МИНИСТЕРСТВО ОБРАЗОВАНИЯ, КУЛЬТУРЫ И ИССЛЕДОВАНИЙ

БЕЛЬЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ «АЛЕКУ РУССО»

ФАКУЛЬТЕТ РЕАЛЬНЫХ НАУК, ЭКОНОМИКИ И ОКРУЖАЮЩЕЙ СРЕДЫ

КАФЕДРА МАТЕМАТИКИ И ИНФОРМАТИКИ

КРИПТОГРАФИЯ И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

РЕФЕРАТ

Автор:

студент группы IS 11Z,

Анна НАГИРНЯК

_____

(подпись)

Научный Руководитель:

Олеся Владимировна СКУТНИЦКИ

_____

(подпись)

Дмитрий Дмитриевич СТОЯН

_____

(подпись)

Бельцы, 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном обществе все большую роль играют компьютеры, и вообще электронные средства передачи, хранения, и обработки информации.

Для того чтобы информационные технологии можно было использовать в различных областях, необходимо обеспечить их надежность и безопасность. Под безопасностью (в широком смысле) понимается способность информационной системы сохранять свою целостность и работоспособность при случайных или преднамеренных внешних воздействиях. Поэтому широкое использование информационных технологий привело к бурному развитию различных методов защиты информации, из которых основными можно, пожалуй, назвать, помехоустойчивое кодирование и криптографию.

В течение многих лет криптография служила исключительно военным целям. Сегодня обычные пользователи получают возможность обращаться к средствам, позволяющим им обезопасить себя от несанкционированного доступа к конфиденциальной информации, применяя методы компьютерной криптографии.

1. ИСТОРИЯ КРИПТОГРАФИИ

С распространением письменности в человеческом обществе появилась потребность в обмене письмами и сообщениями, что вызвало необходимость сокрытия содержимого письменных сообщений от посторонних. Методы сокрытия содержимого письменных сообщений можно разделить на три группы. К первой группе относятся методы маскировки или ***стеганографии***, которые осуществляют сокрытие самого факта наличия сообщения; вторую группу составляют различные методы тайнописи или ***криптографии*** (от греческих слов ***ktyptos*** – тайный и ***grapho*** – пишу); методы третьей группы ориентированы на создание специальных технических устройств, засекречивания информации [6].

История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была своеобразной криптографической системой, так как в древних обществах ею владели только избранные.

Развитию тайнописи способствовали войны. Письменные приказы и донесения обязательно шифровались, чтобы пленение курьеров не позволило противнику получить важную информацию. Например, римский император Цезарь пользовался в своей военной и личной переписке шифром, сущность которого состояла в замене каждой буквы латинского языка на следующую букву алфавита. Тогда знаменитая фраза: «***VENI***, ***VIDI***, ***VICI***» («Пришел, увидел, победил»), которой Цезарь, известил одного из своих друзей в Риме о быстро одержанной им победе, в зашифрованном виде будет иметь следующий вид: «***XFOJ***, ***XJEJ***, ***XJDJ***» [5].

Практически одновременно с криптографией стал развиваться и криптоанализ – наука о раскрытии шифров (ключей) по шифртексту.

В истории криптографии условно можно выделить четыре этапа: наивный, формальный, научный; компьютерный [5].

Для ***наивной криптографии*** (до начала XVI в.) характерно использование любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов. На начальном этапе для защиты информации использовались методы кодирования и стеганографии, которые родственны, но не тождественны криптографии [1].

Большинство из используемых шифров сводились к перестановке или моноалфавитной подстановке. Одним из первых зафиксированных примеров является шифр Цезаря, состоящий в замене каждой буквы исходного текста на другую, отстоящую от нее в алфавите на определенное число позиций. Другой шифр, полибианский квадрат, авторство которого приписывается греческому писателю Полибию, является общей моноалфавитной подстановкой, которая проводится с помощью случайно заполненной алфавитом квадратной

таблицей (для греческого алфавита размер составляет 5×5). Каждая буква исходного текста заменяется на букву, стоящую в квадрате снизу от нее [6].

Этап ***формальной криптографии*** (конец XV – начало XX вв.) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации. Важная роль на этом этапе принадлежит Леону Батисте Альберти, итальянскому архитектору, который одним из первых предложил многоалфавитную подстановку. Данный шифр, получивший имя дипломата XVI в. Блеза Вижинера, состоял в последовательном «сложении» букв исходного текста с ключом (процедуру можно облегчить с помощью специальной таблицы). Его работа «Трактат о шифре» (1466 г.) считается первой научной работой по криптологии.

Одной из первых печатных работ, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования, является труд «Полиграфия» (1508 г.) немецкого аббата Иоганна Трисемуса. Ему принадлежат два небольших, но важных открытия: способ заполнения полибианского квадрата (первые позиции заполняются с помощью легко запоминаемого ключевого слова, остальные – оставшимися буквами алфавита) и шифрование пар букв (биграмм).

Простым, но стойким способом многоалфавитной замены (подстановки биграмм) является шифр Плейфера, который был открыт в начале XIX в. Чарльзом Уитстоном. Уитстону принадлежит и важное усовершенствование – шифрование «двойным квадратом». Шифры Плейфера и Уитстона использовались вплоть до первой мировой войны, так как с трудом поддавались ручному криптоанализу [4].

В XIX в. голландец Керкхофф сформулировал главное требование к криптографическим системам, которое остается актуальным и поныне: секретность шифров должна быть основана на секретности ключа, но не алгоритма. Наконец, последним словом в донаучной криптографии, которое обеспечило еще более высокую криптостойкость, а также позволило автоматизировать (в смысле механизировать) процесс шифрования стали роторные криптосистемы.

Одной из первых подобных систем стала изобретенная в 1790 г. Томасом Джефферсоном, будущим президентом США, механическая машина. Многоалфавитная подстановка с помощью роторной машины реализуется вариацией взаимного положения вращающихся роторов, каждый из которых осуществляет «прошитую» в нем подстановку.

Практическое распространение роторные машины получили только в начале XX в. Одной из первых практически используемых машин, стала немецкая Enigma, разработанная в 1917 г. Эдвардом Хеберном и усовершенствованная Артуром Кирхом. Роторные машины

активно использовались во время второй мировой войны. Помимо немецкой машины Enigma использовались также устройства Sigaba (США), Typex (Великобритания), Red, Orange и Purple (Япония). Роторные системы – вершина формальной криптографии, так как относительно просто реализовывали очень стойкие шифры. Успешные криптоатаки на роторные системы стали возможны только с появлением ЭВМ в начале 40-х гг.

Главная отличительная черта ***научной криптографии*** (1930 – 60-е гг.) – появление криптосистем со строгим математическим обоснованием криптостойкости. К началу 30-х гг. окончательно сформировались разделы математики, являющиеся научной основой криптологии: теория вероятностей и математическая статистика, общая алгебра, теория чисел, начали активно развиваться теория алгоритмов, теория информации, кибернетика. Своеобразным водоразделом стала работа Клода Шеннона «Теория связи в секретных системах» (1949), которая подвела научную базу под криптографию и криптоанализ. С этого времени стали говорить о ***криптологии*** (от греческого ***kryptos*** – тайный и ***logos*** – сообщение) – науке о преобразовании информации для обеспечения ее секретности. Этап развития криптографии и криптоанализа до 1949 г. стали называть донаучной криптологией. Шеннон ввел понятия «рассеивание» и «перемешивание», обосновал возможность создания сколь угодно стойких криптосистем [7].

В 1960-х гг. ведущие криптографические школы подошли к созданию блочных шифров, еще более стойких по сравнению с роторными криптосистемами, однако допускающих практическую реализацию только в виде цифровых электронных устройств.

Компьютерная криптография (с 1970-х гг.) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем «ручные» и «механические» шифры.

2. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Защита данных с помощью шифрования – одно из возможных решений проблемы безопасности. Зашифрованные данные становятся доступными только тем, кто знает, как их расшифровать, и поэтому похищение зашифрованных данных абсолютно бессмысленно для несанкционированных пользователей.

Наукой, изучающей математические методы защиты информации путем ее преобразования, является ***криптология***. Криптология разделяется на два направления – криптографию и криптоанализ

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Под ***конфиденциальностью*** понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в подлинности авторства и целостности.

Криптоанализ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей [3].

Существует ряд смежных, но не входящих в криптологию отраслей знания. Так обеспечением скрытности информации в информационных массивах занимается стеганография. Обеспечение целостности информации в условиях случайного воздействия находится в ведении теории помехоустойчивого кодирования. Наконец, смежной областью по отношению к криптологии являются математические методы сжатия информации.

Современная криптография включает в себя четыре крупных раздела: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами [1].

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений,хранение информации (документов, баз данных) на носителях в зашифрованном виде.

В качестве информации, подлежащей шифрованию и расшифрованию, а также электронной подписи будут рассматриваться тексты (сообщения), построенные на некотором алфавите. Под этими терминами понимается следующее.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст(сообщение) – упорядоченный набор из элементов алфавита. В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие:

- алфавит Z_{33} – 32 буквы русского алфавита (исключая «ё») и пробел;

- алфавит Z_{256} – символы, входящие в стандартные коды ASCII(American Standard Code for Information Interchange) и КОИ-8 (Код Обмена Информацией, 8 бит);
- двоичный алфавит – $Z_2 = \{0, 1\}$;
- восьмеричный или шестнадцатеричный алфавит.

Коды и шифры использовались задолго до появления ЭВМ (Электронно-Вычислительная Машина). С теоретической точки зрения не существует четкого различия между кодами и шифрами. Однако в современной практике различие между ними является достаточно четким. Коды оперируют лингвистическими элементами, разделяя шифруемый текст на такие смысловые элементы, как слова и слоги. В шифре всегда различают два элемента: алгоритм и ключ.

Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Определим ряд терминов, используемых в криптологии

Под шифром понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования.

Шифр – это совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей: $\{Fk : X \rightarrow S, K \in K\}$.

Криптографическая система, или ***шифр*** представляет собой семейство T обратимых преобразований открытого текста в шифрованный. Членам этого семейства можно взаимно однозначно сопоставить число k, называемое ключом. Преобразование T_k определяется соответствующим алгоритмом и значением ключа k.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованному.

Пространство ключей K – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита. Следует отличать понятия «ключ» и «пароль». Пароль также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

Криптосистемы подразделяются на симметричные и асимметричные [или с открытым (публичным) ключом].

В симметричных криптосистемах для зашифрования и для расшифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа открытый (публичный) и закрытый (секретный), которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины распределение ключей и управление ключами относятся к процессам системы обработки информации, содержанием которых является выработка и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Зашифрованием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а расшифрованием данных – процесс преобразования закрытых данных в открытые с помощью шифра. Вместо термина «открытые данные» часто употребляются термины «открытый текст» и «исходный текст», а вместо «зашифрованные данные» – «шифрованный текст».

Дешифрованием называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.

Шифрованием называется процесс зашифрования или расшифрования данных. Также термин шифрование используется как синоним зашифрования. Однако неверно в качестве синонима шифрования использовать термин «кодирование» (а вместо «шифра» – «код»), так как под кодированием обычно понимают представление информации в виде знаков (букв алфавита).

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования открытых данных и расшифрования зашифрованных данных.

Имитозащита – защита от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовстав- ка, представляющая собой

последовательность данных фиксированной длины, полученную по определенному правилу из открытых данных и ключа.

Криптографическая защита – это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием и (или) выработкой имитовставки.

Синхропосылка – исходные открытые параметры алгоритма криптографического преобразования.

Уравнение зашифрования (расшифрования)– соотношение, описывающее процесс образования зашифрованных (открытых) данных из открытых (зашифрованных) данных в результате преобразований, заданных алгоритмом криптографического преобразования [3].

3. ШИФРОВАЛЬНАЯ МАШИНА «ENIGMA». ПРИНЦИП ДЕЙСТВИЯ И БИТВА ЗА ШИФРЫ

«Enigma» (в русской транскрипции ***«Энигма»)*** в переводе с древнегреческого означает «безымянный», «неназванный», «загадочный» (Рис. 1). Работы по применению шифровальной машины с подобным названием начались в Германии в глубокой тайне в 1928 году и активизировались с приходом к власти Гитлера. Работами руководил непосредственно германский Генеральный штаб. К началу Второй мировой войны работы по созданию военного варианта «Enigma» были закончены, машина прошла испытания и была принята на вооружение [5].

Рис. 1. Внешний вид шифровальной машины «Энигма».

«Enigma» относилась к классу электромеханических шифровальных машин. Ее конструкция была основана на системе из трех вращающихся барабанов, осуществлявших замену 26 букв латинского алфавита. Каждый барабан имел 26 входных контактов на одной стороне и столько же выходных контактов — на другой. Внутри каждого барабана проходили провода, связывавшие входные и выходные контакты между собой. Выходные контакты первого барабана соединялись с входными контактами второго. Когда оператор нажимал на какую-либо букву на клавиатуре машины, электрический ток подавался на входной контакт первого барабана, соответствующий этой букве. Ток проходил через первый барабан и поступал на выходной контакт, соответствующий какой-либо другой букве. Затем ток проходил последовательно через второй и третий барабаны и подавался на неподвижный рефлектор (от лат. ***reflecto*** — обращаю назад, отражаю). В конструкции рефлектора 26 контактов разбивались на пары, контакты внутри каждой пары были соединены между собой. Таким образом, рефлектор заменял букву на парную ей [5].

Ток, прошедший через рефлектор, подавался назад, на систему барабанов. Он вновь проходил через три барабана, но в обратном порядке. В конце концов на световом табло машины загоралась одна из 26 лампочек, соответствовавшая зашифрованной букве.

Самым важным свойством машины «Enigma» являлось вращение барабанов. Первый барабан после каждого преобразования буквы поворачивался на одну позицию. Второй барабан поворачивался на одну позицию после того, как первый совершал полный оборот, т. е. после преобразования 26 букв. Наконец, третий барабан поворачивался на одну позицию после того, как второй совершал полный оборот, т. е. после шифрования 676 букв [5].

Благодаря рефлектору «Enigma» на каждом шаге осуществляла перестановку букв внутри пар, и если, к примеру, буква ***N*** заменялась на ***S***, то при том же положении роторов буква ***S*** менялась на ***N*** (ток шел по тем же проводам, но в другую сторону). Этим объяснялась особенность машины: для расшифровки сообщения достаточно было вновь пропустить его через машину, восстановив предварительно изначальное положение барабанов. Таким образом, начальное положение барабанов играло роль ключа шифрования. Это начальное положение устанавливалось в соответствии с текущей датой. Каждый оператор имел специальную книгу, задававшую положение барабанов для каждого дня. В целом получилась компактная, быстродействующая шифровальная машина, достаточно устойчивая к попыткам взлома применяемого шифра.

Очевидная слабость данной системы шифрования заключалась в том, что противнику достаточно было завладеть специальной книгой, задающей ключи шифрования, и самой машиной, чтобы дешифровать многие сообщения.

Немцам, несмотря на колоссальные усилия, не удалось сохранить в тайне работу над «Энигмой». Уже в 1932 году в специально созданном «Шифровальном бюро» в Варшаве начались работы над раскрытием тайны «Энигмы». Возглавлял группу молодой польский математик Мариан Ршевский, выпускник математического факультета университета в Познани. Группа имела в своем распоряжении устаревшую коммерческую шифровальную машину, купленную в Германии. Конечно, эта модель была очень далека от современных для той поры немецких военных шифровальных машин и принесла мало пользы. Поэтому главным моментом в работе ученых для решения задачи «Энигмы» было применение математики (теории групп и теории перестановок). Для раскрытия шифров «Энигмы» польские математики использовали перехваченные шифрованные сообщения и добились значительных успехов. Ими было теоретически воссоздано устройство машины, что позволило позже создать её реальную модель; были разработаны также методы восстановления ключей к шифрам на основе перехваченных сообщений.

Позднее, в 1939 году, перед началом войны все материалы по «Энигме» были поляками переданы во Францию и Англию. Англичане продолжили работы, раскрыв усовершенствования, которые были внесены в конструкцию последних немецких машин и систему кодов, используемую Германией. В этой работе, выполнявшейся большой группой

ученых в местечке Блетчли в 70 км от Лондона, участвовал знаменитый математик Алан Тьюринг, широко известный как автор виртуальной «машины Тьюринга». Благодаря, главным образом, усилиям возглавляемой им группы были созданы механические вычислительные устройства, полным перебором отыскивавшие ключи к шифру на много порядков быстрее, чем это можно было сделать вручную. Подобное механическое устройство, но с возможностью его «программирования» с помощью бумажной перфоленты, созданное специально для дешифровки перехваченных сообщений «Энигмы» и названное «Colossus», некоторые исследователи считают первым в мире по-настоящему программируемым компьютером.

Математикам из Блетчли часто удавалось находить блестящие и в то же время простые решения, во много раз сокращавшие время вскрытия шифровок «Энигмы». Но их оригинальные идеи, в част-ности по организации «распределенных вычислений», приходилось воплощать по преимуществу с помощью карандаша и листа бумаги, что значительно затягивало время дешифровки перехваченных сообщений.

Наконец, осенью 1942 года, в результате спецоперации ВМС (Военно - Морские Силы) Англии, на германской подводной лодке U-571, которую немецкое командование считало затонувшей, была захвачена сама шифровальная машина «Enigma» и процесс дешифровки немецких секретных сообщений был поставлен англичанами на поток.

Вся эта работа по взламыванию немецких секретных шифров сохранялась в глубокой тайне, и немцы до самого конца войны даже не подозревали, что все их секретные сообщения становятся известны антигитлеровской коалиции. О том, какое значение придавало английское командование сохранению в секрете факта взлома немецких секретных шифров, говорит тот факт, что У. Черчилль никак не воспользовался знанием о предстоящем налете немецкой авиации на город Ковентри, сообщения о котором были перехвачены и заблаговременно расшифрованы англичанами. В результате город был подвергнут сильнейшей бомбардировке немецкой авиации, однако англичане сохранили в тайне свои возможности по дешифровке немецких секретных сообщений.

Многие историки, изучающие Вторую мировую войну, убеждены, что взлом англичанами секретных шифров значительно ускорил падение фашистской Германии и сохранил тысячи жизней.

История «Энигмы» держалась в глубокой тайне и после окончания войны; она была опубликована только 30 лет спустя, по истечении срока давности военных секретов.

Так закончилась одна из самых замечательных историй «докомпьютерной» криптографии. Вскоре после войны начался новый этап развития этой древнейшей науки. За дело взялись теоретики — математики и вычислители, вооруженные компьютером [5].

4. ЭЛЕКТРОННАЯ ПОДПИСЬ

С развитием электронной почты с компьютера на компьютер стало поступать огромное количество посланий самого разного свойства. Среди личных посланий, поздравлений, рекламных проспектов и прочего в электронной почте стали попадаться и документы. А обычные строки текста превращаются в документ, когда под ними появляется подпись. К этому нас приучил многовековой опыт «бумажного» обращения с текстами.

Более того, даже один и тот же текст может иметь совершенно разный смысл в зависимости от того, кто его подписал. Одно дело, если текст подписал министр, и совсем другое дело, если тот же самый текст подписал третий секретарь четвертого отдела министерства. Однако если имеется подпись, то имеется и проблема борьбы с ее подделкой. И переход к электронным документам эту проблему только обострил. Поскольку, например, передача по сети сканированного документа, снабженного ручной подписью, проблемы подделки ни в коем случае не решает, а для любой мало-мальски серьезной экспертизы подлинности подписи требуется оригинал «бумажного» документа. Так возникла задача создания электронной цифровой подписи [7].

Электронной цифровой подписью (***ЭЦП***) называется реквизит электронного документа, появление которого в документе получателем подтверждает два факта: то, что документ дошел до получателя без искажений, и то, что он подписан именно отправителем.

В качестве примера рассмотрим протокол формирования ЭЦП, основанный на алгоритме RSA(Random Scheduling Algorithm). В обмене участвуют два абонента: отправитель ***A*** и получатель ***B***. Пусть ***A*** отправляет получателю ***B*** текст ***b*** и желает, чтобы это сообщение было снабжено ЭЦП.

a) ***A*** строит стандартную схему RSA (Random Scheduling Algorithm). Пусть ее открытый ключ (***m***, ***e***) и закрытый ключ (***m***, ***d***). Открытый ключ публикуется, закрытый остается известен только A.

b) ***A*** вычисляет с помощью известного только ему закрытого ключа число ***s*** по формуле

$$s = b^d \bmod m,$$

где ***b*** — отправляемый текст, и отправляет получателю ***B*** исходный текст ***b*** и полученное число ***s*** в качестве его ЭЦП.

c) Проверяющий ***B***, получив число ***s***, выбирает из публикации открытый ключ абонента ***A*** и вычисляет с его помощью число ***b′*** по формуле

$$b' = s\ e \bmod m.$$

Если при этом $b' = b$, то подпись правильна и это означает, что исходный текст принят без искажений и этот текст подписан действительно A. Если же $b' \neq b$, то это означает, что либо в исходный текст внесены изменения, либо он подписан не отправителем A, либо и то и другое вместе

Смысл указанного протокола в том, что абонент B, как и в случае протокола аутентификации, убеждается, что подпись s, полученная им вместе с исходным текстом b, вычислялась с использованием закрытого ключа (m, d), парного к открытому ключу отправителя. А такую операцию по определению мог проделать только сам отправительA, поскольку только он знает закрытый ключ. И при этом опять-таки получатель не приобретает никакой информации о самом закрытом ключе отправителя, т. е. и в этом протоколе вновь работает схема нулевого разглашения.

Схема ЭЦП имеет еще одно важнейшее свойство. Оно заключается в том, что данная конкретная подпись может относиться только к одному конкретному тексту. Действительно, если отправитель A попытается подобрать другой текст b' , так, чтобы он имел ту же подпись, что и исходный текст b, ему придется найти новый текст b' из уравнения

$$(b')^d \bmod m = b^d \bmod m.$$

А такое уравнение, по крайней мере в классе осмысленных текстов, может иметь только одно решение $b' = b$.

Это обстоятельство определяет важнейшее свойство ЭЦП — невозможность отправителя подменить подписанный им текст либо отказаться от подписи. Это свойство, иногда для краткости называемое неотказуемостью либо неотвергаемостью подписи, ставит в жесткие рамки отправителя сообщения, в то же время страхуя получателя от возможных последствий недобросовестности отправителя. С другой стороны, отправитель может быть уверен, что его ЭЦП никто не может подделать, поскольку закрытый ключ знает только он сам. Эти два обстоятельства делают тексты, подписанные с помощью ЭЦП, юридически значимыми. Они могут служить основой сделок, контрактов, могут приниматься в судах в качестве вещественных доказательств и вообще могут признаваться там, тогда и в той степени, где, когда и в какой степени могут признаваться обычные собственноручные личные подписи [3].

5. КРАТКИЕ СВЕДЕНИЯ О КРИПТОАНАЛИЗЕ

Знание некоторых положений криптоанализа необходимо для глубокого понимания криптографии.

Главным действующим лицом в криптоанализе выступает нарушитель (или криптоаналитик). Под ним понимают лицо (группу лиц), целью которых является прочтение или подделка защищенных криптографическими методами сообщений.

В отношении нарушителя принимается ряд допущений, которые, как правило, кладутся в основу математических или иных моделей:

1. Нарушитель знает алгоритм шифрования (или выработки Электронно – Цифровой Подписи) и особенности его реализации в конкретном случае, но не знает секретного ключа.
2. Нарушителю доступны все зашифрованные тексты. Нарушитель может иметь доступ к некоторым исходным текстам, для которых известны соответствующие им зашифрованные тексты.
3. Нарушитель имеет в своем распоряжении вычислительные, людские, временные и иные ресурсы, объем которых оправдан потенциальной ценностью информации, которая будет добыта в результате криптоанализа [4].

Попытку прочтения или подделки зашифрованного сообщения, вы- числения ключа методами криптоанализа называют криптоатакой или атакой на шифр. Удачную криптоатаку называют взломом.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа (т.е. криптоатаке). Показатель криптостойкости – главный параметр любой криптосистемы. В качестве показателя криптостойкости можно выбрать:

- количество всех возможных ключей или вероятность подбора ключа за заданное время с заданными ресурсами;
- количество операций или время (с заданными ресурсами), необходимое для взлома шифра с заданной вероятностью;
- стоимость вычисления ключевой информации или исходного текста.

Все эти показатели должны учитывать также уровень возможной криптоатаки.

Однако следует понимать, что эффективность защиты информации криптографическими методами зависит не только от криптостойкости шифра, но и от множества других факторов, включая вопросы реализации криптосистем в виде устройств или программ. При анализе криптостойкости шифра необходимо учитывать и человеческий

фактор. Например, подкуп конкретного человека, в руках которого сосредоточена необходимая информация, может стоить на несколько порядков дешевле, чем создание суперкомпьютера для взлома шифра.

Современный криптоанализ опирается на такие математические науки как теория вероятностей и математическая статистика, алгебра, теория чисел, теория алгоритмов и ряд других. Все методы криптоанализа в целом укладываются в четыре направления:

1. ***Статистический криптоанализ*** – исследует возможности взлома криптосистем на основе изучения статистических закономерностей исходных и зашифрованных сообщений. Его применение осложнено тем, что в реальных криптосистемах информация перед шифрованием подвергается сжатию (превращая исходный текст в случайную последовательность символов), или в случае гаммирования используются псевдослучайные последовательности большой длины.
2. ***Алгебраический криптоанализ*** – занимается поиском математически слабых звеньев криптоалгоритмов. Например, в 1997 г. в эллиптических системах был выявлен класс ключей, существенно упрощавший криптоанализ.
3. ***Дифференциальный*** (или ***разностный***) ***криптоанализ*** – основан на анализе зависимости изменения шифрованного текста от изменения исходного текста. Впервые использован Мерфи, улучшен Бихэмом и Шамиром для атаки на DES (Data Encryption Standard).
4. ***Линейный криптоанализ*** – метод, основанный на поиске линейной аппроксимации между исходным и шифрованным текстом. Предложенный Мацуи, также впервые был применен при взломе DES (Data Encryption Standard). Как и дифференциальный анализ в реальных криптосистемах может быть применен только для анализа отдельных блоков криптопреобразований [2].

Опыт взломов криптосистем (в частности, конкурсов, которые регулярно устраивает RSA Data Security) показывает, что главным методом остается «лобовая» атака – проба на ключ. Также, как показывает опыт криптосистемы, больше страдают от небрежности в реализации.

Принято различать несколько уровней криптоатаки в зависимости от объема информации, доступной криптоаналитику. Можно выделить три уровня криптоатаки по нарастанию сложности.

1. Атака по шифрованному тексту (***Уровень КА1***) – нарушителю доступны все или некоторые зашифрованные сообщения.

2. Атака по паре «исходный текст – шифрованный текст» (***Уровень КА2***) – нарушителю доступны все или некоторые зашифрованные сообщения и соответствующие им исходные сообщения.
3. Атака по выбранной паре «исходный текст – шифрованный текст» (***Уровень КА3***) – нарушитель имеет возможность выбирать исходный текст, получать для него шифрованный текст и на основе анализа зависимостей между ними вычислять ключ.

Все современные криптосистемы обладают достаточной стойкостью даже к атакам уровня КА3, т.е. когда нарушителю доступно по сути шифрующее устройство [7].

ВЫВОДЫ

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации.

Еще с древних времен криптография играла значимую роль в защите информации. На сегодняшний день без нее также не обходится ни одна передача информации. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.

Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности.

Из вышесказанного следует, что криптография была и будет актуальным феноменом при любой власти, времени и обстановке.

СПИСОК ЛИТЕРАТУРЫ

1. Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М. : Горячая линия – Телеком, 2001. – 120 с
2. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования информации. – М. : Госкомитет СССР по стандартам, 1989.
3. Криптографическая защита информации : учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с. – 100 экз. – ISBN 5-8265-0503-6.
4. Введение в криптографию / Под общ. ред. В. В. Ященко. СПб.: Питер, 2001.
5. Черчхаус Р. Коды и шифры, Юлий Цезарь, «Энигма» и Интернет. М.: Весь мир, 2005.
6. Криптография[online]. Доступно в интернете по адресу: https://ru.wikipedia.org/wiki/Криптография.
7. Музыкантский А. И., Фурин В. В. Лекции по криптографии. — М.: МЦНМО, 2013. — 2-е изд., стереотип. — 68 с.ISBN 978-5-4439-0086-5.