Бюджетное общеобразовательное учреждение города Омска «Лицей № 149»

**Проект**

Криптография как метод кодирования и декодирования информации

Выполнила:

Исакова Софья Геннадьевна,

ученица 9 «4» класса

БОУ г. Омска «Лицей №149»

Руководитель:

Газина Элеонора Шамильевна

учитель математики

БОУ г. Омска «Лицей №149»

Омск, 2020

**Содержание**

Введение ………………………………………………………………………. 3

I. Основная часть

* 1. Предисловие …………………………………………………………… 4

1.2 Базовая терминология: Основные алгоритмы шифрования ………. 4-5

1.3 Виды алгоритмов ……………………………………………………… 6

1.4 Роль криптографии в современном мире ……………………………. 7

1.5 История возникновения криптографии ……………………………… 8

1.5.1 Первые древнейшие шифры ……………………………………..... 9-12

1.5.2 Развитие в Средние Века и Эпоху Возрождения ……………...... 12-13

1.5.3 Новое и новейшее время …………………………………………. 13-15

II. Практическая часть

2.1 Создание сборника ……………………………………………………. 16

2.1.1 Сбор информации ………………………………………………… 16-17

2.1.2 Внедрение изображений ………………………………………….....17

2.1.3 Подбор примеров ………………………………………………….... 17

2.1.4 Написание введения ………………………………………………... 18

2.1.5 Оформление и представление сборника на бумаге ………………. 18

III. Заключение и выводы ……………………………………………………. 19

IV. Список источников и литературы ………………………………………. 20

V. Приложение …………………………………………………………….. 21-32

**Введение**

**Актуальность**: Криптография – наука о методах обеспечения конфиденциальности и аутентичности информации. Криптография включает в себя методы шифрования информации, ассиметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, а также квантовую криптографию.

Этот проект был создан для того, чтобы расширить свои познания в области кодировки и различных шифров. Также, на данный момент, знания о шифрах могут помочь людям, работающим или же заинтересованным в сфере технологий и IT.

**Цель**: составление сборника с известными методами шифрования.

**Задачи**:

1. Найти и изучить информацию о криптографии.
2. Найти информацию о наиболее популярных методах кодирования информации.
3. Оформить презентацию.
4. Систематизировать полученные знания
5. Собрать известные шифры в сборник.

**Методы исследования**:

1. Анализ известных методов шифрования.
2. Сравнение этих методов.

**Проблемный вопрос:** возможно ли скрыть определенную информацию в настоящее время?

**Продукт проекта**: сборник шифров.

**I. Основная часть**

**Предисловие**

В древности криптографию использовали, чтобы сохранить секретность сообщения. Эта задача появилась после того, как человек изобрел письменность. Саму письменность тогда можно было уже считать криптографической системой. Настоящая криптография должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки опасными организациями. Эта наука в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

**Базовая терминология: Основные алгоритмы шифрования**

В криптографической терминологии исходное послание именуют *открытым текстом*. *Шифрование* — это процесс изменения данных таким образом, чтобы они стали неузнаваемыми и бесполезными для несанкционированного лица. А *дешифрование* — процесс превращения данных в их первоначальный вид. Наиболее безопасные виды шифрования используют математические алгоритмы и переменную — *«ключ».* Выбранный ключ (зачастую любая случайная последовательность) вводится при шифровании и является неотъемлемой частью изменения данных. Тот же самый ключ необходим для дешифровки сообщения.

Это основа защиты, если ключ известен только уполномоченному лицу, то данные не смогут раскрыть другие стороны. Только те, кому известен ключ, могут расшифровать сообщение. Такой способ называется *симметричным шифрованием*, и он наиболее популярен. Симметричные алгоритмы подразделяют на *потоковые* *шифры* и *блочные* *шифры*. Потоковые позволяют шифровать информацию побитово, а блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

Шифрование с помощью открытого ключа или *асимметричное шифрование* также возникло в середине 1970-х. Асимметричные шифры используют пару ключей — открытый, им делятся с другими людьми, и соответствующий ему закрытый, пользователь должен хранить его в секрете от других. Например, получатель может сгенерировать пару ключей и поделиться открытым ключом со всеми, кто хочет отослать ему секретное сообщение. Отправитель может зашифровать сообщение для получателя с помощью открытого ключа, а получатель расшифровать его с помощью закрытого.

Ассиметричные шифры допускают, чтобы открытый ключ находился во всеобщем доступе. Это позволяет любому зашифровать сообщение. Однако расшифровать его сможет только нужный человек - тот, кто владеет ключом дешифровки. Ключ для *шифрования* называют *открытым ключом*, а ключ для *дешифрования* - *закрытым ключом* или секретным ключом.

В общем и целом, симметричные алгоритмы работают быстрее, чем ассиметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения.

Многие качественные криптографические алгоритмы доступны широко - в книжном магазине, библиотеке, патентном бюро или в Интернете.

**Виды алгоритмов**

***DES*** выдержал испытание временем, потому что качество шифрования доказывалось на протяжении многих лет опубликованных исследований. После четверти века исследований учёным удалось найти несколько спекулятивных атак, которые в конечном итоге не были столь эффективными, как метод полного перебора. Единственная реальная слабость DES-шифра — его критически маленькая длина ключа в 56 бит. Более того, так как DES был специально разработан для аппаратного обеспечения, то не было предусмотрено, чтобы он эффективно работал в ПО.

***Triple DES (3DES)***  модификация DES, позволяющая увеличить длину ключа до 112 или 168 бит. Получившийся шифр намного медленнее других шифров, использующих такую же длину ключа, но вышел из употребления, когда мощные компьютерные атаки взломали алгоритм.

***AES  (Advanced Encryption Standard или Rijndael)*** поддерживает три длины ключа 128, 192 и 256 бит и использует 128-битный размер блоков. В настоящее время он считается достаточно стойким и используется по всему миру. Архитектура AES основана на принципе, известном как *замена и перестановка*, и быстро работает как в программном, так и на аппаратном уровнях. В отличие от своего предшественника — DES, AES не использует сеть Фейстеля (один из методов построения блочных шифров).

**Роль криптографии в современном мире**

Основные причины, по которым криптография так востребована:

**Конфиденциальность**  —  когда нужно передать данные так, чтобы человек, перехвативший зашифрованное сообщение, не смог узнать его содержание. То же самое относится и к хранимым данным, которые должны быть защищены на случай несанкционированного доступа к ним.

**Аутентификация**  —  это свойство эквивалентно подписи. Получатель сообщения хочет быть уверен, что оно пришло от определённой стороны, а не от кого-либо ещё (даже если позже эта сторона захочет это опровергнуть).

**Целостность**  —  получатель сообщения хочет доказательства того, что оно не было изменено третьей стороной.

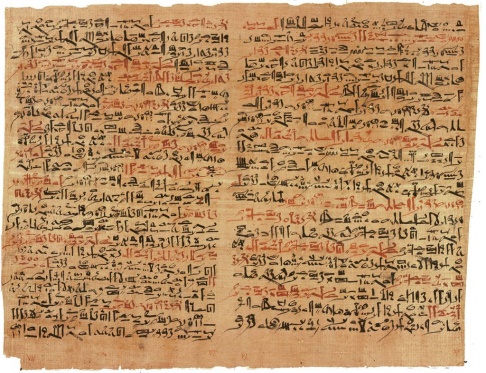
**Отказ от ответственности** — предотвратить отказ автора за создание или отправку сообщения.

Современные алгоритмы шифровки/дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

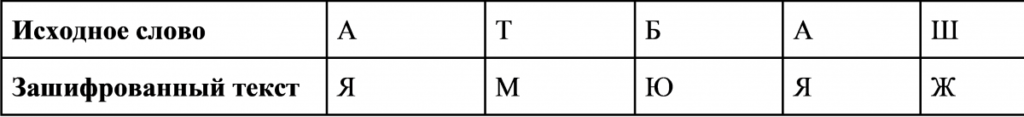
**История возникновения криптографии**

За наукообразным словом «криптография» (с древнегреческого буквально − «тайнопись») скрывается древнее желание человека спрятать важную информацию от посторонних глаз. Можно сказать, что сама письменность в самом начале уже была криптографической системой, так как принадлежала узкому кругу людей, и с помощью нее они могли обмениваться знаниями, недоступными неграмотным. С распространением письма возникла потребность в более сложных системах шифрования. Свои послания пытались шифровать в самых разных древних цивилизациях: Индии, Египте, Месопотамии. Чтобы запутать читателя, использовали методы кодирования и стенографии, которые лишь косвенно относятся к криптографии. Шифрование обычно сводилось к перестановке и замене символов. В более поздний период античности криптография широко использовалась для защиты важной военной информации. греческом городе-государстве Спарта сообщения были зашифрованы записью на пергаменте, обернутом на цилиндр определенного размера, что делало сообщение неразборчивым, пока получатель не оборачивал его вокруг аналогичного цилиндра. Также известно, что шпионы в Древней Индии использовали закодированные сообщения еще во 2 веке до нашей эры. Вероятнее всего, что самая совершенная криптография в Древнем Мире была достигнута римлянами. Ярким примером может послужить шифр Цезаря.

**Первые древнейшие шифры**

Самым древним свидетельством применения шифра (около 4000 до н.э.) ученые считают древнеегипетский папирус с перечислением монументов. Безымянный автор видоизменил известные иероглифы, но, скорее всего, не для сокрытия информации, а для более сильного воздействия на читателя.

Еще один известный шифр – *древнесемитский атбаш*, приблизительно 600 г. до н.э. Здесь информацию запутывали самым простым способом − с помощью подмены букв алфавита. Криптограммы на атбаше встречаются в Библии. Шифр можно разгадать с помощью формулы n−i+1, где n — число букв в алфавите, i — номер конкретной буквы в азбуке.



*Сциталла*, около 400 года до нашей эры. Сциталла — не шифр, а, по сути — устройство, наиболее старый криптографический механизм о котором мы знаем. Это длинный стержень, на который наматывали ленту из пергамента по спирали. Шифруемый текст писали в строки по длине стержня, разматывали и передавали адресату. После разматывания текст становился нечитаемым. Чтобы расшифровать послание, адресату нужен был стержень точно такого же диаметра.



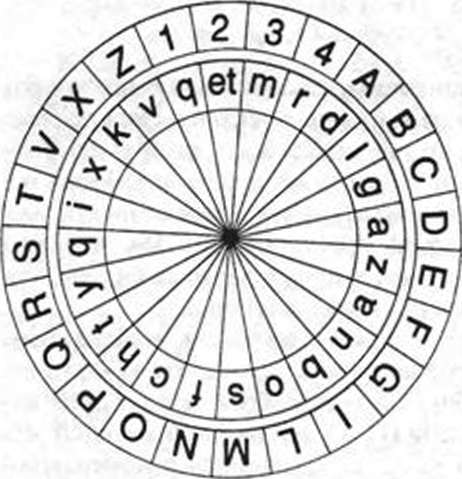
*Шифр Цезаря*, около 100 лет до нашей эры. Гай Юлий Цезарь изобрел и использовал шрифт на основе одного алфавита, этот шрифт назвали его именем. Принцип шифра прост: каждая буква сдвигалась по алфавиту вправо на одно и то же число позиций. Адресату нужно было только знать, насколько — это и был ключ шифрования. Сам диктатор использовал сдвиг на три символа.



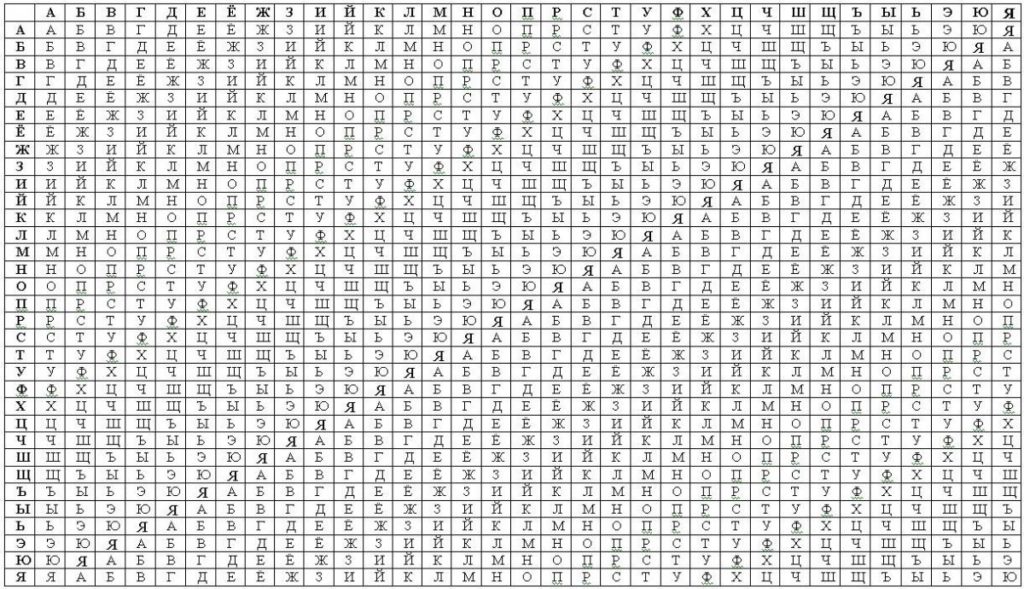
*Литорея*, 1300 год. Удивительно, но криптография существовала и в Древней Руси – факт малоизвестный, но крайне интересный. В древнерусской литературе использовалось тайнописание, называемое Литорея. Она могла быть простой и мудрой. Простая напоминала тарабарскую грамоту, мудрая — шифр простой замены некоторых букв точками, палками, кругами, которые означали разряд числа. Согласные буквы располагали в два ряда, гласные оставались на своих местах



*Диск Альберти*, 1466 год. Шифровальный диск итальянского ученого Леона Альберти состоял из двух частей: внешней, которая двигаться не могла, и внутренней, которая двигалась. Диски делились на 24 клетки, в них были разные символы в разной последовательности. Для шифрования, нужно было вращать внутренний диск через несколько слов. С каждым поворотом образовывалась новая комбинация. В своей книге «Основы современной криптографии» историки С. Баричев, В. Гончаров и Р. Серов говорят о том, что Альберти первым выдвинул идею *двойного шифрования*.



*Шифр Виженера*, 1586 год. Французского дипломата и алхимика Блеза де Виженера историки называют самым известным криптографом XVI века. Виженер изобрел абсолютно стойкий шифр. Его можно представить как последовательность нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания нужна таблица алфавитов. В таблице — строки по 33 буквы, причем каждая следующая строка сдвигается на несколько позиций. Получается, что в такой таблице Виженера 33 различных шифра Цезаря.



Пример шифрования с помощью таблицы Виженера. К исходному слову «Виженер» выбран ключ «Цезарь». Ключ короче исходного слова, поэтому его нужно повторять, пока количество букв не сравняется — «ЦезарьЦезарь…» — в примере достаточно добавить «Ц». Слово шифруется по принципу: буква ключа — строка в таблице, буква исходного слова — столбец. Шифробуква находится на их пересечении.

*Великий шифр Россиньолей*. Французский криптограф Антуан Россиньоль и его сын Бонавентур изобрели шифр, который использовал 587 различных чисел, большая часть из которых обозначала слоги. Это был очень надежный шифр, который не могли взломать столетиями. Некоторые числа в шифре — ловушки, которые ничего не заменяют. Ловушки понадобились, чтобы бороться с частотным анализом.

**Развитие в Средние Века и Эпоху Возрождения**

В средние века криптография становилась все более продвинутой, но шифры замещения все еще оставались стандартом. Аль-Кинди, известный арабский математик, разработал метод, известный как *частотный анализ*, примерно в 800 г. н.э., который сделал шифры замещения уязвимыми для дешифрования. Впервые люди, пытающиеся расшифровать зашифрованные сообщения, получили доступ к систематическому методу, позволяющему криптографии продвигаться еще дальше и оставаться полезной.

В следующую эпоху - эпоху Возрождения - люди сосредоточились на изобретении шифров, а не шифровальных инструментов. *Криптоанализ* - наука, с помощью которой взламываются коды и шифры, начала догонять все еще относительно примитивную науку криптографии.

В 1466 году итальянец Леоне Альберти написал одну из первых научных работ по криптографии − «Трактат о шифрах», а также изобрел *шифровальный диск*. Годом ранее он разработал *полиалфавитный шифр*, который считается решением против метода *частотного анализа* Аль-Кинди. В полиалфавитном шифре сообщение кодируется с использованием двух разных алфавитов. Первый - это алфавит, в котором написано исходное сообщение, а второй - это совершенно другой алфавит, в котором сообщение появляется после кодирования. В сочетании с традиционными заменяющими шифрами, полиалфавитные шифры значительно повышают безопасность кодированной информации. Если читатель не знал алфавит, в котором изначально было написано сообщение, метод частотного анализа был бесполезен.

**Новое и новейшее время**

Большое влияние на шифровальное дело оказало изобретение телеграфа. Прежние шифры вмиг перестали работать, при этом потребность в качественном шифровании только возрастала в связи с чередой крупных военных конфликтов. В XIX-XX веках основные импульсы для развития криптографии давала именно военная сфера.

К началу Первой мировой войны криптографию уже считали полноценным боевым инструментом в США, России, Англии, Германии и не только. Страны перехватывали засекреченные сообщения друг друга, а криптоаналитики рушили планы сохранить политические шаги в секрете. Так, расшифровка перехваченной телеграммы немецкого посла Артура Циммермана подтолкнула США вступить в войну на стороне Антанты.

Ко Второй мировой войне крупные державы использовали электромеханические шифраторы. Шифры устройств в то время считали невскрываемыми. Сами устройства были роторными, как шифровальная машина «Энигма», и на цевочных дисках, как M-209. С помощью «Энигмы» сообщения шифровали войска Германии и ее союзники, при помощи M-209 — армия США. В СССР производили оба типа устройств.



Самыми стойкими ко взлому во Второй мировой войне считали коды, которые создавала *«Энигма».* Принцип работы устройства был такой: при каждом нажатии на клавишу правый ротор сдвигается на одну позицию, а при определенных условиях сдвигаются и другие роторы. Движение роторов каждый раз приводило к разным криптографическим преобразованиям.

Код «Энигмы» дважды был расшифрован. Впервые, до Второй мировой, — в польском Бюро шифров в декабре 1932 года. После этого немецкие ученые усложнили устройство. Шифры новой «Энигмы», которая вышла в 1938 году, можно было расшифровать только с помощью более сложного механизма — «Бомбы Тьюринга», первая версия которой появилась в 1940 году. При этом мало кто знает о нашей шифровальной технике 1940-1950-х годов, например, о советской шифровальной машине «Фиалка», которая так и не была никем взломана и являлась засекреченной до недавнего прошлого.

В 1949 году Клод Шеннон пишет работу «Теория связи в секретных системах», и криптография окончательно переходит в сферу математики. К концу 1960-х роторные шифровальные системы заменяются более совершенными блочными, которые предполагали обязательное применение цифровых электронных устройств.

Начиная с 1990 года, ученые разрабатывали совершенно новую форму криптографии, называемую квантовой криптографией, в надежде еще раз повысить уровень защиты современного шифрования. С распространением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать на порядки более сложные шифры. Шифр или код становится языком общения между компьютерами, а криптография становится полноценной гражданской отраслью. В 1978 году разрабатывается стандарт шифрования DES, который стал основой для многих современных криптографических алгоритмов.

Сфера использования криптографии расширяется, при этом власти различных стран пытаются удержать контроль над использованием шифров. Разработки криптографов засекречиваются, от производителей шифровальных машин требуют оставлять в продуктах «черные ходы» для доступа спецслужб.

Параллельно независимые криптоаналитики разрабатывают способы шифрования, которыми могли бы пользоваться все желающие – так называемую открытую криптографию. Особенно актуально это стало с развитием интернета, где вопрос конфиденциальности информации встал очень остро. Первой криптосистемой с открытым ключом считается созданный в 1977 году алгоритм *RSA*, название которого является акронимом имен создателей – Риверста, Шамира и Адельмана.

**II. Практическая часть**

**Создание сборника**

Во время создания пособия, для того чтобы делать все в правильном порядке и не допустить каких-либо ошибок, мной было решено составить план из нескольких задач. Задумка заключалась в том, что при поэтапной работе с материалом я бы с большей вероятностью смогла реализовать задуманную мной идею и воплотить ее в жизнь.

При составлении учебного пособия о шифрах и кодах, были выполнены следующие задачи:

1. Собрать текстовые описания самых известных методов шифрования и разместить их в порядке от наиболее простых шифров к более сложным.
2. Подобрать или создать своими руками подходящие под описания изображения-шпаргалки для наглядной демонстрации работы шифрования.
3. Выбрать две различные фразы на различных языках и закодировать их всеми использованными шифрами.
4. Написать заметку для читателя и поместить ее перед текстом.
5. Оформить текст, привести его в удобный для прочтения вид и сделать копию на бумажном носителе.

**Сбор информации**

Перед выбором необходимых в пособии шифров, я внимательно изучила несколько статей в Интернете, в которых они бы повторялись или подвергались подробному изучению, а также ознакомилась с первой и седьмой главой книги «Введение в криптографию» Коллектива Авторов.

На основе полученных знаний я выбрала наиболее важные и полезные шифры, написала определение каждого из них и расположила в порядке от самых простых, таких как *ROT1*, где зашифрованным сообщением будет являться предложение, каждая буква которого заменяется следующей за ней в алфавите, до сложных шифров вроде *Шифра Плейфера* со вспомогательной матрицей и сложной в понимании системой кодировки.

**Внедрение изображений**

С уже имеющимися на руках данными мне не составило труда отыскать, а в некоторых случаях составить вручную таблицы, которые были использованы для объяснения принципа работы методов кодировки. Так, на примере азбуки Морзе можно увидеть использованные на рисунке буквы и символы, выделенные красным цветом.

**Подбор примеров**

В качестве примеров были взяты строчки из сказки «Красная Шапочка». За фразой Красной Шапочки на русском «*Для чего это у тебя такие большие уши?»* в оригинале следовал ответ «Это чтобы лучше слышать тебя», но из-за необходимости показать различия шифров с двумя разными алфавитами я заменила его на «*all the better to see you with».*

После того как оба предложения были зашифрованы по каждому методу, для точной уверенности я проверила их на правильность в криптографических онлайн калькуляторах и сравнила полученные результаты.

**Написание введения**

Прежде чем начать оформление текста, я занялась написанием краткого вступления для читателей, чтобы изучать текст было максимально удобно. В нем объяснен принцип зашифровывания примеров в каждом отдельном случае и назначение цветных рамок, использованных как инструмент оформления текста.

**Оформление и представление сборника на бумаге**

В процессе выделения примеров и изображений были исправлены орфографические и пунктуационные ошибки, в завершении я распечатала готовую работу и получила бумажную версию «Пособия начинающего шпиона».

**III. Заключение и выводы**

Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Распространение доступного интернета по всему миру невозможно представить без криптографии. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почтового сервиса, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка. С появлением мессенджеров, социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональной информации в сети происходит без остановки и в огромных количествах. Пока конфиденциальные данные требуют защиты, криптография будет продолжать развиваться. Криптографические системы, используемые в блокчейне криптовалют сегодня, представляют одну из наиболее продвинутых форм этой науки. Они также являются частью традиционной истории человечества.

Я выбрала эту науку криптографию для изучения, потому что с детства интересовалась кодированием и всем, что с ним связано. В будущем мне бы хотелось связать свою жизнь с информационной безопасностью, и такое подробное изучение столь важной темы не только поможет мне в дальнейшем погружении в тему, но и может предоставить наипростейшие знания заинтересовавшимся новичкам или освежить память хорошо ориентирующимся в шифрах людям.

В процессе изготовления моего пособия я научилась составлять план действий и следовать ему, расставлять приоритеты по степени важности определенных задач и правильно оформлять информационный продукт в виде сборника.

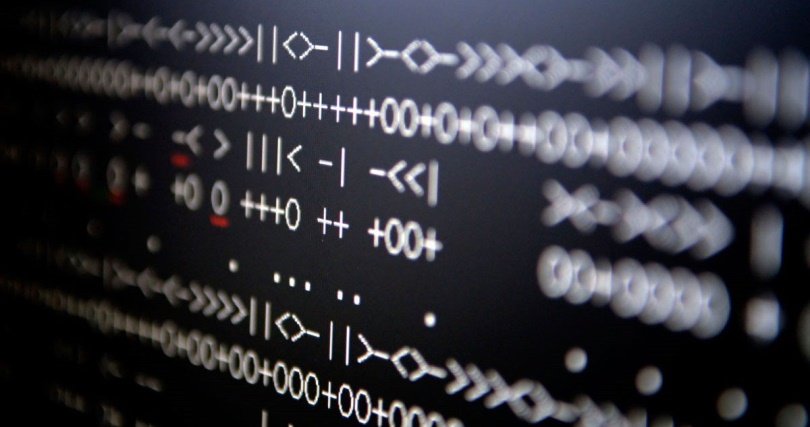
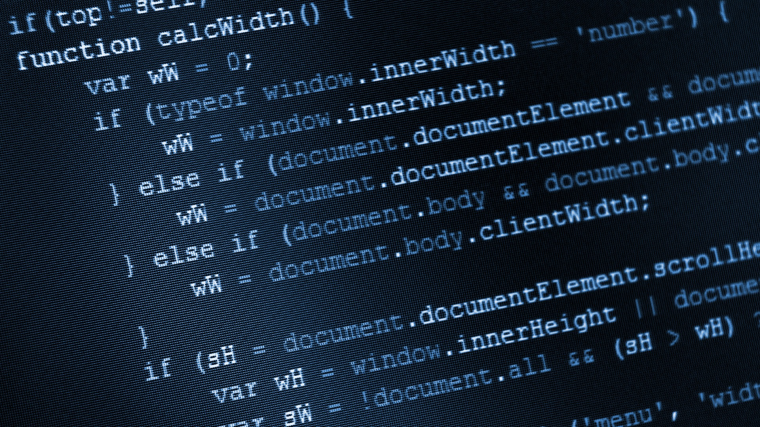
**IV. Список источников и литературы**

1. Коллектив Авторов, «Введение в криптографию», 2017
2. Саймон Сингх, «Книга шифров. Тайная история шифров и их расшифровки», издательство Астрель, 2007
3. Нильс Фергюсон, Брюс Шнайер, «Практическая криптография», издательство Вильямс, 2017
4. <http://algolist.ru/defence/intro.php>
5. <https://naked-science.ru/article/sci/ot-manuskriptov-do-shifrovalnyh>
6. <https://academy.binance.com/ru/articles/history-of-cryptography>
7. <https://tproger.ru/translations/understanding-cryptography/>
8. <http://www.realcoding.net/articles/vvedenie-v-kriptografiyu.html-0>
9. <https://oyla.xyz/article/kod-enigmy>
10. <https://thecode.media/vernam/>
11. <https://www.dcode.fr/hill-cipher>
12. <https://intellect.icu/>
13. <https://planetcalc.ru/>

**V. Приложение**

|  |
| --- |
| Пособие начинающего шпиона |

За авторством С.Г. Исаковой



**Перед прочтением**

Все используемые методы шифрования в этом пособии проверены временем и некоторые из них вряд ли могут быть использованы в качестве реальных кодов с целью засекречивания информации, однако эти методы могут быть интересны для изучения всем, кто, так или иначе, связан с наукой криптографией. К каждому шифру будет прилагаться пример на русском (*Для чего это у тебя такие большие уши?)* и английском (*All the better to see you with)* языках, обе фразы взяты из произведения «Красная шапочка», и каждая из них будет меняться в соответствии с правилами того или иного шифра. Все примеры выделены *курсивом* и помещены в зеленую рамку, как этот текст, для более понятного, интуитивного и удобного ориентирования в тексте

Картинки (шпаргалки), помещенные в красную рамку, содержат важную информацию, которая может помочь в процессе кодирования и декодирования

**Транспозиция**

В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Например, если каждое слово пишется задом наперед, то из *«Для чего это у тебя такие большие уши?»* получается «*?ишу еишьлоб еикат ябет у отэ огеч ялД»*. Другой пример — менять местами каждые две буквы. Таким образом, сообщение *«all the better to see you with»* станет *«la tl eh eb tt re ot es ye uo iw ht»*. Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, чтобы посылать важные сообщения.



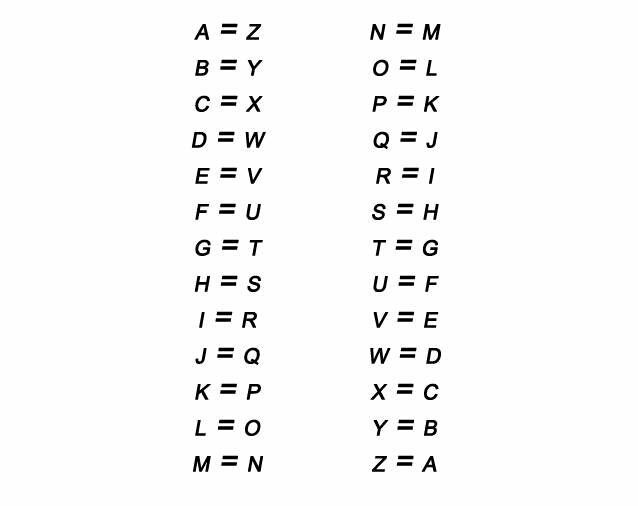
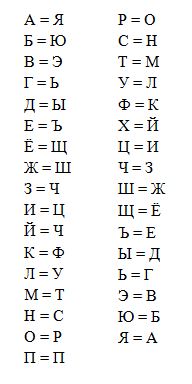
**ROT1**

Ключ прост: каждая буква заменяется на следующую за ней в алфавите. A заменяется на B, B на C, и т.д. «ROT1» значит «ROTate 1 letter forward through the alphabet» (англ. «сдвиньте алфавит на одну букву вперед»). Этот шифр весело использовать, потому что его легко понять и применять, но его так же легко и расшифровать. Из-за этого его нельзя использовать для серьезных нужд, но дети с радостью «играют» с его помощью.

*Для чего это у тебя такие большие уши? - Ема шёдп юуп ф уёва ублйё впмэщйё фщй?*

*all the better to see you with - bbm uif cfuufs up tff xjui*

**Шифр Атбаш**

Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее. Этот шифр использовался для еврейского алфавита и отсюда получил свое название. Первая буква – алеф, заменяется на тау (последнюю), вторая буква – бет, заменяется на шин (предпоследнюю). Из этих букв и сформировалось название.

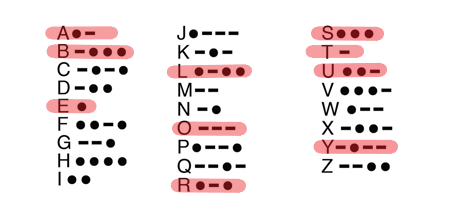
*all the better to see you with- zoo gsv yvggvi gl hvv blf drgs*

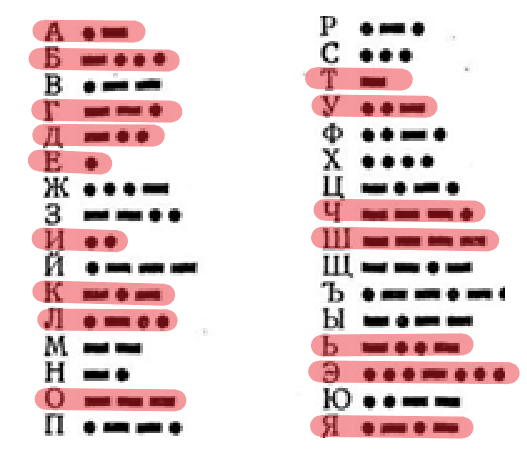
*Для чего это у тебя такие большие уши? - Ыуа зъьр вмр л мъюа мяфцъ юругжцъ лжц?*

**Азбука Морзе**

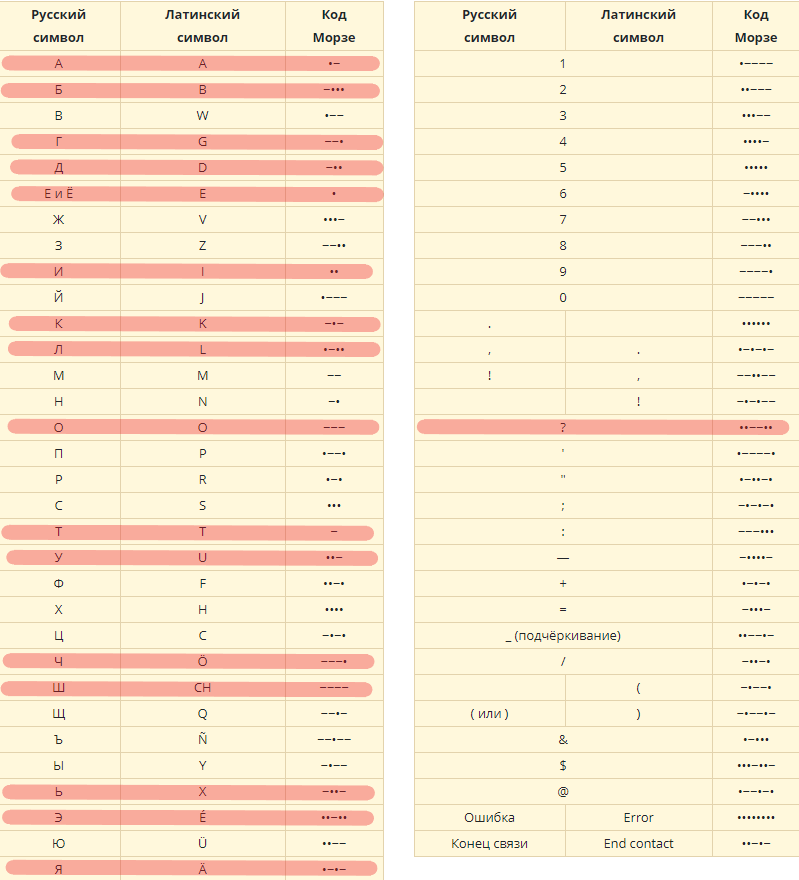
В азбуке Морзе каждая буква алфавита, все цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов, часто называемых «точками и тире». В отличие от большинства шифров, азбука Морзе используется не для затруднения чтения сообщений, а наоборот, для облегчения их передачи (с помощью телеграфа). Телеграф и азбука Морзе навсегда изменили мир, сделав возможной молниеносную передачу информации между разными странами, а также сильно повлияли на стратегию ведения войны.

*all the better to see you with* станет *•− •−•• •−•• − •••• • −••• • − − • •−• − −−− ••• • • −•−− −−− ••− •−− •• − ••••*



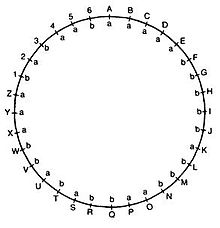


*Для чего это у тебя такие большие уши?* станет −•• •−•• •−•− −−−• • −−• −−− ••−•• − −−− ••− − • −••• •−•− − •− −•− •• • −••• −−− •−•• −••− −−−− •• • ••− −−−− •• ••−−••



**Шифр Бэкона**

Шифр Бэкона - метод сокрытия секретного сообщения, придуманный Фрэнсисом Бэконом в начале XVII века. Он разрабатывал шифры, которые бы позволяли передавать секретные сообщения в обычных текстах так, чтобы никто не знал об этих сообщениях. Шифр базируется на двоичном кодировании алфавита символами «A» и «B», которым можно сопоставить «0» и «1». Затем секретное послание «прячется» в открытом тексте, с помощью одного из способов сокрытия сообщений.

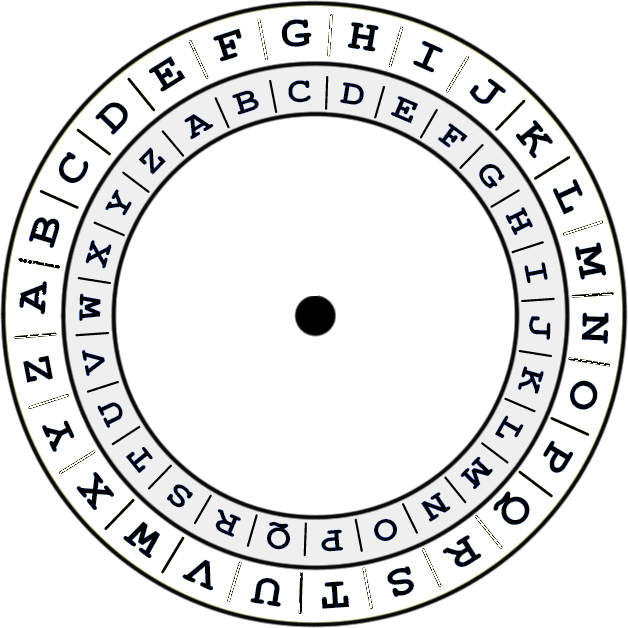


*all the better to see you with -* AAAAAABABBABABB BAABBAABBBAABAA AAAABAABAABAABBBAABBAABAABAAAB BAABBABBBA BAABAAABAAAABAA BBAAAABBBABABAA BABBAABAAABAABBAABBB

*Для чего это у тебя такие большие уши?-* AABAAABABBBBBBB BABBBAABABAAABBABBBA BBBABBAABAABBBA BAABB BAABAAABABAAAABBBBBB BAABAAAAAAABABAABAAAAABAB AAAABABBBAABABBBBBAABBAAAABAAAAABAB BAABBBBAAAABAAA?

**Шифр Цезаря**

Шифр Цезаря называется так, как ни странно, потому что его использовал сам Юлий Цезарь. На самом деле шифр Цезаря — это не один шифр, а целых двадцать шесть в английском языке и тридцать два в русском, использующих один и тот же принцип. Так, **ROT1** — всего один из них. Получателю нужно сказать, какой из шифров используется. Если используется шифр «G», тогда А заменяется на G, B на H, C на I и т.д. Если используется шифр «Y», тогда А заменяется на Y, B на Z, C на A и т.д. На шифре Цезаря базируется огромное число других, более сложных шифров, но сам по себе он не представляет из себя интереса из-за легкости дешифровки.



*В примере представлено преобразование* **ROT 21.**

*all the better to see you with - vgg ocz wzoozm oj nzz tjp rdoc*

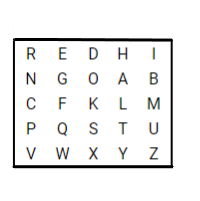
*Для чего это у тебя такие большие уши? - Шау лщчг сжг з жщху жфяэщ хгармэщ змэ?*

**Шифр Плейфера**

Классический шифр Плейфера предполагает в основе матрицу 5х5 (6х6 с русским алфавитом), заполненную символами латинского алфавита (i и j пишутся в одну клетку), которая составляется вручную по определенному плану, кодовое слово и дальнейшую манипуляцию над ними. Сообщение делится на биграммы (пары символов), после чего выполняется шифрование выполняется по нескольким правилам:

1) Если символы биграммы находятся в матрице на одной строке — смещаем их вправо на одну позицию. Если символ был крайним в ряду — он становится первым.

2) Если символы биграммы находятся в одном столбце, то они смещаются на одну позицию вниз. Если символ находился в самом низу столбца, то он принимает значение самого верхнего.

3) Если символы не находятся ни на одной строке, ни на одном столбце, то строится прямоугольник, где символами являются края диагонали, а углы меняются местами.



*Зашифровываемый текст - all the better to see you with*

*Ключ - red riding hood*

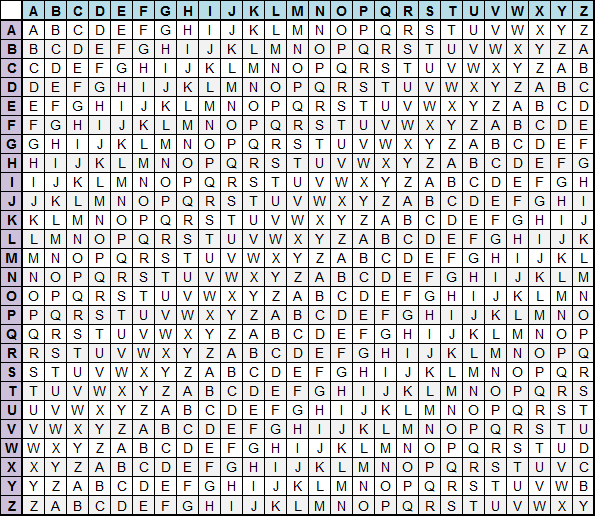
*Зашифрованный текст – LTTYIDGISYQHHPKXDWHWBSZEYA*

*Зашифровываемый текст - Для чего это у тебя такие большие уши?*

*Ключ – красная шапочка*

*Зашифрованный текст – ВНХЖЖДДФЗЕИЗЖВЮУСРТЧВЧМЩРТЖТРТ*

**Шифр Виженера**

Этот шифр сложнее, чем моноалфавитные, в которых каждая буква/символ заменяет лишь одну другую букву/символ. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Применительно к латинскому алфавиту таблица Виженера составляется из строк по двадцать шесть символов, причём каждая следующая строка сдвигается на несколько позиций.

Таким образом, в таблице получается двадцать шесть различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

*Зашифровываемый текст - all the better to see you with*

*Ключ - red riding hood*

*Зашифрованный текст - rpo kph jrzasf wf whv grc joav*

*Зашифровываемый текст - Для чего это у тебя такие большие уши?*

*Ключ – красная шапочка*

*Зашифрованный текст - оья итгн хтю в йпбй гаьце ажллжап угщ?*