**Что изучает криптология?**

Издавна люди изыскивали способы уберечь некоторые важные сообщения от посторонних глаз. Рассказывают, как один царь обрил голову гонца, написал на ней послание и отослал гонца к своему союзнику лишь тогда, когда волосы на его голове отросли. Развитие химии дало удобное средство для тайнописи: симпатические чернила, записи которыми не видны до тех пор, пока бумагу не нагреют или обработают каким-нибудь химикатом. Но чаще стали применять шифры: сначала ими пользовались пираты, отмечая расположение кладов, алхимики, купцы, заговорщики. Впоследствии - дипломаты, стремящиеся сохранить тайны переговоров, военачальники, скрывающие от противника отданные распоряжения, разведчики и другие. [1]

**Криптоло́гия** (от др.-греч. κρυπτός — скрытый и λόγος — слово) — наука, занимающаяся методами шифрования и дешифрования.

**Шифр** – это какая-либо система преобразования текста для обеспечения секретности передаваемой информации.

Шифр может представлять собой совокупность условных знаков (условная азбука из цифр или букв) либо алгоритм кодирования с использованием обычных цифр и букв. Процесс засекречивания сообщения с помощью шифра называется шифрованием. Наука о создании и использовании шифров называется **криптографией.** **Шифрование**– это приведение информации к такому виду, когда содержимое исходного текста невозможно прочитать и трудно раскрыть без знания ключа, а **дешифрование** – это процесс привидения информации к исходному виду. **Ключ**– это информация, с помощью которой выполняется шифрование и дешифрование сообщения. Результатом шифрования является **шифрограмма** или **криптограмма**.

**История развития шифров и криптографии.**

Почти четыре тысячи лет назад в городе Менет-Хуфу на берегу Нила некий египетский писец нарисовал иероглифы, рассказавшие историю жизни его господина. Сделав это, он стал родоначальником документально зафиксированной истории криптографии.

Эта система не была тайнописью в том смысле, как ее понимают в современном мире. Для засекречивания своей надписи египетский писец не использовал никакого полноценного шифра. Дошедшая до наших дней надпись, вырезанная примерно в 1900 году до н. э. на гробнице знатного человека по имени Хнумхотеп, лишь в отдельных местах состоит из необычных иероглифических символов вместо более привычных иероглифов. Безымянный писец старался не затруднить чтение текста, а лишь придать ему большую важность. Вместе с тем, хотя писец применил не тайнопись, он, бесспорно, воспользовался одним из существенных элементов шифрования - умышленным преобразованием письменных символов. Это самый древний известный нам текст, который претерпел такие изменения. [1]

История криптографии насчитывает несколько тысячелетий. Первые письменные источники относятся к 1900-м годам до н. э. Именно этим периодом датируются найденные в Египте свитки, в которых использованы видоизмененные иероглифы, по-видимому, применявшиеся для тайного обмена сведениями. Запись на неизвестном языке — это уже тайная запись.

**Знакомство с шифрами.**

**Шифр Атбаш.**

Шифр Атбаш был, скорее всего, изобретен Ессеями, иудейской сектой повстанцев. [2] Они разработали множество различных кодов и шифров, которые использовались для сокрытия важных имен и названий, чтобы потом избежать преследования. В основе лежит метод замены: вместо первой буквы алфавита писалась последняя буква, вместо второй – предпоследняя и так далее (рис.1). Рис.1

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

ПРИМЕР:

Исходный текст: ЗАКОН СЛОЖЕНИЯ.

Зашифрованный текст: ЧЯФРСНУРЩЪСЦА

**Шифр Юлия Цезаря.**

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.   
Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной перепискиРис.2

Для удобства шифрования можно переписать алфавит так, как показано на рис. 3., либо самостоятельно изготовить шифровальный диск Цезаря (рис.2).

Рис.3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Исходный текст** | 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 |
| **Зашифрованный текст** | 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 |

Достоинства - простота шифрования и дешифрования.

Недостатки - легко взламывается и, поэтому не имеет практически никакого применения.

ПРИМЕР:

Исходный текст: КООРДИНАТНЫЙ ЛУЧ

Зашифрованный текст: НССУЖЛРГХРЮМОЦЪ

**Шифр «Скитала»**

Известно, что в Древней Греции, относящийся к V в. до н. э., во время войн для передачи военных донесений использовалось одно из первых шифровальных приспособлений — «Скитала» (рис.4). «Скитала» представляла собой цилиндрический жезл, на который без нахлестов и разрывов наматывалась узкая полоска папируса или пергамента. Кроме жезла могли использоваться любые другие цилиндрические предметы, например, рукоятки мечей, кинжалов, копий и т.д. Текст записывался построчно вдоль оси «Скиталы», а затем лента снималась с жезла. В результате получались беспорядочно написанные буквы, то есть своего рода шифр перестановки. Дешифровка выполнялась с использованием палочки такого же диаметра. [3]

Для расшифровки адресат использовал палочку такого же диаметра, на которую он наматывал бумагу, чтобы прочитать сообщение. Преимущество шифра скитала состоит в простоте и отсутствии ошибок — очень важное качество на поле боя. Однако такой шифр может быть легко взломан. Например, метод взлома скиталы был предложен ещё Аристотелем. Метод состоит в том, что не зная точного диаметра палочки, можно использовать конус, имеющий переменный диаметр и перемещать бумагу с сообщением по его длине до тех пор, пока текст не начнёт читаться — таким образом, дешифруется диаметр скиталы.

Рис.4

Достоинства - простота и отсутствие ошибок.

Недостатки - легко взламывается.

**Диск Энея.**

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

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

Рис.5.

Достоинства - легок в применении, расшифровка для злоумышленника — задача практически невыполнимая, зашифрованный текст не попадает под подозрение.

Недостатки - метод является медленным и требует наличия литературных навыков. Любой шифровальный аппарат может быть утерян, украден или конфискован.

**Шифр «Квадрат Полибия».**

Греческий писатель Полибий использовал систему сигнализации, которая была широко принята как метод шифрования. Он записывал буквы алфавита в квадратную таблицу и заменял их парой чисел, которые указывали соответственно на номер строки и номер столбца, на пересечении которых находилась зашифровываемая буква. Для латинского языка Полибий использовал квадратную таблицу размером 5х5 (буквы i и j считались сходными и заменялись на одно и то же значение) (рис.6). Для кириллицы квадрат Полибия мог бы иметь размер 6х6 (рис.7).

Рис.6 Рис.7.

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

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

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

В нашей стране принцип использования таблицы Полибия нашел широкое применение в 19 веке в среде революционеров, находящихся в тюремном заключении. Революционерами использовались различные наборы алфавитов (то есть опускалось различное число редко встречающихся букв русского языка) и различные размеры таблиц для перестукивания друг с другом через стены камер. Такие системы получили название «тюремных шифров». [3]

ПРИМЕР:

Исходный текст: ПЛОЩАДЬ ПРЯМОУГОЛЬНИКА

Зашифрованный текст: 35 31 34 53 11 15 56 35 36 63 32 34 43 14 34 31 56 33 24 26 11

**Диск Альберти.**

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

«Диск Альберти» представлял собой пару дисков. Первый диск большего диаметра был неподвижным. Второй диск меньшего диаметра был соотнесен с первым и вращался в любом направлении. Оба диска были разделены на 24 сектора. В сектора большого диска вписывались 20 букв латинского алфавита (Альберти исключил буквы h, j, k, u, w, y) и четыре цифры от 1 до 4. В меньший диск были вписаны все буквы латинского алфавита, но не по порядку, а вперемешку (рис.8).

Рис.8.

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

**Шифр «Пляшущие человечки».**

В 1903 год Конан Дойл написал рассказ «Пляшущие человечки», вошедший в сборник из 13 рассказов «Возвращение Шерлока Холмса». [4]

В этом рассказе Мистер Хилтон Кьюбит нашел записку с изображением пляшущих человечков. Мистер Кьюбит никак не мог понять, что же это значит, а Шерлок Холмс разгадал этот шифр и понял, что записка предназначалась жене мистера Кьюбита – Элизабет Паркер.

Каждый человечек соответствует одной букве алфавита.

В тексте, у некоторых человечков есть флажки. Они разделяют текст на слова.

Преимущество у шифра пляшущих человечков только одно — благодаря стеганографическим свойствам при небольшой длине шифровки может, написан где угодно — на заборе, столбе, асфальте и сойдет за детские рисунки. Что касается недостатков, то их у шифра пляшущих человечков полный набор — будучи симметричным шифром простой замены, он не обеспечивает достаточной конфиденциальности.

**Современная криптография.**

На сегодняшний день, криптография занимает в жизни каждого человека важное место. Любой человек хотя бы раз в день сталкивается с шифрованием данных. Всё большее и большее количество информации передаётся по тем каналам связи, которые требуют особой защищённости данных.

Современная криптография полностью основана на математике. Основная задача, которую преследует математика в криптографии – это криптографическая стойкость, то есть способность противостоять теоретическому и практическому взлому. [6]

Практическое применение криптографии стало неотъемлемой частью жизни современного общества - её используют в электронной коммерции, электронный документооборот (включая электронные подписи), телекоммуникации и других областях. Очень быстро после распространения компьютеров в деловой сфере практическая криптография сделала в своём развитии огромный скачок.

Современный период развития криптографии (с конца 70-х годов по настоящее время) отличается зарождением и развитием нового направления - это криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами.

В наш век все увеличивающегося потока обмена информацией, к которой относится все больше и больше информации о нашей повседневной жизни (цифровизация всего и вся, начиная от дневника и медицинской

карты, и заканчивая финансовыми операциями на рынках ценных бумаг), устойчивое и надёжное шифрование является не просто необходимым, а жизненно важным условием безопасности.

В качестве простых примеров можно привести: обмен сообщениями в

корпоративной почте крупных компаний; переписка в различных интернет мессенджерах (telegram, whatsapp и пр.); эл. дневник ученика; ЕГЭ, врачебная информация; вообще любая информация о персональных данных. Даже обычное управление электронными приборами дома (так называемый умный дом) должно осуществляться по шифрованным каналам данных во избежание вмешательства в их работу злоумышленников. Сейчас коммунальные услуги и все, что связано с ЖКХ, активно уходит в цифровой мир, обмен данными в системе также должно быть безопасным от вмешательства извне, и шифрование - как раз метод, позволяющий этого

достичь. [7]

Сейчас любая передача данных должна быть шифрованной, если она не предназначается широкому кругу лиц (публичная информация).

Шифрование публичным ключом.

Алгоритм шифрования, применяющийся сегодня в различных модификациях буквально во всех компьютерных системах. Есть два ключа: открытый и секретный. Открытый ключ — это некое очень большое число, имеющее только два делителя, помимо единицы и самого себя. Эти два делителя являются секретным ключом, и при перемножении дают публичный ключ. Например, публичный ключ — это 1961, а секретный — 37 и 53. Открытый ключ используется для того, чтобы зашифровать сообщение, а секретный — чтобы расшифровать. Без секретного ключа расшифровать сообщение невозможно. Когда вы отправляете свои личные данные, допустим, банку, или ваша банковская карточка считывается банкоматом, то все данные шифруются открытым ключом, а расшифровать их может только банк с соответствующим секретным ключом. Суть в том, что математически очень трудно найти делители очень большого числа.