Тип работы: Глава диплома

Предмет: Педагогика

-

Введение

Криптографию можно назвать математическим искусством, однако, сталкиваясь с ней ежедневно при использовании гаджетов и компьютеров, люди порой даже не догадываются о настолько интересном и специфичном предмете. Для того, чтобы лучше понять предмет криптографии обратимся к истории ее возникновения и развития.
История криптографии насчитывает более 4 тысяч лет. Казалось бы, проблема защиты информации обострилась лишь в 20-ом веке, когда в мире появились первые ЭВМ, когда был изобретён персональный компьютер, когда человечество получило доступ к важнейшей технологии – к сети Интернет. Но на самом деле, криптография в том или ином виде уже давным-давно сопровождает человечество.
Для начала, что же такое криптография? Некоторые источники говорят о том, что криптография – это наука. Изучая различные словари, мы пришли к выводу, что необходимо разделять понятия «криптография» и «криптология». Криптология - наука, исследующая криптографические преобразования. В криптологии различают направления: криптографию и криптоанализ. Иными словами, криптография, несмотря на то, что это очень обширная тема для обсуждений, является лишь частью науки под названием криптология. Так всё же, что такое криптография? Криптография - отрасль знаний, изучающая принципы, средства и методы преобразования данных с целью сокрытия их информационного содержания, предотвращения их не обнаружимой модификации и/или несанкционированного использования.
Для того, чтобы снизить порог вхождения, необходимо описать ещё несколько терминов, которые будут использоваться в данной статье.
Наукой не установлен точный исторический период, когда появилась криптография, каковы были ее первоначальные формы и кто был ее создателем. Так, американский криптограф Л.Д. Смит утверждает, что криптография существовала даже в те времена, когда в Гизе не возвышались Великие Пирамиды. Однако, другой американец, Флетчер Пратт, в своей книге утверждает, что криптография – это «искусство шифрования — это процесс выражения слов, передающих смысл только немногим лицам, которым известен этот секрет». Согласно этому определению, криптография могла возникнуть, как только человечество достигло определенного уровня цивилизации. В любом случае, криптография – одна и древнейших отраслей знаний.
В качестве доказательства вышесказанному, надо отметить, что в исторических документах таких государств, как Египет, Индия, Месопотамия фигурируют различные системы и способы составления шифрованного письма. Возьмём Индию. В древнеиндийских рукописях приводится более 60 методов письма, некоторые из них с уверенностью можно назвать криптографическими, т.е. обеспечивающие секретность переписки. Был метод, суть которого заключалась в замене гласных букв на согласные и наоборот.
В Месопотамии одним из самых старых зашифрованных текстов является клинопись, содержащая рецепт изготовления глазури для гончарных изделий. Автор, стремясь не допустить раскрытия столь важного рецепта, использовал редко употребляемые символы знаки, некоторые же он просто игнорировал. Кроме этого, вместо имён использовались цифры.
Криптография уже в древности широко использовалась и в Древнем Египте. Так, в стране шифровались религиозные тексты и медицинские рецепты.
А в Древней Греции криптография уже тогда была очень хорошо развита. Так, в Спарте для шифрования текста был разработан прибор, получивший название «Сцитала». Устройство состояло из двух цилиндров одинакового размера. Для того, чтобы обе стороны могли понимать друг друга, каждой стороне выдавался один из цилиндров.
Шифровался текст следующим образом: отправитель наматывал на цилиндр узкую полоску пергамента; текст, который необходимо передать, выписывали на ленту вдоль цилиндра, затем ленту смывали и

отправляли корреспонденту. Последний, обернув лентой свой цилиндр, расшифровывал сообщение. Секретность переписки обеспечивал диаметр цилиндра. Кроме того, вместо цилиндров применялись рукоятки кинжалов, мечей и др. Данная система примечательна ещё тем, что был изобретён метод дешифровки данного шифра, приписываемый Аристотелю. Использовался длинный конус. Он оборачивался у основания полоской перехваченного пергамента. Далее, пергамент сдвигался к вершине конуса. Там, где диаметр конуса совпадал с диаметром «Сциталы», буквы на пергаменте сочетались в слоги и слова.
Можно сделать вывод, что вместе с криптографией возник и криптоанализ - наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа (термин был предложен американским криптографом Уильямом Ф. Фридманом в 1920 году).
Другим известным изобретением является «линейка Энея». Эней Тактик очень серьёзно изучал тему шифрования информации. До т.н. «линейки» был изобретён «диск Энея», который, на самом деле, нельзя считать настоящим криптографическим инструментом, поскольку дешифровка сообщений была довольно простой – сообщение передавалось вместе с диском. Достаточно было украсть диск, чтобы завладеть информацией.
Тогда на смену диску пришла «линейка Эдея». Данный инструмент передачи сообщений оказался более эффективным, чем диск, так как главная особенность «линейки» - её не надо было переносить вместе с текстом. Линейки были только у отправителя и получателя. Гонцы получали нить со завязанными в необходимых местах узлами. Понять смысл сообщения можно было только соотнеся узлы к буквам, нарисованным на линейке. Поэтому, потеря или воровство катушки с ниткой имели не такие критичные последствия для отправителя и получателя. Таким образом, «линейка Эдея» стала первым настоящим не взламываемым криптографическим инструментом.
Средневековая криптография. С VIII века н.э. вклад в криптографию вносили, в основном, арабы. Халиль аль-Фарахиди, арабский филолог, предположил, что некоторые стандартные фразы, которые используются в письмах, можно использовать для дешифрования остального текста. Например, первыми словами на греческом языке византийскому императору наверняка будут «Во имя Аллаха». Зная это, можно расшифровать оставшийся текст. Позднее, филолог написал книгу, где подробно описал этод метод – «Китаб аль-Маумма», на русском – «Книга тайного языка».
Другой представитель региона, учёный Абу Бакр Ахмед бен-Али бен-Вахшия ан-Набати, написал книгу «Книга о большом стремлении человека разгадать загадки древней письменности», в которой приводятся описания различных шифров, в т.ч. с применением нескольких алфавитов. Более того, арабы внесли вклад и в криптоанализ. Так, в «Манускрипте о дешифровке криптографических сообщений» был впервые упомянут частотный криптоанализ.
В 1412 году выходит книга Шехаба Калкашанди – «Энциклопедия всех наук». Сама по себе энциклопедия включала в себя 14 томов. Несмотря на то, что в книге было описано очень много фактов о различных способах шифрования информации, книга была известна первым в истории описания криптоанализа на основе частоты появления знаков в исходном и шифрованном тексте. Более того, в книге была таблица с указанием частоты встречаемости символов в текстах Корана.
В Древней Руси использовалась литорея – свой способ шифрования. Было два варианта шифрования – простой и мудрый.
В Византии использовались различные методы шифрования, но большинство из них ориентировано на безграмотность людей. Например, текст, написанный на другом языке, являлся слабым, но шифром.
Криптография эпохи возрождения. В Италии был изобретён «диск Альберти», названный так в часть его создателя, Леона Баттисты Альберти, учёного, гуманиста, писателя (рисунок 2).
Ключевой вехой в развитии криптографии является фундаментальный труд Клода Шеннона «Теория связи в секретных системах». В этой работе, по мнению многих современных криптографов, был впервые показан подход к криптографии в целом как к математической науке. Были сформулированы её теоретические основы и введены основные понятия.
В 1960-х годах начали появляться различные блочные шифры, которые обладали большей криптостойкостью по сравнению с результатом работы роторных машин. Однако они предполагали обязательное использование цифровых электронных устройств — ручные или полумеханические способы шифрования уже не использовались.
Классическая криптография использовала симметричные алгоритмы шифрования. Шифрование и дешифрование отличаются в таких алгоритмах только порядком выполнения операций. Алгоритмы всегда используют один и тот же секретный элемент - закрытый ключ. Каждый из участников обмена, зная ключ, может как зашифровать, так и расшифровать сообщение.

Криптография – очень важная область знаний, изучению и совершенствованию которой многие учёные посвящают всю свою карьеру. С недавних пор криптографию вводят в школьный курс изучения математики, ежегодно при крупных ВУЗах России проводятся очные и заочные олимпиады, позволяющие школьникам получить не только дополнительные знания, но и понять с чем в будущем они смогут связать свою профессиональную деятельность.
Таким образом, актуальность данной работы приобретает все более ярко выраженный характер, а именно: развитие криптографии, то есть шифрование, данных происходит весьма высокими темпами, поэтому подготовка школьников к участию в олимпиадах, подготовка самих олимпиад приобретает уже стратегическое значение в подготовке кадров.

Список литературы

1. Астахова, Л.В. Защита облачной базы персональных данных с использованием гомоморфного шифрования / Л.В. Астахова, Д.Р. Султанов, Н.А. Ашихмин // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016 г. – Т. 16, № 3. – С. 52–61.
2. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. — СПб : НИУ ИТМО, 2012 г. — 142 с.
3. Комиссаренко В.В. Современные тенденции развития средств и методов криптографической защиты информации. В кн.: 2-я конф-ия. «Технологии защиты информации и информационная безопасность организаций», г. Минск, 2016 г.
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – Москва: ДМК Пресс, 2012 г. – 593 с.
5. Ященко В.В. Введение в криптографию. – Издание 4 дополненное – МЦНМО: Москва, 2012 г.
6. Актуальные направления и нерешённые проблемы криптографии. [Электронный ресурс]. Под свободной редакцией – Режим доступа: http://cryptowiki.net (30.15.2018 г.)
7. Жуков А.Е. Легковесная криптография. Часть 1. [Электронный ресурс]: Вопросы кибербезопасности №1 – Москва: АО НПО «Эшелон», 2015 г. – Режим доступа: https://cyberleninka.ru/article/n/legkovesnaya-kriptografiya-chast-1 (04.06.2018 г.)
8. Рябко Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс]: монография / Б.Я. Рябко, А.Н. Фионов – Электрон. дан. – Москва: Горячая линия – Телеком, 2011 г. – 232 с. – Режим доступа: https://e.lanbook.com/book/5192 (07.06.2018 г.)