Акматкулов А.А.
Кыргызский Государственный Технический
Университет им. И. Раззакова

О РОЛИ КИПТОГРАФИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: *берилген макалада бүгүнкү күндөгү криптографиянын базалык түшүнүктөрү жана методдору каралды. Алардын мани маңызын жеңилдетип берүүгө аракет жасалды.*

Аннотация:*в данной статье рассмотрены базовые понятия и методы современной криптографии. При изложении основной упор был сделана доступность материала.*

Abstract: *In given to article basic concepts and methods of modern cryptography are considered. At a statement the main emphasis was put on availability of material.*

Түйүндүү түшүнүктөр: *маалымат технологиялары, информацияны берүү, сактоо жана ыңгайлаштырып иштеп чыгуу, криптография, кедергиге каршы код берүү, ээсин аныктоо (тактоо)*

Ключевые слова: *информационные технологии, передача информации, криптография, помехоустойчивое кодирование, аутентификация.*

Keywords: *information technology, communication, cryptography, FEC authentication.*

В современной высшей школе все большую роль играют компьютеры, и вообще обучение электронным средствам передачи, хранения, и обработки информации.

Для того чтобы информационные технологии можно было использовать в различных областях, необходимо обеспечить их надежность и безопасность. Под безопасностью 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.

Простейшие способы шифрования появились очень давно, однако научный подход к исследованию и разработке криптографических методов появился только в прошлом (XX) веке. К настоящему времени криптография содержит множество результатов (теорем, алгоритмов), как фундаментальных, так и прикладных.

Занятие криптографией невозможно без серьезной математической подготовки. Особенно необходимы знания в области дискретной математики, теории чисел, абстрактной алгебры и теории алгоритмов. Вместе с тем не следует забывать, что криптографические методы предназначены в первую очередь для практического применения, а теоретически стойкие алгоритмы могут оказаться незащищенными перед атаками, не предусмотренными математической моделью. Поэтому после анализа абстрактной математической модели всегда необходим анализ полученного алгоритма с учетом ситуации, в которой он будет использоваться на практике.

Созданный нами учебно методический комплекс (УМК) для студентов экономико-инженерных специальностей КГТУ им.И. Раззакова. Поэтому автор предполагает у читателей наличие определенной математической культуры. Однако, как было указано выше, в криптографии особенно важным является четкое знание не только математики, но и «предметной области».

Целью данных методических указаний является ознакомление студентов с основными понятиями, методами и задачами криптографии. При этом автор исходил из того, что студенты сталкиваются с «настоящей» криптографией, поэтому основное внимание уделялось доступности материала, а не полноте и глубине изложения.

Следовательно, данные методические указания ни в коем случае нельзя рассматривать как полноценный учебник или справочник, содержащий готовые к употреблению криптографические алгоритмы. Это всего лишь начальный курс криптоанализа.

В первой части методического указания в контексте УМК рассматриваются базовые криптографические понятия, схемы и алгоритмы. Детальному анализу изучения более сложных криптографических схем и протоколов, вопросам криптоанализа и стойкости криптосистем будут указаны на учебники [2-4].

Криптография — это наука о способах преобразования информации с целью ее защиты от незаконных пользователей. Методы решения противоположной задачи (взлом криптографической защиты) составляют предмет другой науки — криптоанализа. Вместе с тем, было бы неправильным разделять криптографию и криптоанализ. И криптография, и криптоанализ изучают одни и те же объекты, но с разных точек зрения. Поэтому они скорее являются двумя частями одной и той же науки (она называется «криптология»), а не независимыми дисциплинами. Изучать их тоже надо совместно, потому что невозможно серьезно заниматься криптографией (например, разрабатывать шифры), не изучив криптоанализ.

Таким образом, рассматриваемый предмет правильнее было бы называть криптологией. Однако, учитывая сложившуюся традицию, всюду в данных методических указаниях будет использоваться термин «криптография». Проблемы и методы, подробное изложение этих методов можно найти в учебниках [там же].

Криптография возникла как наука о методах шифрования, и долгое время именно шифрование (т.е. защита передаваемых или хранимых данных от несанкционированного чтения) оставалась единственной проблемой, изучаемой криптографией. Однако в последнее время, в связи с бурным развитием информационных технологий, возникло множество новых применений, напрямую не связанных с сокрытием секретной информации.

Необходимость применения криптографических методов вытекает из условий, в которых происходит хранение и обмен информацией. В современных информационных системах очень часто происходит обмен данными в коллективах, члены которых не доверяют друг другу. В качестве примеров можно привести подписание контрактов или других документов, финансовые операции, совместное принятие решений и т.п.

В таких ситуациях необходимы средства, гарантирующие, что в процессе обмена или хранения информация не будет подвергнута искажениям, или не будет подменена целиком. Такую гарантию может дать только применение научно обоснованных криптографических методов.

Итак, целью применения криптографических методов является защита информационной системы от целенаправленных разрушающих воздействий (атак) со стороны противника. Способы защиты существенно зависят от ситуации: от какого рода угрозы необходимо защищаться, какими возможностями обладает противник. К ним оносятся:

- Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к данным). Это одна из основных задач криптографии, для ее решения применяется шифрование данных, т.е. такое их преобразование, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом.
- Обеспечение целостности данных — гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права. Под модификацией понимается вставка, удаление или подмена информации, а также повторная пересылка перехваченного ранее текста.
- Обеспечение аутентификации.

Под аутентификацией понимается проверка подлинности субъектов (сторон при обмене данными, автора документов, и т.д.) или подлинности самой информации. Частным случаем аутентификации является идентификация — процедура доказательства субъектом того, что он действительно является именно тем, за кого себя выдает. Во многих случаях субъект - 1должен не просто доказать свои права, но сделать это так, чтобы проверяющий субъект -2 не смог впоследствии сам использовать полученную информацию для того, чтобы выдать себя за первым. Подобные доказательства называются «доказательствами с нулевым разглашением».

- Обеспечение невозможности отказа от авторства — предотвращение возможности отказа субъектов от совершенных ими действий (обычно — невозможности отказа от подписи под документом). Эта задача неотделима от двойственной — обеспечение невозможности приписывания авторства. Наиболее яркий пример ситуации, в которой стоит такая задача — подписание договора двумя или большим количеством лиц, не доверяющих друг другу.

В такой ситуации все подписывающие стороны должны быть уверены в том, что в будущем, во-первых, ни один из подписавших не сможет отказаться от своей подписи и, во-вторых, никто не сможет модифицировать, подменить или создать новый документ (договор) и утверждать, что именно этот документ был подписан. Основным способом решения данной проблемы является использование цифровой подписи.

Помимо перечисленных основных задач можно назвать также электронное голосование, жеребьевку, разделение секрета (распределение секретной информации между несколькими субъектами таким образом, чтобы воспользоваться ей они могли только все вместе) и многое другое. Подробное описание криптографических приложений можно найти в источниках[2–4].

Чем шифрование отличается от кодирования? Слова «кодирование» и «шифрование» часто используются как синонимы. Однако в современной прикладной математике (к которой можно отнести и криптографию) эти термины разделяются. Под шифрованием понимается такое преобразование текста (сообщения), в результате которого прочитать преобразованный текст может только тот, кто обладает специальным ключом.

Кодированием называется любое преобразование данных из одной формы представления в другую. Таким образом, кроме шифрования, термин «кодирование» включает в себя также так называемое «помехоустойчивое кодирование» (преобразование текста, позволяющее восстанав-

ливать его в случае сбоя при передаче или хранении), сжатие данных и т.п. В широком смысле, кодированием можно назвать также сканирование текста или изображения (информация преобразуется из визуального представления в цифровое), и даже ввод текстов с клавиатуры.

Рисунок 1. Простейшая модель криптосистемы

Простейшую модель криптографической системы можно изобразить так, как показано на рисунке (см. рис. 1). Таким образом, имеется некая информационная система, включающая двух или более абонентов (законных пользователей) и канал (или каналы), по которым абоненты могут обмениваться сообщениями. Имеется также возможность появления противника, т.е. незаконного пользователя. Противник может перехватывать сообщения, передаваемые абонентами друг другу.

Здесь необходимы следующие пояснения: Во-первых, противник может быть как внешним (т.е. не входить в число абонентов системы), так и внутренним (быть абонентом системы). В последнем случае этот абонент считается незаконным пользователем, если он пытается получить доступ к сообщениям, на которые не имеет права (например, конфиденциальные сообщения, которыми обмениваются другие абоненты).

Во-вторых, противник может перехватывать сообщения с разными целями — например, с целью разглашения перехватываемой информации (использование этой информации в своих целях или передача информации другому лицу), подмены или имитации сообщения и т.д. Подобные цели называются угрозами. Для защиты от различных видов угроз необходимо применять различные криптографические методы. Рассматриваемая нами задача обеспечения конфиденциальности информации представляет собой задачу защиты от угрозы разглашения.

Наконец, следует иметь в виду, что описанная модель может применяться и в случаях, внешне отличных от обмена сообщениями. Например, при защите данных, хранящихся на компьютере, можно считать, что абонент А и абонент Б — одно и то же лицо, работающее с данными в разные моменты времени. В этом случае «каналом» является жесткий диск компьютера, на котором хранятся данные.

Итак, рассматривается модель, в которой противник имеет доступ к каналу передачи сообщений. Поэтому абонент, передающий сообщение (отправитель) должен перед отправкой преобразовать исходную информацию (открытый текст) в закрытый текст (который называется шифртекстом, зашифрованным текстом или криптограммой).

Преобразование открытого текста в шифртекст называется шифрованием (часто используется также термин зашифрование). Абонент, получивший такой зашифрованный текст (получатель), с помощью обратного преобразования (расшифрования, расшифровки) восстанавливает исходный открытый текст.

Процедуры шифрования и расшифрования используют некоторые секретные данные, называемые ключами, причем в некоторых криптосистемах ключ шифрования и ключ расшифрования совпадают, а в других — различаются. Ключи известны только абонентам криптосистемы, причем для обмена данными с различными пользователями один и тот же абонент может использовать различные ключи.

Противник не знает ключ расшифрования, но может попытаться вскрыть шифр, т.е. либо подобрать ключ, либо преобразовать зашифрованный текст в открытый каким-либо другим способом. Методы вскрытия шифров называются криптоанализом, а противник, применяющий эти методы — криптоаналитиком. Успех криптоанализа зависит как от свойств криптографической системы, так и от имеющихся у противника ресурсов (время, мощность вычислительных машин и т.п.). Способность шифра (криптосистемы) противостоять попыткам взлома (атакам) называется стойкостью шифра.

Существуют абсолютно стойкие системы шифрования, однако они очень не удобны и требуют больших затрат при использовании. Ни одна из широко используемых на практике систем

шифрования не является абсолютно стойкой. Это означает, что если противник обладает неограниченными ресурсами и достаточно широкими возможностями для атаки (например, имеет доступ к некоторым открытым текстам и соответствующим им шифртекстам, полученным с использованием одного и того же ключа), то рано или поздно он сможет взломать шифр.

Однако если выгода от использования полученной информации будет меньше, чем затраты на взлом, противник вряд ли будет этим заниматься. Поэтому при выборе алгоритма шифрования необходимо точно оценить соотношение ценности защищаемой информации, стойкости шифра и удобства его использования — иначе затраты на защиту информации могут превысить стоимость самой информации.

Введем формальное определение шифра и его составных частей [**Ошибка! Источник ссылки не найден.**]. Пусть T, C и K — конечные множества возможных открытых текстов, шифртекстов и ключей. Обычно каждое из этих множеств представляет собой множество *слов* в некотором *алфавите*, причем алфавиты открытых текстов, шифртекстов и ключей могут различаться. Для большинства современных систем шифрования открытые тексты, шифртексты и ключи представляют собой слова в алфавите {0,1}, т.е. последовательности нулей и единиц.

Процедура шифрования задает функцию E_k: $T \to C$, которая отображает множество открытых текстов во множество шифртекстов в зависимости от некоторого ключа $k \in K$. Аналогично, процедура расшифрования D_k: $C \to T$ также зависит от ключа k и отображает множество шифртекстов во множество открытых текстов. Так как получатель всегда должен иметь возможность по шифртексту восстановить исходный текст, то при любом k из K функции E_k и D_k должны удовлетворять условию: $D_k \circ E_k = I$, где I — тождественное отображение T в T.

Выводы: Получившаяся последовательность нулей и единиц является числовым представлением текста. Часто при реализации алгоритмов шифрования и расшифрования бывает удобно считать, что длина ключа, используемого для преобразования текста, равна длине самого текста или зависит от длины текста каким-то определенным образом.

Литература:

1. Учебно-методический комплекс по средствам и защиты информаций.сост. Акматкулов А.А.- ИУиБ, КГТУ им. И.Раззакова.- Бишкек, 2013.-190 с.

2. Программирование алгоритмов защиты информации. / Домашев А.В., Грунтович М.М., Попов В.О. и др. – М.: «Нолидж», 2002. – 416 с.

3. Хорев П.Б. Методы и средства защиты информации в компьютерныхсистемах. – М.: Издательский центр «Академия», 2005. – 256 с.

4. Хорев П.Б. Технологии объектно-ориентированного программирования. –

М.: Издательский центр «Академия», 2004. – 448 с.