Опишем весь алгоритм:

1. Пользователь А устанавливает какое-то конкретное значение x.

2. В зависимости от значения x с помощью формулы Кеплера определяется значение y.

3. Пользователь А отправляет значение y пользователю В.

4. Пользователь В, используя секретный ключ – конкретное пересечение, определяет значение x.

5. Пользователи А и В получают доступ к информации.

Из этого следует, что другие пользователи, не зная секретного ключа, не имеют доступа к передаваемой информации. Вся сложность данного алгоритма заключается в бесконечно большом количестве значений, в которых происходит пересечение. Другие пользователи, не зная секретного ключа, не имеют доступа к передаваемой информации. Следовательно, данный алгоритм может использоваться как алгоритм защиты передаваемой информации между двумя пользователями.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

В. В. Егоров
(Екатеринбург, УрФУ, evv93@mail.ru)

Целью прохождения практики на предприятии являлось ознакомление и изучение средств защиты персональных данных от несанкционированного доступа (НСД). Особое внимание было уделено средствам защиты информации, в основе которых лежат принципы использования криптографии, использование этих средств на предприятии.

Криптография в прошлом использовалась лишь в военных целях. Однако сейчас, по мере образования информационного общества, она становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные

платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Криптография позволяет реализовывать следующие механизмы защиты информации:

- шифрование данных, передаваемых по каналам связи или хранимым в базах данных;
- контроль целостности данных, передаваемых по каналам связи;
- идентификация (опознавание) субъекта или объекта системы (сети);
- аутентификация (проверка подлинности) субъекта или объекта сети;
- контроль (разграничение) доступа к ресурсам системы (сети).

Базовых методов преобразования информации, которыми располагает криптография, немного, среди них:

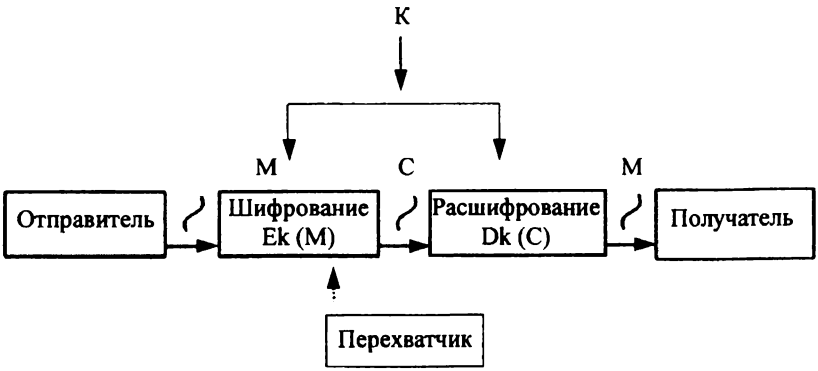
- шифрование (симметричное и несимметричное);
- вычисление хэш-функций;
- генерация электронной цифровой подписи;
- генерация последовательности псевдослучайных чисел.

В настоящее время проблема защиты от НСД весьма актуальна. Все нынешние государственные структуры, работа которых связана с персональными данными (ПД), либо с любой другой информацией, имеющей некую ценность, являются плохо защищенными.

Многие компании предоставляют услуги по созданию средств защиты информации (СЗИ). В данном случае наиболее целесообразно использовать средства криптографической защиты информации (СКЗИ). Одной из таких компаний, выполняющих госзаказы по созданию и обслуживанию СКЗИ, является «ООО Цинтур».

В работе рассмотрены различные виды шифрования. Шифрование – это преобразование данных в нечитабельную форму при помощи ключей шифрования (рисунок).

Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу. За каналом следит злоумышленник с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы



Обобщенная схема криптосистемы

перехватчик не смог узнать содержание сообщения М, отправитель шифрует его с помощью обратимого преобразования Ek и получает шифртекст (или криптограмму) C = EK (M), который отправляет получателю.

Законный получатель, приняв шифртекст С, расшифровывает его с помощью обратного преобразования D = Ek – 1 и получает исходное сообщение в виде открытого текста М:

$$Dk\ (C) = Ek - 1\ (Ek\ (M)) = M.$$

Преобразование выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом К. Ключ К может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным; зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (владельцами).

Криптосистема имеет разные варианты реализации: набор инструкций, аппаратные средства, комплекс программ компьютера, которые позволяют зашифровать открытый текст и расшифровать шифротекст различными способами, один из которых и выбирается с помощью конкретного ключа К.

Более подробно в этой части работы рассмотрены симметричные и асимметричные криптографические системы с открытым и закрытым ключами.

Раскрыта роль и необходимость криптоанализа. Криптоанализ – это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу [1].

Фундаментальное правило криптоанализа, впервые сформулированное голландцем А. Керкхоффом еще в XIX в., заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, правило Керкхоффа указывает на то, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации. Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и финансов, тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Криптографическими методами можно обеспечить не только конфиденциальность, но и проконтролировать целостность передаваемых или хранимых данных. Контроль целостности в основном производится путем расчета некоторой «контрольной суммы» данных. Математиками и инженерами, работающими в области передачи данных и теории кодирования, разработано множество алгоритмов, рассчитывающих контрольные суммы передаваемых данных. Для многих приложений простой контрольной суммы (например, известного алгоритма crc32 или последовательного побайтного или пословного сложения исходного текста с известной константой) оказывается достаточно, особенно тогда, когда важна скорость обработки данных и не известен заранее объем данных (типичный случай – передача данных по каналам связи).

Проблема простых алгоритмов вычисления контрольной суммы в том, что достаточно легко подобрать несколько массивов данных, имеющих одинаковую контрольную сумму. Криптографически стойкие контрольные суммы вычисляются как результат применения к исходному тексту так называемой хэш-функции.

Одним из результатов теории сложности теории функций является гипотеза о существовании односторонних функций. Под односторонней функцией понимается функция, определенная (например) на множестве натуральных чисел и не требующая для вычисления своего значения больших вычислительных ресурсов. Но вычисление обратной функции (т. е. по известному значению функции восстановить значение аргумента) оказывается невозможно теоретически или (в крайнем случае) невозможно вычислительно. Строгое существование односторонних функций пока не доказано. Поэтому все используемые в настоящее время хэш-функции являются лишь «кандидатами» в односторонние функции, хотя и имеют достаточно хорошие свойства.

В настоящее время все больше и больше набирает популярность использование электронного документооборота. Это гораздо удобнее и выгоднее. В связи с этим в работе особое внимание уделено рассмотрению принципов использования хэш-функций в создании и использовании электронно-цифровых подписей.

Идея электронной подписи проста. В процессе шифрования с использованием асимметричного алгоритма для зашифрования сообщения используется открытый ключ, а для расшифрования – секретный. Но в применении к шифрованию ключи взаимозаменяемы. Можно зашифровать сообщение на своем секретном ключе, и тогда любой желающий сможет его расшифровать, используя открытый ключ. Это свойство асимметричных алгоритмов, и используется оно при формировании и проверке электронно-цифровой подписи. Собственно электронно-цифровая подпись документа – это его хэш-сумма, зашифрованная секретным ключом. Проверка электронно-цифровой подписи документа сводится к вычислению хэш-суммы документа, расшифрованию хэш-суммы, содержащейся в подписи, и сравнению двух величин. Если значения вычисленной

и сохраненной в подписи хэш-сумм совпали, то считается, что подпись под документом верна [1].

Во многих приложениях задача идентификации и аутентификации доступа человека или программы к некоторому ресурсу является даже более важной, чем задача обеспечения конфиденциальности. Практически все многопользовательские и сетевые операционные системы требуют аутентификации пользователя, равно как банкоматы и кассовые терминалы. С развитием Интернета и безбумажных технологий число приложений, которые требуют аутентификации пользователей, будет только возрастать.

Идентификацией субъекта при доступе к информационной системе называется процесс сопоставления его с некоторой хранимой системой-характеристикой субъекта – идентификатором. В дальнейшем идентификатор субъекта используется для предоставления субъекту определенного уровня прав и полномочий при использовании информационной системой. Аутентификацией субъекта называется процедура верификации принадлежности идентификатора субъекту. Аутентификация производится на основании того или иного секретного элемента (аутентификатора), которым располагают как субъект, так и информационная система. Обычно информационная система располагает не самим секретным элементом, но некоторой информацией о нем, на основании которой принимается решение об адекватности субъекта идентификатору.

В работе рассмотрены наиболее распространенные и эффективные методы идентификации и аутентификации.

Один класс методов аутентификации основывается на том, что аутентифицируемый субъект должен иметь некоторый секретный элемент (пароль, секретный ключ или специальный аутентификационный токен). Другой класс методов аутентификации применим в основном для аутентификации людей. Он основывается на наличии уникальных физических свойств самого человека (отпечатки пальцев, форма кисти руки, голос, радужная оболочка глаза). У каждого класса методов есть как достоинства, так и недостатки. Алгоритмически процедура аутентификации представляется как последовательная передача одной или нескольких информационных по-

сылок между субъектом и информационной системой и промежуточная их обработка обеими сторонами. В результате этих действий обе стороны обмена должны удостоверить, что они являются теми, за кого себя выдают.

В результате работы изучены средства защиты персональных данных от несанкционированного доступа, в основе работы которых лежит использование криптографических методов и алгоритмов защиты информации. Изучена сфера применения этих средств в компании ООО «Цинтур». Также получены практические навыки работы с данными средствами.

Библиографические ссылки

1. *Соколов А. В.*, *Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. М. : ДМК, 2002. 450 с.

РЕАЛИЗАЦИЯ КРИПТОСИСТЕМЫ ПЭЙЕ НА ЭРЛАНГЕ

А. Н. Комиссаров, *Д. А. Подкорытов*, *С. О. Суханинский*
(Курган, КГУ, cerg121@yandex.ru)

В настоящее время все более активно развиваются технологии облачных вычислений. Основными причинами такого развития являются доступность, низкая стоимость и вычислительная эластичность данной технологии. Также у компаний и физических лиц появляется возможность значительно уменьшить расходы на инфраструктуру информационных технологий. Но несмотря на все эти преимущества, существует реальная угроза раскрытия конфиденциальных данных, хранящихся в облачной инфраструктуре, так как у ее провайдера появляется возможность неконтролируемого доступа к обрабатываемым данным.

Единственным действенным решением этой проблемы может служить шифрование всей конфиденциальной информации перед передачей в облако. К сожалению, все распространенные в настоя-