УДК 003.26

С. М. Калиновский

Институт бизнеса БГУ, Минск, Беларусь, kalina19901958@gmail.com

РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ ДЛЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

В работе рассматриваются вопросы, связанные с распределением ключей для криптографических систем. Дается понятие распределения ключей. Определены требования, предъявляемые к протоколам распределения ключей. Приведены их достоинства и недостатки.

***Ключевые слова**: криптографическая стойкость, криптографическая система, криптографический алгоритм, криптографический ключ, протокол распределения ключей, управление ключами*

S. Kalinouski

School of Business of BSU, Minsk, Belarus, kalina19901958@gmail.com

KEY DISTRIBUTION FOR CRYPTOGRAPHIC SYSTEMS

The paper discusses issues related to the distribution of keys for cryptographic systems. The concept of key distribution is given. The requirements for key distribution protocols have been determined. The advantages and disadvantages of key distribution protocols of various cryptographic systems are given.

***Keywords:** cryptographic strength, cryptographic system, cryptographic algorithm, cryptographic key, key distribution protocol, key management*

В настоящее время в сфере информационных технологий криптографические системы применяются не только для зашифрования сообщений, но и в других областях жизнедеятельности человека. Любая криптографическая система основана на использовании криптографических ключей. Под ключевой информацией понимают совокупность всех действующих в информационной сети или системе ключей [1].

Современная криптография включает в себя четыре крупных раздела: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами [2]. Эффективность криптографической защиты информации в компьютерных сетях во многом зависит от их стойкости криптографических преобразований и надежности протоколов управления ключами.

Стойкость – это способность криптографической системы противостоять попыткам ее математического анализа. Протоколы управления криптографическими ключами включают протоколы генерации, распределения, хранения, смены и уничтожения криптографических ключей [1].

Безопасность передачи информации в криптографических системах более всего зависит от наличия ключей и методов их распределения. Это слабое место в криптографических приложениях. Применять криптографические системы достаточно просто, но хранить и использовать ключи, а также обмениваться ими сложнее.

Распределение ключей – это процесс передачи секретной информации между двумя и более участниками, чтобы обеспечить безопасность и конфиденциальность коммуникации. Ключи используются в криптографии для шифрования и дешифрования данных, а также для аутентификации и целостности сообщений [3].

Существует несколько методов распределения ключей:

1. Распределение ключей в традиционных симметричных и асимметричных криптографических системах производится методом их рассылки специально выделенными курьерами между участниками обмена информацией. Такой метод является сложным в исполнении, затратным и неоперативным, однако безопасным и надежным при соблюдении всех правил конспирации.

2. Использование центра распределения ключей. Центр распределения ключей – это доверенная сторона или устройство, которое выполняет функцию генерации и распределения ключей между участниками криптографической системы. Он играет важную роль в обеспечении безопасности передачи данных, так как ключи используются для шифрования и расшифрования информации [3].

Центр распределения ключей отвечает за генерацию, хранение и распределение ключей для криптографических систем.

Преимущества использования центра распределения ключей:

1. Централизованное управление.
2. Удобство использования.
3. Безопасность.
4. Легкость масштабирования.

Недостатки использования центра распределения ключей:

1. Единственная точка отказа.
2. Уязвимость к атакам.
3. Сложность управления.
4. Зависимость от центра распределения ключей.

Центр распределения ключей является критическим компонентом в системе криптографии, поскольку отвечает за безопасное распределение ключей между участниками. Поэтому важно обеспечить его защиту от атак [3].

Защита центра распределения ключей от атак должна включать:

1. Физическую защиту.
2. Криптографическую защиту.
3. Механизмы аутентификации участников.
4. Механизмы резервного копирования и восстановления.
5. Системы анализа проводимых атак, а также журналирования, мониторинга сетевого трафика и системы обнаружения вторжений.

Существуют такие протоколы распределения ключей с участием центра распределения ключей:

1. Протокол Диффи-Хеллмана – один из наиболее известных протоколов распределения ключей с участием центра распределения ключей. С его помощью генерируется общий секретный ключ, который может быть использован для зашифрования и расшифрования сообщений.

Схема распределения ключей Диффи-Хеллмана имеет важное преимущество перед другими – отсутствие необходимости иметь защищенный канал для передачи ключей.

2. Протокол RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) основан на сложности факторизации больших целых чисел и использует два ключа: открытый и закрытый (секретный). Открытый ключ служит для зашифрования сообщения, а закрытый для расшифрования. RSA является первой системой, которая используется как для шифрования, так и для цифровой электронной подписи.

3. Протокол Цербера (в древнегреческой мифологии Kerberos – трехголовый пес, который защищал выход из подземного царства Аида). Трем головам Цербера в протоколе

соответствуют три участника шифрованной передачи данных: клиент, сервер и доверенный посредник между ними.

В протоколе Цербера реализованы взаимная аутентификация и механизм отметки времени, гарантирующие подлинность сеанса распределения сеансового ключа для пользователей A и B. В качестве центра распределения ключей в протоколе Цербера выступает сервер TGS [4].

Протокол Цербера включает в себя работу с тремя серверами: опознавательный сервер (AS – Authentication Server), сервер, предоставляющий билет (TGS – Ticket-Granting Server) и реальный сервер (сервер обработки данных), который обеспечивает услуги.

Схема протокола Цербера показана на рис. 1.

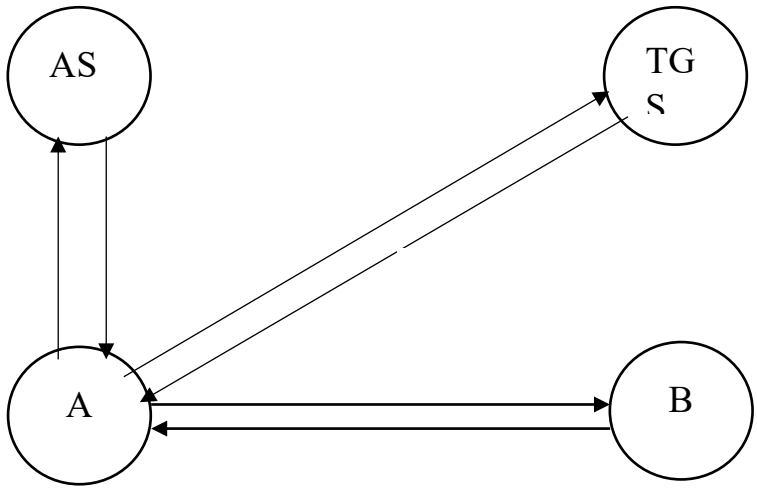

Рис. 1. Схема протокола Цербера

Недостатком этого протокола является знание центром содержания ключей и кто их использует. Сотрудники центра могут свободно читать сообщения, зашифрованные на этих ключах, фактически владеть всей информацией, циркулирующей в информационной системе.

В случае прямого обмена ключами, то есть от одного адресата другому появляется проблема определения (аутентификации) подлинности корреспондентов. Она решается двумя способами:

1. Механизм «запрос-ответ». Корреспондент A передает корреспонденту B какой-то элемент, например, число. Корреспондент B прибавляет к этому числу какое-то число, о котором известно корреспонденту A и отправляет ему полученную сумму. Корреспондент A проводит проверку и удостоверяется в подлинности сообщения.
2. Механизм отметки времени («временной штемпель»). Он подразумевает фиксацию времени для каждого сообщения. В этом случае каждый пользователь информационной системы может знать насколько «старым» является пришедшее сообщение.

При использовании отметок времени встает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса, так как сообщение с «временным штемпелем» не может быть передано мгновенно [2].

Кроме этого, в настоящее время в Республике Беларусь применяется электронная цифровая подпись (уже выдано их более двух миллионов), использование которой позволяет решить проблему аутентификации.

На данный момент более актуальной задачей является распределение ключей для группы участников. Такая задача возникает при организации безопасной связи внутри групп абонентов, при аутентификации участников группы, при формировании групповой цифровой подписи, при организации конференц-связи и т. д. [2].

При комплексном использовании симметричных и асимметричных криптографических систем достигается их эффективность. Оказывается, эти криптосистемы могут друг друга дополнять, при этом устраняя имеющиеся недостатки.

Главное достоинство асимметричных криптосистем с открытым ключом – высокая безопасность: секретные ключи и их значения никому не передаются, их подлинность не вызывает сомнений. Однако одним из серьезных недостатков является то, что быстродействие асимметричных криптосистем с открытым ключом обычно в сотни и более раз меньше быстродействия симметричных криптосистем с секретным ключом.

Быстродействующие симметричные криптосистемы имеют существенный недостаток: секретные ключи симметричной криптосистемы по мере расходования должны постоянно обновляться и передаваться корреспондентам по информационному обмену, и во время этих обновлений возникает опасность раскрытия секретного ключа.

Комбинированное применение симметричного и асимметричного шифрования позволяет устранить основные недостатки, присущие обоим методам. Комбинированный (гибридный) метод шифрования дает возможность сочетать преимущества высокой секретности, предоставляемые асимметричными криптосистемами с открытым ключом, с преимуществами высокой скорости работы, присущими симметричным криптосистемам с секретным ключом [1].

Совместное использование этих криптосистем позволяет эффективно реализовать криптографическое закрытие передаваемой информации с целью обеспечения ее безопасности.

Метод комбинированного использования симметричного и асимметричного шифрования заключается в следующем: симметричную криптосистему применяют для шифрования исходного открытого текста, а асимметричную с открытым ключом – только для шифрования секретного ключа симметричной криптосистемы.

В результате асимметричная криптосистема с открытым ключом не заменяет, а лишь дополняет симметричную криптосистему с секретным ключом, позволяя повысить в целом защищенность передаваемой информации [1].

При комбинированном методе шифрования применяются криптографические ключи как симметричных, так и асимметричных криптосистем. Очевидно, выбор длин ключей для криптосистемы каждого типа следует осуществлять таким образом, чтобы злоумышленнику было одинаково трудно атаковать любой механизм защиты комбинированной криптосистемы.

В табл. 1 приведены распространенные длины ключей симметричных и асимметричных криптосистем, для которых трудность атаки полного перебора примерно равна трудности факторизации соответствующих модулей асимметричных криптосистем [1].

Таблица 1

Длины ключей для симметричных и асимметричных криптосистем при одинаковой их криптостойкости

Длина ключа симметричной криптосистемы, бит	Длина ключа асимметричной криптосистемы, бит
56	384
64	512
80	768
112	1 792
128	2 304

Если используется короткий сеансовый ключ (например, 56-битный ключ алгоритма DES), то не имеет значения, насколько велики асимметричные ключи. Злоумышленник будет атаковать не их, а сеансовый ключ [1].

У протоколов распределения ключей для криптографических систем существуют свои достоинства и недостатки, однако, они нашли свое применение в информационных системах для гарантированного закрытия информации различного характера.

Распределение ключей для криптографических систем обеспечивается различными протоколами как с использованием центров распределения ключей, так и их прямым обменом между пользователями.

Список использованных источников

1. Защита информации [Электронный ресурс]. – Режим доступа: https://yztm.ru/lekc2/l17/. – Дата доступа: 03.04.2024.

2. *Фомина, И. А.* Управление ключами в криптографических системах / И. А. Фомина // Вестник Нижегородского университета им. Н. И. Лобачевского. – 2010. – С. 165-169.

3. Распределение ключей в криптографии [Электронный ресурс]. – Режим доступа: https://nauchniestati.ru/spravka/raspredelenie-klyuchej-s-uchastiem-czentra-raspredeleniya-lyuchej/ – Дата доступа: 03.04.2024.

4. *Харин, Ю. С.* Математические основы криптологии / Ю. С. Харин и др. – Минск : БГУ, 1999. – 319 с.