**Муниципальное бюджетное общеобразовательное учреждение**

**«Средняя общеобразовательная школа №30»**

142121, Российская Федерация, Московская область, Подольск, Юбилейная, 5

Тел:8(496)755-88-48 E-mail: [pdls\_mbou\_30@mosger.ru](mailto:pdls_mbou_30@mosger.ru)

**ПРОЕКТ на тему:**

**«Шифрование информации»**

Выполнила:

Абрамова Виктория Алексеевна

10 класс, МБОУ СОШ №30

Научный руководитель:

Иванова Наталья Юрьевна,

учитель информатики

МБОУ СОШ №30

**Содержание**

[**Введение** 3](#_Toc133166081)

[**Что такое шифр и шифрование?** 3](#_Toc133166082)

[**1.1 Азбука Морзе** 4](#_Toc133166083)

[**1.2 Шифр Цезаря** 6](#_Toc133166084)

[**1.3 Шифр Гронсфельда** 7](#_Toc133166085)

[**1.4 Цифровые шифры** 8](#_Toc133166086)

[**1.5 Квадрат Полибия** 8](#_Toc133166087)

[**1.6 Шифр Виженера** 10](#_Toc133166088)

[**1.7 Шифр Ришелье** 11](#_Toc133166089)

[**2.1 Современная криптография** 12](#_Toc133166090)

[**2.2 Симметричные криптосистемы** 13](#_Toc133166091)

[**2.3 Криптосистема с открытым ключом** 15](#_Toc133166092)

[**2.4 Управление криптографическими ключами** 16](#_Toc133166093)

[**Написание программ для простейших шифров** 17](#_Toc133166094)

[**Применение криптографии в современном мире** 19](#_Toc133166095)

[**Заключение** 22](#_Toc133166096)

# **Введение**

Любой из нас знает такое слово как "шифрование". Оно входит в состав криптографии. Она появилась впервые в Древнем Египте. Криптографии уже больше 4-х тысяч лет.

Существуют свидетельства, что криптография как техника защиты текста появилась вместе с письменностью, и уже древними цивилизациям Индии, Египта и Месопотамии были известны способы тайного письма.

В наше время, каждый встречается с шифрованием даже не замечая этого. Мы используем разные Интернет-ресурсы каждый день, которые зашифровывают данные для того, чтобы избежать получения этих данных третьими лицами.

Когда мы набираем текст в поисковой строке, поисковик шифрует доступные ему данные. В наш век довольно ценна информация. Вряд ли кто-то захочет, чтобы его сообщение прочитал кто-то другой, а не получатель. Многие люди передают в сообщениях большое количество ценной и конфиденциальной информации. Большинство сервисов обмена сообщений поддерживают шифрование, чтобы ваша информация не попала злоумышленнику

**Актуальность темы:** Актуальность данной проблемы в том, что в наше время, развитие хищения личных данных и ценной информации растет все больше.

**Объект исследования:** Что такое шифрование, способы шифрования информации и области применения.

**Цель:** Рассмотреть простейшие и наиболее современные шифры, ознакомиться с литературой по теме.

# **Что такое шифр и шифрование?**

Шифр - какая-либо система преобразования текста с ключом для обеспечения конфиденциальности передаваемой информации. Шифры применяются для тайной переписки дипломатических представителей со своими правительствами, некоторыми интернет-сервисами по различным причинам, банками для обеспечения безопасности транзакций, а также в вооруженных силах для передачи текста секретных документов по техническим средствам связи.

Шифр может представлять собой условную азбуку из цифр или букв, либо алгоритм преобразования обычных цифр и букв. Шифрованием называется процесс засекречивания сообщения с помощью шифра. Криптографией называется наука о создании и использовании шифров. Наука о методах получения исходного значения зашифрованной информации называется криптоанализ.

Важным параметром любого шифра является ключ. Ключ - это параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма. В современной криптографии предполагается, что вся секретность криптографического алгоритма сосредоточена в ключе, но не деталях самого алгоритма (принцип Керкгоффса).

Не стоит путать шифр с кодированием. Кодирование - это фиксированное преобразование информации из одного вида в другой. В наше время кодирование практически не используется для защиты информации, в основном оно используется лишь от ошибок при передаче данных и других целях, не связанных с защитой.

## **1.1 Азбука Морзе**

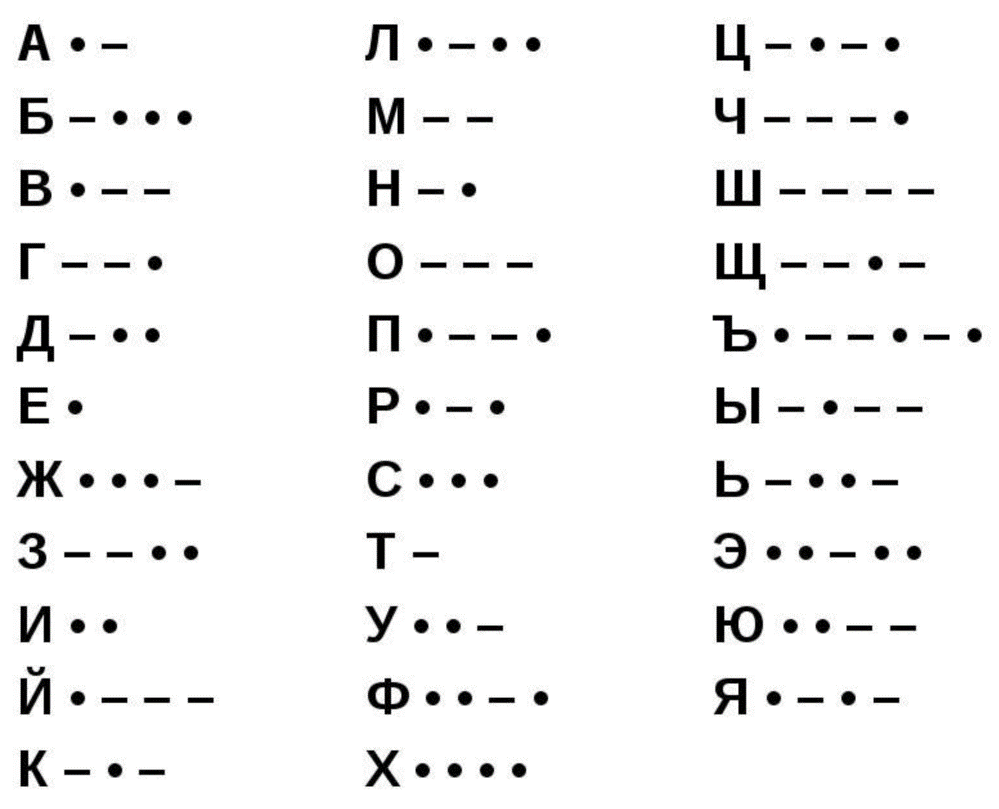
Азбука Морзе – довольно распространенный способ знакового кодирования. В нём все буквы, знаки препинания и другие символы представляются в виде последовательности сигналов. Тире – длинный сигнал, точка – короткий. Азбука Морзе была создана изобретателями Сэмюэлем Морзе, Альфредом Вейлем и Джозефом Генри в 1838 году для изобретенного ими телеграфного аппарата, получившего название аппарат Морзе. Некоторые исследователи полагают, что автором кода был Альфред Вейл — партнёр Самюэля Морзе по бизнесу, известный тем, что ввел «коммерческий код» из групп по 5 символов.

Первый, оригинальный, код Морзе отличался от современного. В нем использовались посылки множества разных длительностей: «точка», «тире», «длинное тире», которое в 4 раза длиннее «точки». Также использовались паузы разной длины внутри символа.

В 1848 году Фридрих Герке усовершенствовал код Морзе, введя туда новые символы, сделав неизменными межэлементные паузы внутри символа и оставив только два по длительности элемента: короткий - точка и длительный - тире.

Русский вариант азбуки был принят в 1856 году. В 2004 году Международный союз электросвязи (МСЭ) ввёл в азбуку Морзе новый код для символа «@» (· — — · — ·) для удобства передачи адресов электронной почты.

Для передачи сообщений на русском также придумали трёхбуквенные сокращения: ЗДР – здравствуйте, ДСВ – до свидания, СПБ – спасибо, БЛГ – благодарю и другие.

****

**Особенности кода Морзе:**

* Для кодирования используются два звуковых сигнала: длинный (тире) и короткий (точка).
* За единицу времени принимается длительность короткого сигнала (одной точки).
* Длительность тире равно длительности трёх точек.
* Пауза между элементами одного знака – одна точка.
* Пауза между знаками в слове – три точки.
* Пауза между словами – семь точек.

## **1.2 Шифр Цезаря**

Шифр Цезаря является одним из самых простых и известных методов шифрования. Данный шифр заключается в том, что каждый символ заменяется другим символом, который находится на некоторое количество позиций левее или правее него. Например, в шифре со сдвигом вправо на 3, буква Д будет заменяться на букву Ж.

Данный шифр назван в честь римского полководца Гая Юлия Цезаря. Он использовал данный шифр со сдвигом 3, чтобы защищать военные сообщения.

Например, сопоставим обычный русский алфавит и шифрованный со сдвигом вправо на 3:

|  |  |
| --- | --- |
| Обычный 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 |
| Шифрованный | 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 |

Или возьмём текст, и зашифруем его:

**Исходный текст:**

*Компьютер выполняет ваши команды, но не способен читать ваши мысли.*

**Шифрованный текст:**

*Нсптябхзу еютсорвзх егыл нспгржю, рс рз фтсфсдзр ълхгхя егыл пюфол.*

Я считаю, что шифр Цезаря довольно просто взломать и сообщение потеряет свою конфиденциальность. В наше время этот мало где используется. Например, взломщик может знать или просто догадаться, что использовался простой шифр подстановки, подобрать значение сдвига и расшифровать сообщение.

То есть, чтобы прочитать сообщение, написанное шифром Цезаря достаточно знать сдвиг. Допустим сдвиг k=3, то текст можно расшифровать по формуле x=y-k, где x -номер исходного символа в алфавите, а y – номер символа в шифрованном алфавите.

## **1.3 Шифр Гронсфельда**

Шифр Гронсфельда – представляет собой модификацию шифра Цезаря числовым ключом, является шифром сложной замены. Необходимо записать цифры числового ключа под буквами исходного сообщения. Цифры ключа необходимо циклически повторять, пока длина числового ключа не будет соответствовать длине исходного сообщения. Шифр текст получается примерно также, как в шифре Цезаря, только сдвиг будет не 3 , а на ту цифру ключа, которая записана под буквой.

Данный шифр был создан графом Гронсвельдом - руководителем первой дешифровальной службы Германии в XVII веке. Этот шифр можно считать усовершенствованием шифра Цезаря.

Например, возьмем текст и зашифруем его:

K=39425 (ключ)

|  |  |
| --- | --- |
| Исходный текст | Итоговый проект |
| Ключ | 39425394 253942 |
| Шифрованный текст | Лытеуедн схсноф |

Следует отметить, что шифр Гронсфельда вскрывается относительно легко потому, что в числовом ключе каждая цифра имеет только десять значений, следует, мы имеем лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

## **1.4 Цифровые шифры**

Алфавит разбивается на группы с равным количеством букв в одной группе, и каждой группе присваивается свой номер. Для шифровки используются две цифры. Первая из которых – номер группы, а вторая - порядковый номер буквы в группе.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| АБВГ | ДЕЖЗ | ИЙКЛ | МНОП | РСТУ | ФХЦЧ | ШЩЪЫ | ЬЭЮЯ |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

В таблице может быть разное количество групп, и буквы могут идти не по порядку.

Например, возьмем слово и зашифруем его:

Исходное слово: криптография

Зашифрованное: 33 51 31 44 53 43 14 51 11 61 31 84

## **1.5 Квадрат Полибия**

Одну из первых систем шифрования, в которой использовалась таблица, описал древнегреческий историк Полибий. Точно неизвестно, является ли писатель автором этого шифра. Тем не менее специалисты называют этот шифр «квадратом Полибия». Этот шифр широко применялся как греками, так и римлянами еще до наступления нашей эры .

При использовании данного шифра составляется таблица, в каждую клетку которой, вписывается буква. Вписывать буквы можно в любом порядке.

Алгоритм шифрования заключается в том, что при шифровании исходного текста, нужно найти в составленной таблице нужную букву и в шифрованный текст вставить букву, находящуюся в нижней от неё ячейке того же столбца. Если буква исходного текста находится в ячейке нижней строки таблицы, то в шифрованный текст нужно вставить букву, находящуюся в верхней ячейке того же столбца.

В русском алфавите 33 буквы .

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

В качестве примера зашифруем с помощью шифра «квадрат Полибия» исходный текст: «Шифрование информации»

Шифрованный текст: «Гоьэузетол отьуэсебоо»

Или например зашифруем слово «Капсула»: «Пефцшре»

Это был **первый метод** шифрования с помощью квадрата Полибия.

**Второй метод:**

Вместо буквы записываются соответствующие ей цифры из таблицы. Всего две цифры. Первая – номер столбца, вторая – номер строки. Эти цифры являются координатами буквы. Первая цифра – вертикальная координата, вторая – горизонтальная. В результате мы получим запись координат для каждой буквы. Составив таблицу мы получим две строки, одна с горизонтальными координатами всех букв, а вторая с вертикальными.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | К | А | П | С | У | Л | А |
| Вертикальные | 5 | 1 | 5 | 2 | 4 | 1 | 1 |
| Горизонтальные | 2 | 1 | 3 | 4 | 4 | 3 | 1 |

Затем считываем координаты с составленной таблицы по строкам, а не по столбцам. И потом вновь заменяем на буквы согласно таблице.

Координаты по строкам: 51 52 41 12 13 44 31

Заменяем буквы по таблице по новым координатам и строим таблицу.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Буквы | Д | К | Г | Е | Л | У | В |
| Вертикальные | 5 | 5 | 4 | 1 | 1 | 4 | 3 |
| Горизонтальные | 1 | 2 | 1 | 2 | 3 | 4 | 1 |

В итоге после шифрования у нас получается: дкгелув

**Третий метод:**

Мы берем первые координаты по строкам: 51524112134431

Эту последовательность цифр сдвигаем циклически влево на один

шаг: 15241121344315

Далее полученную последовательность вновь разбиваем на группы по два: 15 24 11 21 34 43 15

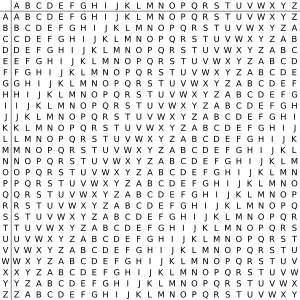
Составляем таблицу по полученным координатам:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | Э | С | А | Б | Т | О | Э |
| Вертикальные | 1 | 2 | 1 | 2 | 3 | 4 | 1 |
| Горизонтальные | 5 | 4 | 1 | 1 | 4 | 3 | 5 |

После шифрования у нас получается: эсабтоэ

## **1.6 Шифр Виженера**

В шифре Цезаря любая буква алфавита смещается на несколько позиций; к примеру в шифре Цезаря при сдвиге +3, А стало D, В стало бы Е и так далее. Шифр Виженера складывается из последовательности нескольких шифров Цезаря с разными значениями сдвига. Для зашифровывания может применяться таблица алфавитов, называемая tabula recta либо квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера оформляется из строк по 26 символов, при этом каждая следующая строка смещается на несколько позиций. Таким образом, в таблице получается 26 разных шифров Цезаря. На каждом этапе шифрования применяются различные алфавиты, выбираемые в зависимости от символа ключевого слова.



Например, зашифруем слово «Programs». Для шифрования этим методом нужен ключ. Допустим, наш ключ, это слово «net». Наше ключевое слово должно соответствовать длине исходного слова, для этого мы циклически повторяем его до тех пор, пока их длины не будут равны.

Исходное слово: programs

Ключ: netnetne

Дальше по таблице Виженера, представленной выше, мы смотрим и шифруем слово. Для этого необходимо сопоставлять букву исходного слова с буквой ключа соответственно. По таблице мы ищем букву исходного слова по горизонтали, а букву ключа по вертикали. Находим букву, стоящую на их пересечении, и записываем ее. Например, первая буква нашего исходного слова «p», а первая буква ключа «n». По таблице Виженара, мы смотрим, что на их пересечении стоит буква «c».

Таким образом, мы получаем:

Исходное слово: programs

Ключ: netnetne

Шифрованное слово: cvhtvtzw

## **1.7 Шифр Ришелье**

Данный метод шифрования заключается в том, что исходный текст разбивается на отрезки, а буквы внутри отрезков переставляются в соответствии с ключом.

Например:

*Исходный текст: шифр ришелье (шиф рриш елье)*

Ключ: 321 4312 1324

*Шифрованный текст: фиш ишрр еьле*

То есть, в ключе мы указываем на какую позицию переставляется каждая буква в отрезке, и на какие отрезки мы разбиваем исходный текст.

## **2.1 Современная криптография**

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.

2. Криптосистемы с открытым ключом.

3. Системы электронной подписи.

4. Управление ключами.

Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание.

Основные направления использования криптографических методов – хранение информации на носителях в зашифрованном виде, передача конфиденциальной информации по каналам связи, установление подлинности передаваемых сообщений.

Криптографические методы можно разбить на две группы:

1. Сжатие информации с помощью замены слов, предложений, сочетаний букв.
2. Обработка информации путем замены или перемещения букв, при котором объем данных не меняется.

По способу реализации криптографические методы возможны в аппаратном и программном исполнении.

Для защиты текстовой информации при передачах на удаленные станции телекоммуникационной сети используются аппаратные способы шифрования и кодирования. Для обмена информацией между ЭВМ по телекоммуникационной сети, а также для работы с локальными абонентами возможны как аппаратные, так и программные способы. Для хранения информации на магнитных носителях применяются программные способы шифрования и кодирования.

Аппаратные способы шифрования информации применяются для передачи защищенных данных по телекоммуникационной сети.

Для реализации шифрования с помощью смешанного алфавита используется перестановка отдельных разрядов в пределах одного или нескольких символов.

Программные способы применяются для шифрования информации, хранящейся на магнитных носителях (дисках, лентах). Это могут быть данные различных информационно-справочных систем АСУ, АСОД и др. программные способы шифрования сводятся к операциям перестановки, перекодирования и сложения по модулю 2 с ключевыми словами.

Особое место в программах обработки информации занимают операции кодирования. Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется кодированием. На практике кодирование всегда используется для уменьшения объема памяти, так как экономия памяти ЭВМ имеет большое значение в информационных системах. Кроме того, кодирование можно рассматривать как криптографический метод обработки информации.

## **2.2 Симметричные криптосистемы**

Симметричные криптосистемы (симметричное шифрование, симметричные шифры) - способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ.

Классическими примерами таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

* Простая перестановка
* Одиночная перестановка по ключу
* Двойная перестановка
* Перестановка «Магический квадрат»

В настоящее время симметричные шифры — это:

* блочные шифры. Обрабатывают информацию блоками определённой длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект — нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.
* поточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме.

**Виды симметричных шифров**

**Блочные шифры:**

* AES (англ. Advanced Encryption Standard) — американский стандарт шифрования
* ГОСТ 28147-89 — советский и российский стандарт шифрования, также является стандартом СНГ
* DES (англ. Data Encryption Standard) — стандарт шифрования данных в США
* RC5
* Blowfish
* Twofish
* IDEA (International Data Encryption Algorithm, международный алгоритм шифрования данных)

**Потоковые шифры:**

* RC4 (алгоритм шифрования с ключом переменной длины)
* SEAL (Software Efficient Algorithm, программно-эффективный алгоритм)
* WAKE (World Auto Key Encryption algorithm, алгоритм шифрования на автоматическом ключе)

## **2.3 Криптосистема с открытым ключом**

Криптографическая система с открытым ключом (разновидность асимметричного шифрования, асимметричного шифра) - система электронной подписи (ЭП), при которой открытый ключ передаётся по открытому каналу и используется для проверки ЭП и для шифрования сообщения.

Асимметричное шифрование с открытым ключом базируется на следующих принципах:

* Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным.
* Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным.
* Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.

Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ. Отправитель шифрует свое сообщение открытым ключом получателя и передает его получателю (владельцу ключей) по открытым каналам. При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа.

В результате можно обеспечить надёжное шифрование сообщений, сохраняя ключ расшифровки секретным для всех - даже для отправителей сообщений.

**Виды асимметричных шифров**

* RSA (Rivest-Shamir-Adleman)
* DSA (Digital Signature Algorithm)
* Elgamal (Шифросистема Эль-Гамаля)
* Diffie-Hellman (Обмен ключами Диффи — Хелмана)
* ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи.
* ГОСТ Р 34.10-2012

## **2.4 Управление криптографическими ключами**

Под ключом в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения. В последнее время безопасность защищаемой информации стала определяться в первую очередь ключом. Сам шифр, шифрмашина или принцип шифрования стали считать известными противнику и доступными для предварительного изучения, но в них появился неизвестный для противника ключ, от которого существенно зависят применяемые преобразования информации. Теперь законные пользователи, прежде чем обмениваться шифрованными сообщениями, должны тайно от противника обменяться ключами или установить одинаковый ключ на обоих концах канала связи. А для противника появилась новая задача - определить ключ, после чего можно легко прочитать зашифрованные на этом ключе сообщения.

Отметим теперь, что не существует единого шифра, подходящего для всех случаев. Выбор способа шифрования зависит от особенностей информации, ее ценности и возможностей владельцев по защите своей информации. Прежде всего подчеркнем большое разнообразие видов защищаемой информации: документальная, телефонная, телевизионная, компьютерная и т.д. Каждый вид информации имеет свои специфические особенности, и эти особенности сильно влияют на выбор методов шифрования информации. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации. Выбор вида шифра и его параметров существенно зависит от характера защищаемых секретов или тайны.

Любая современная криптографическая система построена на использовании криптографических ключей. Она работает по определенной процедуре, состоящей из: одного или более алгоритмов шифрования ; ключей, используемых этими алгоритмами шифрования; системы управления ключами; незашифрованного текста; и зашифрованного текста (шифртекста).

Асимметричные ключи отличаются от симметричных ключей тем, что алгоритмы используют отдельные ключи для шифрования и дешифрования, в то время как алгоритм симметричного ключа использует один ключ для обоих процессов. Поскольку в асимметричном алгоритме используется несколько ключей, процесс создания занимает больше времени, чем алгоритм с симметричным ключом. Однако преимущества заключаются в том, что асимметричный алгоритм намного более безопасен, чем алгоритм с симметричным ключом.

При использовании симметричного ключа ключ должен быть передан получателю, где всегда существует вероятность того, что ключ может быть перехвачен или подделан. При использовании асимметричного ключа сообщение и / или сопутствующие данные могут быть отправлены или получены с использованием открытого ключа; однако получатель или отправитель будет использовать свой личный закрытый ключ для доступа к сообщению и / или сопровождающим данным.

## **Написание программ для простейших шифров**

В практической части своей работы, я бы хотела написать несколько программ по выбранной теме. Для того чтобы создать программу, необходимо определиться, на каком языке программирования будет написана ваша программа и какой именно шифр вы будете использовать.

В этой части своей работы я напишу программу для трёх шифров, разобранных выше в моей работе. Программы будут представлены на языках программирования python .

Первая программа будет шифровать ваш текст с помощью всеми известного и довольно простого шифра – **Азбуки Морзе**.

morze = {'a': '•—', 'b': '—•••', 'c': '—•—•', 'd': '—••', 'e': '•', 'f': '••—•', 'g': '——•', 'h': '••••', 'i': '••', 'j': '•———', 'k': '—•—', 'l': '•—••', 'm': '——', 'n': '—•', 'o': '———', 'p': '•——•', 'q': '——•—', 'r': '•—•', 's': '•••', 't': '—', 'u': '••—', 'v': '•••—', 'w': '•——', 'x': '—••—', 'y': '—•——', 'z': '——••'}

a = input()

a = a.lower()

g = []

j=0

for i in a:

k = morze.get(i,'\t')

if k != '\t':

j = k+" "

g.append(j)

else:

j ='\t'

g.append(j)

print("".join(g))

**Шифр Цезаря:**

abc = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"

shift = int(input('Сдвиг:'))

n = len(abc)

message = input("Введите слово: ")

result = ""

for symbol in message:

ind = abc.index(symbol)

ind\_2 = ind+shift

if ind\_2&n:

ind\_2=ind\_2-n

symbol\_2 = abc[ind\_2]

result = result + symbol\_2

print("Результат: ",result)

## **Применение криптографии в современном мире**

Криптография — это наука, изучающая сохранение целостности данных и способы шифровки. В этой области трудятся сотни и тысячи специалистов. Работа данных специалистов имеет множество как положительных, так и отрицательных сторон.

Информация шифруют для того, чтобы она не досталась противнику. Естественно, это касается не всей информации, а только действительно секретной и важной. Шифр и шифрование применяются, когда информацию нужно передать своим людям, но имеется большая вероятность того, что она попадёт в чужие руки. Информация может быть и военной, и дипломатической, и касаться государственной разведки. А может принадлежать какой-либо коммерческой структуре.

С военной информацией работают военные шифровальщики, если она касается международной разведки и контрразведки - это дело сотрудников ФСБ. В коммерческих структурах этим занимаются сотрудники отделов информационной безопасности.

Разработкой шифрующих программ и способов шифровки занимаются криптографы. Для этой работы требуется высокая квалификация. Это же касается и работы специалиста по взлому шифров, криптоаналитика.

К минусам профессии шифровальщика относится повышенная секретность. Если шифровальщик занимается важными и серьезными секретами государства, он не должен говорить о своей работе никому, даже о том, в какой структуре он работает и как именно называется его специальность. От его умения молчать и уровня квалификации могут зависеть успехи (или же провалы) спецслужб. Если шифровальщик служит в Армии, то ещё несколько лет после службы он не может выезжать за рубеж.

Также весьма секретной информацией является коммерческая. В коммерческих структурах этот минус оборачивается плюсом: даже у рядовых шифровальщиков отдела информационной безопасности весьма высокие зарплаты.

Шифровальщик может работать в IT-службах, отделах информационной безопасности компаний. Военные шифровальщики и шифровальщики системы федеральной безопасности - это связисты. Они находятся на службе в соответствующих структурах Министерства обороны или ФСБ.

Специальность шифровальщика можно получить в Армии. Например, во время срочной службы, можно попасть в школу шифровальщиков при военном училище. Шанс повышается, если у вас есть диплом техникума связи.

Также можно поступить на учёбу и самостоятельно. Есть довльно много вузов по данной специальности.

**Вузы:**

• [Краснодарское высшее военное училище имени генерала армии С. М. Штеменко (КВВУ им. Штеменко)](https://kvvu.mil.ru/)

Специальность «Защита информации на объектах информатизации военного назначения».

Квалификация «Специалист по защите информации».

• [Институт криптографии, связи и информатики (ИКСИ) Академии ФСБ России](http://academy.fsb.ru/index_i.html)

Специальность «Криптография»

• [Московский государственный технический университет им.](https://bmstu.ru/)

[Н. Э. Баумана (МГТУ им. Баумана)](https://bmstu.ru/)

Факультет «Информатика и системы управления».

В функции шифровальщиков входит исключительно защита информации. Этим и обусловлен достаточно узкий спектр их профессиональных обязанностей. Он включает в себя:

* Расшифровку входящих данных.
* Шифровку важных документов.
* Работу со специальными программами шифрования, ключами, кодами и т.д.
* Перехват секретных сведений.
* Пресечение попыток взлома сайтов
* Защита информации о влиятельных персонах

Защита информации имеет важное значение в сохранении информации корпоративных данных. Утечка эксклюзивных разработок и статистических показателей приводит к серьезным убыткам. Этим объясняется достаточно высокая заработная плата профессиональных криптографов.

Уровень дохода зависит от квалификации специалиста. Как и другие IT-эксперты шифровальщики разделяются на специалистов junior, middle и senior класса. Начинающие профи получают оклад в размере 40 – 70 тысяч рублей в зависимости от региона, направления деятельности и масштабности компании. Профессионалы с опытом работы и знанием сложного специализированного ПО получают 100 – 110 тысяч рублей. Шифровальщики экстра-класса, готовые работать со сложными алгоритмами, кодами и шифрами получают до 500 тысяч рублей.

## **Заключение**

В ходе работы над индивидуальным проектом, была достигнута поставленная цель. Я рассмотрела простейшие и наиболее современные шифры. Описала наиболее известные из них. Написала программы по простейшим шифрам. Рассказала об областях применения шифрования информации, особенностях профессии связанной с шифрованием и об обязанностях таких специалистов. Нашла и поделилась несколькими вузами с факультетами по данной специальности. Проделанная работа помогла мне понять, как важно шифрование информации в совремнном мире.

## **Список использованных источников и литературы**

Урок информационно-технологического профиля "Криптография – один из способов защиты информации". // Открытый урок Первое сентября URL: https://urok.1sept.ru/articles/612933 (дата обращения: 24.12.2022).

Лекция №11 Шифрование информации // Helpiks URL: https://helpiks.org/7-49972.html (дата обращения: 10.01.2023).

Лекция 4 способы защиты информации Криптография. Модель криптографической системы. Технология шифрования речи. Общие положения защиты информации и характеристика защитных действий. // StudFiles URL: https://studfile.net/preview/2892371/page:5/ (дата обращения: 15.03.2023).

СОВРЕМЕННОЕ ШИФРОВАНИЕ ИЗНУТРИ: КАКИМ ОБРАЗОМ ПРОИСХОДИТ, ГДЕ ИСПОЛЬЗУЕТСЯ, НАСКОЛЬКО БЕЗОПАСНО // Trashbox.ru URL: https://trashbox.ru/link/what-is-encryption (дата обращения: 25.03.2023).

Шифровальщик (Криптограф) // Профгид URL: https://www.profguide.io/professions/Kriptograf.html (дата обращения: 22.04.2023).

Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. - М.: Гелиос АРВ, 2016

Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. - М.: Теис, 2017

<https://camo.githubusercontent.com/e678c34d30536f92fce7bce7d42ad11c1e690d9bd238209ab3e218510a70f8fa/68747470733a2f2f75706c6f61642e77696b696d656469612e6f72672f77696b6970656469612f636f6d6d6f6e732f7468756d622f322f32352f566967656e25433325413872655f7371756172652e7376672f33303070782d566967656e25433325413872655f7371756172652e7376672e706e67>

<https://fikiwiki.com/uploads/posts/2022-02/1645043987_6-fikiwiki-com-p-kartinki-azbuka-morze-7.png>