УДК 004.942

С. Умрзоков

Студент Машиностроительного факультета

Ташкентский государственный технический университет

Узбекистан, Ташкент

научный руководитель: Ганиева Т.И.

старший преподаватель

Ташкентский государственный технический университет

Узбекистан, Ташкент

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Аннотация: В криптографии большое внимание уделяется не только созданию и исследованию шифров, но и разработке криптографических протоколов. В статье рассматриваются особенности криптографии, криптографические алгоритмы, криптографические протоколы, политика безопасности, оценивание риска, перспективы развития криптографии на современном этапе

Ключевые слова: криптография, алгоритм, активная криптографическая атака, крипто анализ, крипто стойкость, пассивная криптографическая атака, символ, асимметричное шифрование, шифр система.

S. Umrzokov

Student of the Machine-building faculty

Tashkent State Technical University

Uzbekistan, Tashkent

supervisor: Ganieva T.I.

Senior Lecturer

Tashkent State Technical University

Uzbekistan, Tashkent

CRYPTOGRAPHIC PROTOCOLS

Abstract: In cryptography, much attention is paid not only to the creation and study of ciphers, but also to the development of cryptographic protocols. The article discusses the features of cryptography, cryptographic algorithms, cryptographic protocols, security policy, risk assessment, prospects for the development of cryptography at the present stage

Keywords: cryptography, algorithm, active cryptographic attack, crypto analysis, cryptographic strength, passive cryptographic attack, symbol, asymmetric encryption, encryption system.

В настоящее время криптография занимается поиском и исследованием математических методов преобразования информации. Параллельно развивается и совершенствуется крипто анализ – наука о преодолении криптографической защиты информации. Криптография решает такие задачи как:

– шифрование данных с целью защиты от несанкционированного доступа;

– проверка подлинности сообщений;

– проверка целостности передаваемых данных;

– обеспечение невозможности отказа.

В современной криптографии большое внимание уделяется разработке криптографических протоколов, то есть процедур или алгоритмов взаимодействия абонентов с использованием криптографических средств. Криптографические протоколы – сравнительно молодая отрасль криптографической науки. Эта область криптографии бурно развивается, и на настоящий момент имеется уже несколько десятков различных типов криптографических протоколов.

Криптографический протокол – это такая процедура взаимодействия двух или более абонентов с использованием криптографических средств, в результате которой абоненты достигают своей цели, а их противники - не

достигают. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах. Каждый криптографический протокол предназначен для решения определенной задачи и имеет следующие свойства:

– при выполнении протокола важен порядок действий;

– каждое действие должно выполняться в свою очередь и только по окончании предыдущего;

– протокол должен быть непротиворечивым;

– протокол должен быть полным, то есть для каждой возможной ситуации должно быть предусмотрено соответствующее действие.

Свойства протокола напоминают известные свойства алгоритма. Протокол – это и есть алгоритм действия нескольких сторон в определенной ситуации. В криптографических протоколах используются стандарты шифрования, представленные на (рис. 1).

Криптографические протоколы можно условно разделить на две группы:

прикладные протоколы

примитивные протоколы

Прикладной протокол решает конкретную задачу, которая на практике.

Примитивный протокол используется как своеобразные "строительные блоки" при разработке прикладных протоколов.

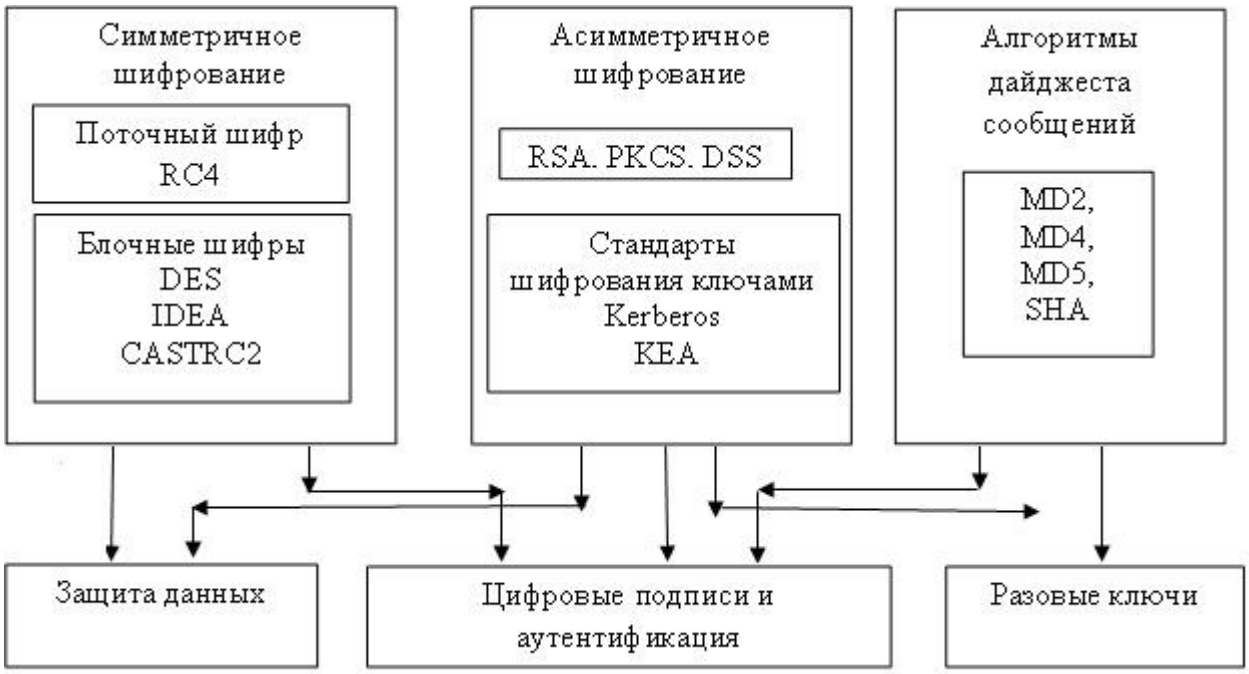

Рисунок 1 – Криптографические методы и шифры

Ниже показаны основные типы протоколов (рис. 2).

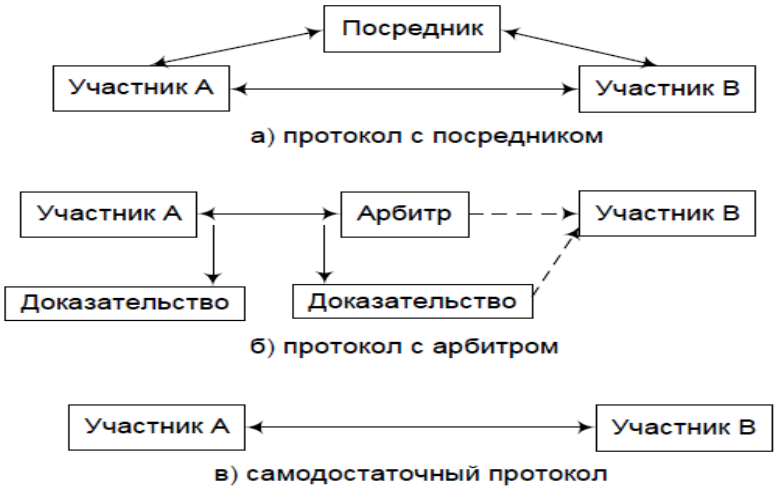

Рисунок 2 – Типы протоколов

Рассмотрим назначение некоторых видов протоколов:

– протоколы конфиденциальной передачи сообщений;

– протоколы аутентификации и идентификации;

– протоколы распределения ключей;

– протоколы электронной цифровой подписи;

– протоколы обеспечения неотслеживаемости.

Протоколы конфиденциальной передачи сообщений. Задача конфиденциальной передачи сообщений состоит в следующем. Имеются два участника протокола, которые являются абонентами сети связи. Участники соединены некоторой линией связи, по которой можно пересылать сообщения в обе стороны. Линию связи может контролировать противник. У одного из абонентов имеется конфиденциальное сообщение m, и задача состоит в том, чтобы это сообщение конфиденциальным же образом передать второму абоненту. Протоколы этого типа, наверно, появились раньше других криптографических протоколов, так как задача конфиденциальной передачи сообщений – исторически первая задача, которая решалась криптографией.

Протоколы аутентификации и идентификации. Они предназначены для предотвращения доступа к некоторой информации лиц, не являющихся ее пользователями, а также предотвращения доступа пользователей к тем ресурсам, на которые у них нет полномочий. Типичная сфера применения – организация доступа пользователей к ресурсам некоторой большой информационной системы.

Протоколы распределения ключей необходимы для обеспечения секретными ключами участников обмена зашифрованными сообщениями.

Протоколы электронной цифровой подписи позволяют ставить под электронными документами подпись, аналогичную обыкновенной подписи на бумажных документах. В результате выполнения протокола электронной цифровой подписи к передаваемой информации добавляется уникальное числовое дополнение, позволяющее проверить ее авторство.

Протоколы обеспечения неотслеживаемости ("Электронные деньги"). Под электронными деньгами в криптографии понимают электронные платежные средства, обеспечивающие неотслеживаемость, то есть невозможность проследить источник пересылки информации.

Рассмотрим простейший протокол для обмена конфиденциальными сообщениями между двумя сторонами, которые будем называть абонент А и абонент В. Пусть абонент А желает передать зашифрованное сообщение абоненту В.

В этом случае их последовательность действий должна быть следующей:

Абоненты выбирают систему шифрования (например, шифр Цезаря со сдвигом на n позиций).

Абоненты договариваются о ключе шифрования.

Абонент А шифрует исходное сообщение с помощью ключа выбранным методом и получает зашифрованное сообщение.

Зашифрованное сообщение пересылается абоненту А.

Абонент А расшифровывает зашифрованное сообщение с помощью ключа и получает открытое сообщение.

Этот протокол достаточно прост, однако он может действительно использоваться на практике. Криптографические протоколы могут быть простыми и сложными в зависимости от назначения.

Для современных криптографических систем защиты информации сформулированы следующие требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– знание алгоритма шифрования не должно влиять на надежность защиты;

– любой ключ из множества возможных должен обеспечивать надежную защиту информации;

– алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

И так, криптография сегодня - это важнейшая часть всех информационных систем:

– от электронной почты до сотовой связи,

– от доступа к сети Internet до электронной наличности.

Криптография обеспечивает подотчетность, прозрачность, точность и конфиденциальность. Она предотвращает попытки мошенничества в электронной коммерции и обеспечивает юридическую силу финансовых транзакций.

Библиографический список:

1. Басалова Г.В. Основы криптографиии. – Тула: Изд-во Тульского государственного университета, 2009. – 127 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си, Триумф – 2013 – 235 с.

3. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. – М.: Бином, 2007. – 376 с.

4. Ященко В.В. Введение в криптографию. – М.: МЦНМО, 2012. - 348 с. ISBN 978-5-4439-0026-1.

5. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. – М.: Гелиос АРВ, 2005. – 98с.

6. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: Интернет –Ун-т Информ. Технологий, 2005. –19 с.