5. Протоколы распределения ключей

*Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли.*

*Схемы предварительного распределения ключей. Неравенство Блома. Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции.*

Протокол распределения ключей (key establishment protocol) - это криптографический протокол, в процессе выполнения которого общий секрет становится доступен двум или более сторонам для последующего использования в криптографических целях. .

Протоколы распределения ключей подразделяются на два класса: протоколы транспортировки ключей и обмена ключами. Протоколы распределения ключей могут строиться как без участия «третьей стороны», так и с ее участием. Доверенная «третья сторона» может выполнять различные функции: сервер аутентификации, центр распределения ключей, центр трансляции ключей, удостоверяющий центр и др.

К основным свойствам протоколов распределения ключей относят свойства аутентификации ключа, подтверждения ключа и явной аутентификации ключа.

(Неявная) аутентификация ключа (implicit key authentication) — свойство, посредством которого один участник протокола убеждается, что никакая другая сторона, кроме специально идентифицированного второго участника протокола (и возможно, центра доверия), не может получить доступ к секретным ключам, полученным в протоколе.

Разъясним это определение. Здесь нет гарантий, что второй участник действительно получил доступ к ключу, но никто другой, кроме него, не мог его получить. Неявная аутентификация ключа независима от реального обладания ключом другим участником и не требует каких бы то ни было действий от второй стороны.

Протокол аутентичного распределения ключей (authenticated key establishment protocol) ~ это протокол распределения ключей, который обеспечивает аутентификацию ключей в смысле предыдущего определения.

Подтверждение ключа (key confirmation) - свойство, посредством которого один участник протокола убеждается, что другой участник (возможно, не идентифицированный) действительно обладает секретными ключами, полученными в протоколе.

В протоколах применяется четыре способа подтверждения ключа:

1. вычисление хеш-кода ключа;
2. использование ключа в хеш-функции с ключом;
3. шифрование известной величины, используя ключ;
4. доказательства с нулевым разглашением знания.

Явная аутентификация ключа (explicit key authentication) - свойство, которое выполняется, когда имеют место (неявная) аутентификация ключа и подтверждение ключа одновременно. В этом случае известно, что идентифицированная сторона протокола реально обладает специфицированным ключом.

Понятие аутентификации ключа не тождественно понятию аутентификации субъекта-участника протокола. Аутентификация участника в смысле ранее введенных понятий (идентичность стороны и ее «присутствие» в текущий момент времени) требуется далеко не во всех протоколах. Например, известный «классический» протокол обмена ключами Диффи - Хеллмана не обеспечивает ни аутентификацию ключа, ни подтверждение ключа, ни аутентификацию участников протокола.

Протокол распределения ключей (key distribution protocol) – протокол получения пользователями ключей, необходимых для функционирования криптографической системы. Различают следующие типы протоколов распределения ключей: протоколы передачи (уже сгенерированных) ключей; протоколы совместной выработки общего ключа (открытое распределение ключей); схемы предварительного распределения ключей.

Открытое распределение ключей (public key distribution) — протокол совместной выработки пользователями (общего) секретного ключа путем обмена сообщениями по открытому каналу связи. Протокол должен исключать возможность получения информации о ключе посторонними, а также любым участником до завершения им действий, предусмотренных протоколом.

Схема предварительного распределения ключей (preliminary key distribution scheme) – схема разделения секрета, применяемая в сети связи для уменьшения объема хранимой информации о ключах. Суть схемы предварительного распределения ключей состоит в том, что предварительно распределяются не ключи, а сгенерированные в центре распределения ключей секретные данные меньшего объема, по которым каждый пользователь самостоятельно вычисляет по оговорённому алгоритму необходимый для связи ключ. Схема предварительного распределения ключей должна быть устойчивой относительно компрометации части ключей, в том числе, вследствие обмана или сговора некоторых пользователей, и гибкой, то есть быстро восстанавливаться как после частичной компрометации, так и после подключения новых пользователей.

В схеме Блома доверенная сторона раздаёт каждому участнику открытый и закрытый ключ. Участники, обмениваясь между собой только открытыми ключами по незащищённым каналам связи, могут сгенерировать секретный сеансовый ключ для общения между собой.

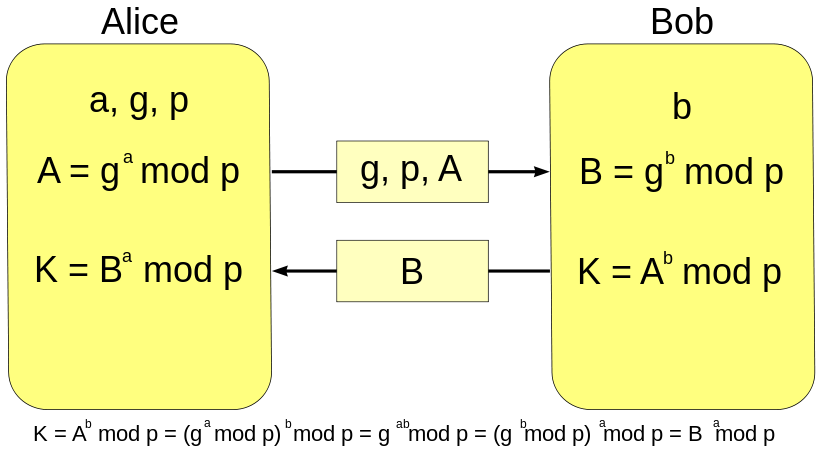
Надёжность схемы напрямую зависит от размера секретной матрицы, используемой в схеме. Для восстановления секретной матрицы (точнее, любой выполняющей аналогичную функцию) необходимо иметь число ключей, равное количеству строк матрицы.

Схема используется в протоколе HDCP в целях защиты видео от копирования.

Для вычисления общего секретного ключа двух сторон нужно знать секретную матрицу. Её можно восстановить, если получить k линейно независимых идентификаторов.

Передача ключа по открытым каналам была большой проблемой криптографии 20 века. Но эту проблему удалось решить после появления алгоритма Диффи-Хеллмана. Данный алгоритм позволил дать ответ на главный вопрос:

«Как при обмене зашифрованными посланиями уйти от необходимости передачи секретного кода расшифровки, который, как правило, не меньше самого послания?» Открытое распространение ключей Диффи-Хеллмана позволяет паре пользователей системы выработать общий секретный ключ, не обмениваясь секретными данными (рис 5.1).

Рис 5.1 Алгоритм Диффи-Хеллмана, где K – итоговый общий секретный ключ

При работе алгоритма каждая сторона:

генерирует случайное натуральное число a — закрытый ключ

совместно с удалённой стороной устанавливает открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где

p является случайным простым числом

(p-1)/2 также должно быть случайным простым числом (для повышения безопасности)[5]

g является первообразным корнем по модулю p (также является простым числом)

вычисляет открытый ключ A, используя преобразование над закрытым ключом

A = ga mod p

обменивается открытыми ключами с удалённой стороной

вычисляет общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a

K = Ba mod p

К получается равным с обеих сторон, потому что:

Ba mod p = (gb mod p)a mod p = gab mod p = (ga mod p)b mod p = Ab mod p

В практических реализациях для a и b используются числа порядка 10100 и p порядка 10300. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

В чистом виде алгоритм Диффи-Хеллмана уязвим для модификации данных в канале связи, в том числе для атаки «Человек посередине», поэтому схемы с его использованием применяют дополнительные методы односторонней или двусторонней аутентификации.

Конференц-связь - это многосторонняя рассылка сообщений в режиме реального времени (число участников обмена сообщениями не менее трех).

В случае обмена секретной информацией всем участникам обмена необходимо иметь общий секретный ключ. Протокол распределения ключей конференц-связи - это обобщение протокола двустороннего распределения ключей с целью обеспечения трех или более участников общим секретным ключом.

К распределению ключей конференц-связи выдвигается несколько вполне очевидных требований:

1) различные группы участников М вырабатывают разные секретные ключи, так как участникам одной конференции не должны быть доступны данные, передаваемые в других конференциях);

2) эти сеансовые ключи динамические (т. е. протоколы с пред- распределенными ключами исключаются), более того, в различных конференциях, даже при одинаковом составе участников, должны быть разные ключи, так как очень высок риск их компрометации;

3) информация, которой обмениваются участники в процессе выполнения протокола распределения ключей несекретная, т. е. передается по открытым каналам;

4) каждая сторона индивидуально вычисляет сеансовый ключ (это следствие из предыдущего требования).

Предложен ряд протоколов распределения ключей конференц-связи. Аутентификации ключа они не обеспечивают, являясь, по сути, только обобщениями протокола Диффи - Хеллмана для числа участников, большего двух.

Теория и практика конструирования протоколов распределения ключей конференц-связи в настоящее время бурно развиваются, что связано с развитием средств для групповой работы в информационных системах, таких, как системы обмена сообщениями, системы планирования ресурсов предприятия, дистанционное обучение, многообразные военные применения и др. Одной из актуальных проблем является разработка протоколов для групп с динамическим составом участников. Очевидный и главный недостаток всех существующих протоколов заключается в том, что вся конференция компрометируется при компрометации общего ключа конференции хотя бы у одного из участников.