, умением анализировать и делать выводы. Но другие люди и не занимаются таким необычным, трудным делом, как расшифровка шифров.[6]

1.8. Шифры: общество и литература.

Но в это же время появляется большой интерес к криптографии во многих слоях общества, и не только военных. Особенно это отражено в литературе того времени. Например, в романе Жюль Верна «Путешествие к центру Земли» дешифрование пергамента, заполненного руническими письменами, явилось первым шагом героического путешествия. Эти письмена представляют собой часть шифра замены, который образует текст на латинском языке, и который, в свою очередь, приобретает смысл только тогда, когда буквы идут в обратном порядке: «Спустись в кратер вулкана Снайфельдс, который тень Скартариса ласкает перед июльскими календами, отважный странник, и ты достигнешь центра Земли». В Британии одним из наиболее выдающихся авторов художественных произведений, посвященных криптографии, был сэр Артур Конан Дойль. И не удивительно, что Шерлок Холмс был экспертом в криптографии и, как он сообщил доктору Ватсону, был «автором небольшого научного труда, в котором проанализировано сто шестьдесят различных шифров». О самом известном случае дешифрования, которое выполнил Холмс, говорится в рассказе «Пляшущие человечки»; в этом рассказе использовался шифр, состоящий из человечков, напоминающих детские рисунки, но при этом каждая поза этих человечков является отдельной буквой.

---

[6] Введение в криптографию; Под редакцией В. В. Ященко, Издание четвертое, дополнительное.- Москва МЦНМО 2012.

Как Шерлок Холмс разобрался в хитросплетениях человечков, можно прочитав это произведение. Да и вообще, многие рассказы о Шерлоке Холмсе сопровождаются раскрытием различных головоломок и шифров.[7]

Ещё одна детективная история, о которой написано немало и посвящена загадке Биля и его сокровищ. С описанием загадки Биля можно ознакомиться в приложении № 3.

Многие и по сей день ищут письма Биля и пытаются разгадать. И меня эта история тоже очень заинтересовала.[8]

1.9. Шифры и дальние расстояния.

В конце девятнадцатого века криптография пребывала в замешательстве. С тех пор, как усилиями Бэббиджа и Касиски шифр Виженера перестал быть надежным, криптографы искали новый шифр, шифр, который смог бы заново обеспечить секретность связи, давая тем самым возможность бизнесменам и военным пользоваться оперативностью телеграфа, не опасаясь, что их сообщения будут перехвачены и дешифрованы. Такие факторы, как появление радио и Первая мировая война, резко обострили потребность в стойком шифровании. Имелась надежда, что будет придуман какой-нибудь новый шифр, который сможет обеспечить секретность в интересах военного командования. Однако в период между 1914 и 1918 годами ничего существенного сделано не было, был лишь только составлен каталог криптографических ошибок и неудач. Шифровальщики изобрели несколько новых шифров, но, один за другим, все они были раскрыты.

Шифр Энигмы

Энигма — это шифровальная машина, использовавшаяся нацистами во времена Второй Мировой. Принцип ее работы таков: есть несколько колес и клавиатура. На экране оператору показывалась буква, которой шифровалась соответствующая буква на клавиатуре. То, какой будет зашифрованная буква, зависело от начальной конфигурации колес. Соль в том, что существовало более ста триллионов возможных комбинаций колес, и со временем набора текста колеса сдвигались сами, так что шифр менялся на протяжении всего сообщения. Все Энигмы были идентичными, так что при одинаковом начальном положении колес на двух разных машинах и текст выходил одинаковый. У немецкого командования были Энигмы и список положений колес на каждый день, так что они могли с легкостью расшифровывать сообщения друг друга, но враги без знания положений послания прочесть не могли. Когда Энигма попала в руки к союзникам, они все равно сперва не могли ничего с ней сделать, потому что не знали положений-ключей. Дело по взлому шифра Энигмы было начато в польской разведке и доведено до конца в британской с помощью ученых и специальных машин (например, Turing Bombe, чья работа заключалась в том, чтобы моделировать одновременно работу сразу нескольких десятков Энигм). Отслеживание коммуникаций

[7] А.К.Дойль. Приключения Шерлока Холмса. Пляшущие человечки.

нацистов дало армии союзников важное преимущество в войне, а машины, использовавшиеся для его взлома, стали прообразом современных компьютеров.[9]

1.10. Криптография в России.

Как отмечает в своей книге исследователь истории шифровального дела Т. А. Соболева, первым из российских государей, осознавшим всю важность криптографии для безопасности страны, стал Петр I (1672−1725). Он поставил шифровальную службу действительно на профессиональную основу. С 1700 г. вся работа по созданию шифров, шифрованию и расшифрованию велась в цифирном отделении Посольского приказа, а позднее, с 1709 г., — в Посольской канцелярии. Типичным шифром того времени был шифр простой замены: каждая буква алфавита заменялась новым знаком, буквой или сочетанием букв. Кроме того, добавлялись «пустышки» —незначащие символы, а также вводились специальные обозначения.

Большее развитие и всплеск использования была зафиксирована в в начале 19 века. Первая половина XIX века вся криптографическая деятельность, а также руководство службой перлюстрации осуществляются в Канцелярии только что созданного (1802г.) Министерства иностранных дел. Непосредственно руководит Канцелярией (с 1810 г.) статс-секретарь Карл Васильевич Нессельроде, позднее ставший министром иностранных дел и государственным канцлером. К числу ярких успехов того времени относится дешифрование военной переписки Наполеона. Этот факт сыграл важную роль в исходе Отечественной войны 1812 г. и поражении наполеоновской армии.

Тайная сыскная полиция и военные ведомства Российской империи и при Александре 3 и При Николае 2 очень часто и с пользой использовали имеющиеся в то время шифры.

Особенное место в развитии крипографии в России можно связать с именем Владимира Ивановича Кривоша. В. И. Кривош, словак по происхождению, стал одним из ведущих российских криптографов. За предложенные им усовершенствования российской криптографической службы он получил орден Святого Владимира 4-й степени из рук П. А. Столыпина.

Появление в начале XX века радиосвязи значительно повысило требования к стойкости армейских шифров, в условиях, когда почти каждое сообщение могло быть перехвачено противником. К началу Первой мировой войны для русской армии был создан сложный шифр двойной перестановки с частой сменой ключей, представлявший проблему для самых опытных криптоаналитиков того времени. В XX отечественная криптографии заняла лидирующие позиции. Все больше российских программистов работает в

[9] А.П. Алферов, А.Ю. Зубов, А.С.Кузьмин, А.В. Черёмушкин Основы криптографии. – Москва «Гелиос АРВ», 2002.

международных криптографических проектах. С 1999 года ассоциация «РусКрипто» проводит ежегодные конференции под тем же названием.[10]

1.11. Шифры наших дней.

На данный момент большинство шифров связаны с компьютерами и программированием. И это не удивительно! Взлет современных технологий всячески способствует этому. В своей работе я лишь немного коснусь этой темы из-за её многогранности, трудности и обилии информации. Хотя мне бы очень хотелось изучить эту тему более детально и попробовать свои силы в создании универсального на сегодняшний день шифра с использованием современных технологий.

Компьютеризация современного общества дошла до той черты, когда буквально вся информация – книги, рабочие документы, фото- и видео-файлы, а также личная информация хранится на жестких дисках компьютеров. В связи с этим остро ставится вопрос о сохранении этих данных от доступа посторонних лиц. Наиболее очевидным выходом является шифрование данных.

Среди криптографических программных средств с платной лицензией здесь можно выделить продукты eToken и ruToken, среди свободно распространяемых программ – PGP, TrueCrypt. Однако данные программы обладают рядом недостатков – они либо платные, либо являются продуктами иностранного производства, где не гарантировано отсутствие закладок. Также порой бесплатные программы не имеют документированного сопровождения на русском языке. Еще одной проблемой бесплатных программ является использование морально устаревших алгоритмов шифрования. Поэтому сейчас многие российские разработчиков программ нацеленных на создание может не универсального, но достаточно надёжного шифра для сохранения информации.[11]

2. Практическая часть.

Несмотря на то, что на данный момент большинство способов зашифровать и дешифровать тот или иной текст связан с программным обеспечением, мне бы хотелось создать свой шифр все же опирающийся на логику, какие-то математические расчеты и правила. После долгих раздумий я понял, что для этого как никогда хорошо подходят кубик Рубика и шрифт Брайля. Впереди несколько слов, объясняющие, что они из себя представляют

---

[10] Соболева Т. А. Тайнопись в истории России (История криптографической службы России XVIII – начала XX в.). М., 1994.

[11] Агрaновский А.В, Р.А.Хади Практическая криптография: алгоритмы и их программирование. – Солон Пресс, 2009.

2.1. Кубик Рубика.

Небольшой экскурс в историю. Кубик Рубика - механическая головоломка, изобретённая в 1974 году и запантетованная в 1975 году венгерским скульптором и преподавателем архитектуры Эрнё Рубиком. Головоломка представляет собой пластмассовый куб 3×3×3 (в первоначальном варианте) с 54 видимыми цветными наклейками. Грани большого куба способны вращаться вокруг 3 внутренних осей куба. Каждая из шести граней состоит из девяти квадратов и окрашена в один из шести цветов, в одном из распространённых вариантов окраски, расположенных парами друг напротив друга: красный — оранжевый, белый — жёлтый, синий — зелёный.

Повороты граней позволяют переупорядочить цветные квадраты множеством различных способов. Задача игрока заключается в том, чтобы «собрать кубик Рубика»: поворачивая грани куба, вернуть его в первоначальное состояние, когда каждая из граней состоит из квадратов одного цвета. В середине 1970-х Эрнё Рубику никак не удавалось втолковать студентам математическую теорию групп, и первый кубик Рубика был построен, как обучающий инструмент, чтобы помочь его студентам понять трехмерные объекты. [12], [13]

2.2. Шрифт Брайля.

Второй мой помощник в создании моего универсально шифра – шифр Брайля. Создан он был, как и все многие нововведения для военных.

В начале 19-го века был изобретен шрифт для военных нужд с целью передачи данных в полной темноте. Изначально его условно называли «ночное письмо». Это было необходимо для того, чтобы в ночное время не привлекать противника отблесками света при получении распоряжений командования. Но его основатель, французский офицер-артиллерист, не остановился на этом и в 1821 году отправился со своими новациями в Королевский институт слепых, где Луи Брайль заинтересовался изобретением. Брайль усовершенствовал азбуку для незрячих, скомпоновав по 6 выпуклостей для каждой отдельной буквы французского алфавита. Буквы в общепризнанной системе представляют собой шесть выпуклостей в два вертикальных ряда. Чтение происходит справа налево на первой странице и наоборот на следующей. Эти выпуклости шрифта Брайля очень хорошо ложатся на кубик Рубик с его шестью сторонами и девятью квадратами каждого цвета. Принцип шифра основан на точечном методе. В приложении № 4 – наглядное расположение точек, которые соответствуют каждой букве уже нашего родного русского языка, а также некоторые символы, которые мы часто используем.[14]

Буквы и символы, которые изображаются точками в шрифте Брайля, послужат нам при расшифровке послания. Выпуклостями или точками

послужат нам белые квадраты на кубике Рубика. А их расположение и расшифровка будет совпадать с расположением по шрифту Брайля. Например, буква «А» будет представлена так, что на стороне кубика один лишь белый квадрат будет расположен в верхнем левом углу. При этом на кубике мы задействуем и будем рассматривать только крайние вертикальные полоски, которые состоят из шести квадратов. (Каждая буква в шрифте Брайля зашифровывается от 1 до 6 точек). Все остальные буквы расшифровываются аналогично.

2.3. Составление шифра Рубика-Брайля-Чернигова.

Алгоритм составления шифра:

1. Перед нами – кубик Рубика. Нам не нужно точное расположение каждого блока, нам необходимо знать только расположение квадратов того цвета, который мы выбрали. В моём случае, это белый цвет. Для зашифровки сообщения необходимо разобрать кубик Рубика. Как именно это будет сделано – не важно, можно начинать зашифровку и с собранного куба, но это (я убедился на собственном опыте) не очень удобно. Поэтому рекомендуется разобрать кубик Рубика перед началом процесса шифровки.

2. Подбираем ключ. У меня он состоит из двух элементов:

1) Начальное расположение кубика и сторона, на которой мы будем читать наш текст, например это может быть зашифровано, #БК#, что обозначает, что собирать буквы мы будем на белой стороне (Б), а вверху будет располагаться красная сторона (К). Окрас сторон мы определяем по квадрату, который находится в центре стороны.

2)Второй элемент ключа я назвал К(от англ. Key – ключ) . К его составлению мы приступим лишь в конце нашей работы, в конце зашифровки фразы.

3. Начинаем процесс шифровки. Нужно делать это очень скрупулёзно и внимательно. Потому, что небольшая ошибка приведёт к сбою в шифровании и придётся начинать всё сначала. Затем нужно зашифровать каждый символ: буквы, цифры, знаки (кроме пробелов), выбранной фразы в обратном порядке, начиная от последней буквы к первой. При этом получатель начнёт расшифровывать текст от первой буквы к последней и сможет легко прочитать текст.

Давайте попробуем зашифровать фразу «**Нас ждёт успех».**

Как мы уже выше говорили, буквы шифруются с помощью 2 алфавитов: алфавита Брайля, который используется не столько для зашифровки сообщения, сколько для того, чтобы спрятать наш зашифрованный текст на кубике Рубика, и мой собственный алфавит формул. Алфавит формул и их расшифровку можно посмотреть в приложении № 5 к данной работе. Эти формулы помогут нам в перестановке блоков кубика Рубика в нужное нам положение. То есть квадраты с белым цветом будут становиться на позиции, совпадающие с точками шрифта Брайля. (Все эти формулы хорошо известны людям, которые умеют собирать кубик Рубика).

4. Далее мы будем шифровать наш исходный текст. Зашифровываем последнюю букву нашей фразы, в данном случае это буква «Х». Она в шрифте

Брайля представлена так, что белый квадрат должен состоять из трёх точек (квадратов), и эти квадраты должны находиться в левом верхнем углу, в средней левой и в средней правой позиции. (Смотреть шрифт Брайля).

После этого смотрим, какая буква идёт следующей (предпоследней). Это буква «Е». Для того, чтобы воссоздать её в моём случае, я могу воспользоваться данным алгоритмом: |БС (П) «2-ой пиф-паф» [3] | . Расшифруем: | - это предыдущая или последующая буквы, БС – это положение кубика из которого мы начинаем составлять букву. Если при этом ничего не написано, то наше положение кубика #БК# не изменяется. В нашем случае, мы начинаем составление буквы «Е» из положения, когда белая сторона смотрит на нас, а синяя располагается сверху. (П) – направление проворота формулы, «2-ой пиф-паф» - название формулы (смотреть в приложении № 2), [3]- цифра три обозначает сколько раз эту формулу мы должны произвести. После того, как получатель провернёт все эти манипуляции, на стороне БК у него появятся белые блоки, которые будут стоять в верхнем левом углу и среднем правом. Смотрим на шрифт Брайля. Таким образом у нас зашифровывается буква «Е».

Затем я смотрю на следующую букву «П» и шифрую её таким же подбором формул. Также шифруем и остальные символы. В итоге у меня получилось следующее: | БС (П) «2-ой пиф-паф» [3] | F; B2; L2 | ОБ (П) «Пропеллер» [1] ; F; ОБ (П) «ƛ» | ЖО (П) «краб» [2]; F | (П) «∨» [1]; СБ (П) «ƛ» | F | ОБ (П) «ƛ» | D; F`; L` | (П) « − » [1]; D; F` | БО (П) «2-ой пиф-паф» [3]; СБ «2-ые глаза»; F | L`; D2; F` СЖ (П) «пиф паф» [1] |.

5. После этого необходимо записать все формулы полученного текста зеркально, то есть написать их противоположности, например: вместо F – F`, вместо «∨» - « − ». А вот, например, «ƛ» останется неизменной, так как она сама себе является противоположностью. Затем необходимо записать всё в обратном порядке. В итоге получаем: | СЖ (П) «Пиф- паф» [5]; F; D2 ; L | F`; СБ «2-ые глаза»; БО (П) «2-ой пиф-паф» [3] | F; D`; (П) «∨» [1] | L; F; D` | ОБ (П) «ƛ» | F` | СБ (П) «ƛ»; (П) «−» [1] | F`; ЖО (Л) «краб» [2] | ОБ (П) «ƛ» ; F`; ОБ (П) «[Ь» [1] | L2; B2; F | БС (П) «2-ой пиф-паф» [3] |.

6. Осталось только подставить ключ. И вот, наконец, мы пришли ко второму элементу ключа нашего шифра, я его назвал К. Мы смотрим на развернутый вид нашего кубика после того, как мы провели все манипуляции и зашифровали все буквы. В нашем случае нам лишь необходимо обращать внимание на расположение белых блоков и на цвета средних квадратов.

Проставляем цифры «0» и «1», где 0- это квадраты не с белым цветом, а 1- это квадраты с белым цветом. Наше расположение можно посмотреть в приложении 3 к данной работе. Далее выписываем порядок нулей и единиц, начиная с верхнего левого угла, слева направо и сверху вниз. Вот, что у нас получилось: 10000000010000000000000001010000001110101. При этом цифры «0», которые встречаются до первого появления «1» не пишутся. Затем мы переводим данный набор цифр в десятичную систему счисления. Это можно легко сделать на калькуляторе в любом компьютере.

7. В итоге получится вот такое вот сообщение: К: 550829576309; #БК# | СЖ (П) «Пиф-паф» [5]; F; D2 ; L | F`; СБ «2-ые глаза»; БО (П) «2-ой пиф-паф»

[3] | F; D`; (П) «∨» [1] | L; F; D` | ОБ (П) «ƛ» | F` | СБ (П) «ƛ»; (П) «–» [1] | F`; ЖО (Л) «краб» [2] | ОБ (П) «ƛ» ; F`; ОБ (П) «[Ь» [1] | L2; B2; F | БС (П) «2-ой пиф-паф» [3] |. Основываясь на нём наш получатель после расшифровки получит фразу «Нас ждёт успех».

Для большей надёжности можно не записывать число K, а заранее обговорить его. Или сделать постоянную константу для всех сообщений. Но тогда придётся добавлять ещё один алгоритм для подстановки первой буквы.

Заключение:

В данной работе я поставил перед собой цель узнать как можно больше об истории зарождения и развития криптографии и, конечно же попытаться создать свой универсальный шифр, опираясь на тех помощники, которые я знаю. Этими помощниками в моей работе выступили: кубик Рубика и шрифт Брайля. Благодаря изучению и разработки своего шифра, я пришел к следующим выводам.

1. Криптография – одна из самых интересных, загадочных и захватывающих наук современности.

2. Эта наука очень актуальна в современном мире, потому что сохранность информации даёт большой потенциал для собственного развития. А дешифровка посланий соперников даёт большое преимущество. После написания своей работы, я ещё раз убедился, что те, кто владеет информацией и умеет её скрывать, тот владеет миром.

3. Работа над созданием своего универсального шифра – это очень трудная, монотонная, скрупулёзная, но необычайно интересная и захватывающая работа.

4. Думаю, что многие, кто заинтересуется темой шифрования способен создать свой универсальный шифр, основываясь на своих собственных знаниях и умениях.

5. Развитие криптографии идёт очень стремительно, это связано с развитием современных технологий. И умение скрывать, а также расшифровывать тексты является одной из самых востребованных профессий современности.

6. В результате работы над этой темой у меня получилось создать свой универсальный шифр, который, я надеюсь, может пригодиться для передачи какой-нибудь информации.

Используемая литература:

Агрaновский А.В, Хади Р.А. Практическая криптография: алгоритмы и их программирование. – Солон Пресс, 2009

Азбука *Брайля* — азбука для незрячих или плохо видящих людей
Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. – Москва «Гелиос АРВ», 2002

А.К. Дойль. Приключения Шерлока Холмса. Пляшущие человечки. Издательство: АСТ, 2016 г.

Бернет С., Пейн С. Криптография. Официальное руководство RSA Security.- Москва изд. «Бином», 2002

Введение в криптографию; Под редакцией *В. В. Ященко*, Издание четвертое, дополнительное. - Москва МЦНМО 2012.

Иванов М.А. Криптография. Криптографические методы защиты информации в компьютерных системах и сетях. – М, 2003.

Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М, 2005.

Сингх С. Тайная история шифров и их расшифровки. Издательство: Аванта+, 2009 г.

Соболева Т. А. Тайнопись в истории России (История криптографической службы России XVIII – начала XX в.). М., 1994.

Приложение 1: шифровка с помощью способа замены

Например: СО СДВИГОМ НА ТРИ БУКВЫ
Алфавит открытого текста:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Шифр алфавит:
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
Исходный текст: ЗАВТРА
Зашифрованный текст: КГЕХУГ

Приложение 2: Квадрат Де Виженера

Первая строчка – открытый алфавит.

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

Здесь ряд 1 представляет собой алфавит шифра Цезаря со сдвигом на 1 позицию, то есть этот шифралфавит может использоваться в качестве алфавита шифра Цезаря, в котором каждая буква открытого текста заменяется буквой, расположенной в алфавите на одну позицию дальше. Точно так же ряд 2 представляет собой алфавит шифра Цезаря со сдвигом на 2 позиции и так далее.

Получателю сообщения, чтобы расшифровать слово, следует знать, какая из строк квадрата Виженера использовалась для зашифровывания каждой из букв. Это обеспечивается с помощью ключевого слова. Чтобы показать, как применяется ключевое слово с квадратом Виженера для зашифровывания короткого сообщения, зашифруем следующую фразу: «деньги передать мне» с помощью ключевого слова «рубль»

Ключевое слово	р	у	б	л	ь	р	у	б	л	ь	р	у	б	л	ь	р	у
Исходный текст	д	е	н	ь	г	и	п	е	р	е	д	а	т	ь	м	н	е

сообщения																	
Зашифров. Текст сообщения	ф	ш	о	з	я	щ	г	ё	ь	б	ф	у	у	з	и	ю	ш

Прежде всего ключевое слово буква за буквой записывается над сообщением, и его повторяют до тех пор, пока каждой букве в сообщении не будет сопоставлена буква ключевого слова. Далее приступим к созданию шифртекста, что делается следующим образом. Чтобы зашифровать первую букву «Д», определим вначале букву ключа над ней, «Р», которая, в свою очередь задает строку в квадрате Виженера. Именно строка, начинающаяся с буквы Р, — 17-ая строка, — и является шифралфавитом, который будет использован для нахождения буквы, которой будет заменена буква **Д** открытого текста. Посмотрим, где столбец с буквой **Д** в первой строке пересекается со строкой, начинающейся с буквы **Р**; это будет буква **Ф**. И так далее. Следовательно, буква **Д** в открытом тексте будет буквой **Ф** в шифртексте. Поэтому зашифрованный текст у нас будет выглядеть следующим образом: «ФШОЗЯЩГЁЬБФУУЗИЮШ». Неоспоримым достоинством шифра Виженера является то, что он неуязвим для частотного анализа. К примеру, криптоаналитик, применяющий частотный анализ к фрагменту шифртекста, обычно начинает с того, что определяет, какая буква чаще всего встречается в шифртексте — в нашем случае это буквы Ф и У, а затем делает предположение, что они являются и наиболее часто встречающимися буквами в русском языке, **О, А, Е.** Но в нашем случае это буквы Ф,У,Б. Несомненно, что для криптоаналитика это создает сложности. То, что буква, которая несколько раз появляется в шифртексте, может представлять собой различные буквы открытого текста, создает для криптоаналитика огромные затруднения. Затем этот шифр видоизменялся. Многоалфавитный подход сохранялся, но вместо букв в качестве замены стали использовать цифры, буквосочетания, и даже словосочетания. Но это очень усложняло не только работу дешифровальщиков, но и работу разработки ключа и методов его передачи.

Приложение 3: История Биля.

Вот загадка для тех, кто хочет попытать счастье. Вот его история. Однажды он появился в одной гостинице, как постоялец и несколько раз таинственно исчезал, доверив хозяину свои вещи – небольшую коробочку с тайными записями. Он дал наказ хозяину, чтобы тот открыл эту коробочку, только после 10 лет с определённого момента, если он сам или посланник от него не появятся. Хозяин так и сделал, и обнаружил письмо, где Биль пишет об огромных сокровищах – золоте, найденных, когда он и его товарищи ходили на охоту за бизонами и спрятанными в каком-то месте. Он разделил сокровища на три части и описание места, где оно лежит, зашифровал. Расшифровали и нашли лишь одну часть сокровищ. Несмотря на все усилия членов Ассоциации, охотников за сокровищами и профессиональных криптоаналитиков, первый и третий шифры Биля так и остались неразгаданными в течение всего этого времени; и золото, и серебро, и драгоценные камни еще только предстоит отыскать. Множество попыток по дешифрованию вращалось вокруг Декларации Независимости, которая явилась ключом для второго шифра Биля.

Но почему же не могут расшифровать 2 и 3 части. Возможно Биль мог придумать специальный, предназначенный для данного случая ключевой текст для первого и третьего шифров. В самом деле, если ключевой текст был написан самим Билем, то этим можно было бы объяснить, почему поиски по опубликованным изданиям не дали результата. Мы можем предположить, что Биль, например, написал рассказ об охоте на бизонов длиной 2000 слов, который существовал всего в одном экземпляре. И только тот, у кого был этот рассказ, — уникальный ключевой текст, — смог бы дешифровать первый и третий шифры Биля. Биль упоминал, что он оставил ключ в «руках друга» в Сент-Луисе, но если друг потерял или уничтожил ключ, то вполне возможно, что криптоаналитики никогда не смогут разгадать шифры Биля.

Создание для сообщения ключевого текста одноразового использования является несравненно более надежным, чем применение ключа на основе опубликованной книги, но практическую ценность это имеет только в том случае, если у отправителя есть время для подготовки ключевого текста и у него есть возможность передать его получателю, а эти требования невыполнимы для обычной повседневной переписки. В случае же Биля, он мог на досуге составить, не спеша, свой ключевой текст, в любой момент, когда бы ему ни пришлось проезжать через Сент-Луис, передать его там своему другу, а затем, когда потребуются сокровища, попросить друга выслать ключевой текст по почте или забрать его самому.

Возможно, Агентство национальной безопасности уже дешифровало эти письма Биля и не опубликовало отчет. Наконец, мы не можем исключить возможность того, что шифры Биля являются тщательно разработанной мистификацией и что в действительности Биля никогда не существовало. Скептики полагали, что неизвестный автор, вдохновленный рассказом Эдгара По «Золотой жук», придумал всю эту историю и опубликовал брошюру в качестве способа нажиться на алчности других людей.

Приложение 4: Наглядное расположение точек шрифта Брайля.

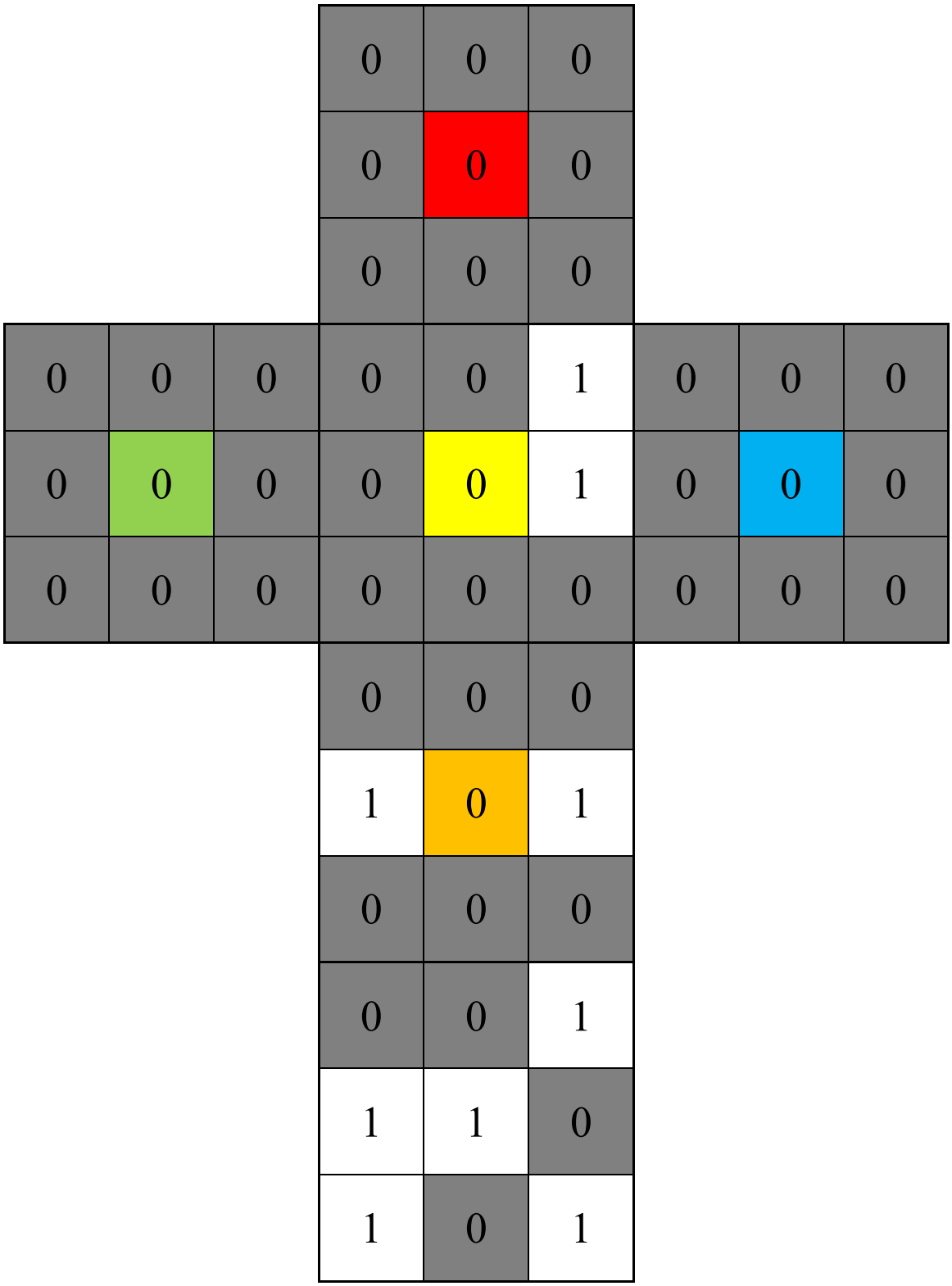
Приложение 5: Алфавит формул.

Название формулы	Расшифровка формулы
Подстановка ребра	U (R U' R') U' (F' U F)
3-х ходовка	R U R'
Глаза	R2' D R' U2 R D' R' U2 R'
Уши	Rw U R' U' Rw' F R F'
Рыбка	R U R' U R U2' R'
Вертолёт	R U2' R2' U' R2 U' R2' U2' R
2-ые глаза	F R U R' U' R U R' U' R U R' U' F'
Воздушный змей	Rw U R' U' M U R U' R'
H	R U R' U' M' U R U' Rw'
Снежинка	S R' U' R U R U R U' R' S'
T	R U R' U' R' F R F'
_	F R U R' U' F'
\/	Инверсия «_»
Пропеллер	R B' R' U' R U B U' R'
[Ь	Инверсия «Пропеллер»
[C	R U R2' U' R' F R U R U' F'
| C	R' U' R' F R F' U R
U-per/треугольник рёбер	R U` R U R U R U` R` U`R2
Z-per/саночки	M' U' M2' U' M2' U' M' U2' M2' U
H-per/крест рёбер	M2' U' M2' U2' M2' U' M2'
A-per/Треугольник углов	x R' U R' D2 R U' R' D2 R2
E-per/терминатор	x' R U' R' D R U R' D' R U R' D R U' R' D'
J-per/ ƛ	R U R' F' R U R' U' R' F R2 U' R' U'
R-per/7	R' U2 R U2' R' F R U R' U' R' F' R2 U'
F-per/||	R' U R U' R2' F' U' F U R U' Lw R U' R' U
T-per	R U R' U' R' F R2 U' R' U' R U R' F'
G-per/8	R2' Uw' R U' R U R' Uw R2 B U' B'
V-per/летающая тарелка	L' U R U' L U L' U R' U' L U2 R U2 R'
N-per/X	z R U R' D R2 U' R U D' R' D R2 U' R D'
Y-per/копьё	F R U' R' U' R U R' F' R U R' U' R' F R F'
Пиф-Паф	RUR`U`
Рыбный Пиф-Паф	RUR^1U
Мясной Пиф-Паф	$RU^1R^1U^1$
Кувалда	R^1FRF^1
Морской Пиф-Паф	RUR^1F^1
хвостик рыбки	$R\ U2\ R^1$

Анти пиф-паф	URU^1R^1
Краб	RU^1R^1U
Акула пиф-паф	$RU2R^1U^1$
Весёлая Варвара	$R\ U2\ R^1\ U2$
Поющая варвара	RU2RU2
2T	M2 U2 M2 U2

Язык вращений кубика:
F - front - фронтальная сторона
B - back - задняя сторона
L - left - левая сторона
R - right - правая сторона
U - up - верхняя сторона
D - down - нижняя сторона
Если после буквы ничего не стоит, то, значит, крутим эту сторону по часовой, как если бы мы смотрели на грань в лицо.
Если после буквы стоит штрих ', значит, крутим против часовой, как если бы мы смотрели на грань в лицо.
Если после буквы стоит двойка 2, значит, крутим эту сторону на 180 градусов.
Редкие виды вращений:
Буква+w:
Fw - фронтальная вместе со средним слоем
Bw - задняя вместе со средним слоем
Lw - левая вместе со средним слоем
Rw - правая вместе со средним слоем
Uw - верхняя вместе со средним слоем
Dw - нижняя вместе со средним слоем
Fw' - фронтальная вместе со средним слоем против часовой стрелки
Bw' - задняя вместе со средним слоем против часовой стрелки
Lw' - левая вместе со средним слоем против часовой стрелки
Rw' - правая вместе со средним слоем против часовой стрелки
Uw' - верхняя вместе со средним слоем против часовой стрелки
Dw' - нижняя вместе со средним слоем против часовой стрелки
Fw2 - фронтальная вместе со средним слоем на 180 градусов
Bw2 - задняя вместе со средним слоем на 180 градусов
Lw2 - левая вместе со средним слоем на 180 градусов
Rw2 - правая вместе со средним слоем на 180 градусов
Uw2 - верхняя вместе со средним слоем на 180 градусов
Dw2 - нижняя вместе со средним слоем на 180 градусов

Приложение 6: Запись цифр «0» и «1» на развёрнутом плане кубика Рубика после применения формул зашифровки.



Приложение 7: Базовый словарь шифровальщика.

1. Шифр (от фр. *chiffre* «цифра» от араб. صِفْر, *sifr* «ноль») — система обратимых преобразований, зависящая от некоторого секретного параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.
2. Шифрова́ние — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.
3. Криптогра́фия (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.
4. Стеганография - секретная переписка, осуществляемая путем сокрытия имеющегося сообщения.
5. Дешифровальшик -взломщик шифров.
6. Шифртекст — сообщение после зашифровывания.
7. Исходный текст – тот текст, который нужно зашифровать.
8. Зашифрованный текст – текст, который подвергся зашифровки.
9. Частотный анализ, частотный криптоанализ — один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.
10. Криптоанализ - наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.
11. Код — взаимно однозначное отображение конечного упорядоченного множества символов, принадлежащих некоторому конечному алфавиту, на иное, не обязательно упорядоченное, как правило, более обширное множество символов для кодирования передачи, хранения или преобразования информации.
12. Номенклатор — это система шифрования, основанная на шифралфавите, который применяется для зашифровывания большей части сообщения, плюс небольшой набор кодовых слов.
13. Информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.
14. Безопасность данных - такое состояние хранимых, обрабатываемых и принимаемых данных, при которых невозможно их случайное или преднамеренное получение, изменение или уничтожение.

15. Метод (способ) защиты данных - совокупность приемов и операций, реализующих функции защиты данных. Примерами их могут служить, например, методы шифрования.

16. Механизм защиты - совокупность средств защиты, функционирующих совместно для выполнения определенной задачи по защите данных (криптографические протоколы, механизмы защиты операционных систем и т.д.).