Протокол Диффи-Хеллмана с применением криптоалгоритма RSA

Описание проблемы

Протокол Диффи-Хеллмана (или Диффи-Хеллмана-Меркла) - это криптографический протокол, который используется для безопасного обмена секретными ключами между двумя участниками, не имеющими предварительного общего секрета.

Основная идея протокола заключается в том, чтобы создать общий секретный ключ, используя открытые каналы связи. Ключ, полученный с помощью протокола Диффи-Хеллмана, может затем использоваться для шифрования сообщений между участниками общения.

Протокол Диффи-Хеллмана является основой для многих криптографических систем, таких как SSL, TLS и SSH, которые используются для обеспечения безопасной связи в Интернете. Также этот протокол может использоваться для защиты коммуникаций в любой другой сфере, где безопасность передачи информации имеет первостепенное значение, например, в системах электронного голосования или в области финансовых транзакций.

В чистом виде алгоритм Диффи–Хеллмана уязвим для модификации данных в канале связи, в том числе для атаки «Man-in-the-middle (человек посередине)», поэтому схемы с его использованием применяют дополнительные методы односторонней или двусторонней аутентификации.

История

Передача ключа по открытым каналам была большой проблемой криптографии XX 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.

Основы криптографии с открытыми ключами были выдвинуты Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman), а также независимо от них Ральфом Мерклом (Ralph Merkle).

Их вкладом в криптографию было утверждение, что ключи можно использовать парами – ключ шифрования и ключ дешифрования – при условии, что исключается возможность определения содержимого ключа расшифровки, исходя из содержимого открыто передаваемого ключа шифрования. Диффи и Хеллман впервые представили эту идею на Национальной компьютерной конференции в 1976 году, а через несколько месяцев была опубликована их основополагающая работа «New Directions in Cryptography» («Новые направления в криптографии»).

Годом позже был изобретён первый алгоритм асимметричного шифрования RSA, который позволил решить проблему общения через незащищённый канал.

В 2002 году Мартин Хеллман писал: “Эта система … с тех пор известна под названием алгоритма Диффи-Хеллмана. Однако, когда система была впервые описана на бумаге Диффи и мной, это была система распространения открытых ключей, концепция которой была выработана Мерклом, и поэтому она должна называться „алгоритмом Диффи-Хеллмана – Меркла“, если её связывают с именами. Я надеюсь, что это небольшое изменение поможет признанию равного вклада Меркла в изобретение криптографии с открытыми ключами.”

В уже истёкшем патенте U.S. Patent 4 200 770 в качестве создателей данного алгоритма указано три автора: Хеллман, Диффи и Меркл.

Только в декабре 1997 года появилась обновлённая информация о том, что Малькольм Вильямсон уже в 1974 году изобрёл математический алгоритм, основанный на коммутативности показателей при последовательном возведении в степень $((b^x)^y = (b^y)^x = b^{xy}$. Данный метод можно назвать аналогом алгоритма Диффи-Хеллмана.

Описание алгоритма

Предположим, существует два абонента: Алиса и Боб. Обоим абонентам известны некоторые два числа g и p, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: Алиса – число a, Боб – число b. Затем Алиса вычисляет остаток от деления:

$$A = g^a mod\ p\ (1)$$

и пересылает его Бобу, а Боб вычисляет остаток от деления:

$$B = g^b mod\ p\ (2)$$

и передаёт Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть, у него нет возможности вмешаться в процесс передачи).

На втором этапе Алиса на основе имеющегося у неё a и полученного по сети B вычисляет значение:

$$B^a mod\ p = g^{ab} mod\ p\ (3)$$

Боб на основе имеющегося у него b и полученного по сети A вычисляет значение:

$$A^b\ mod\ p = g^{ab}\ mod\ p\ (4)$$

Как нетрудно видеть, у Алисы и Боба получилось одно и то же число:

$$K = g^{ab}\ mod\ p\ (5)$$

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой

(за разумное время) проблемой вычисления (3) или (4) по перехваченным, если числа p, a, b выбраны достаточно большими. Работа алгоритма показана на рисунке.

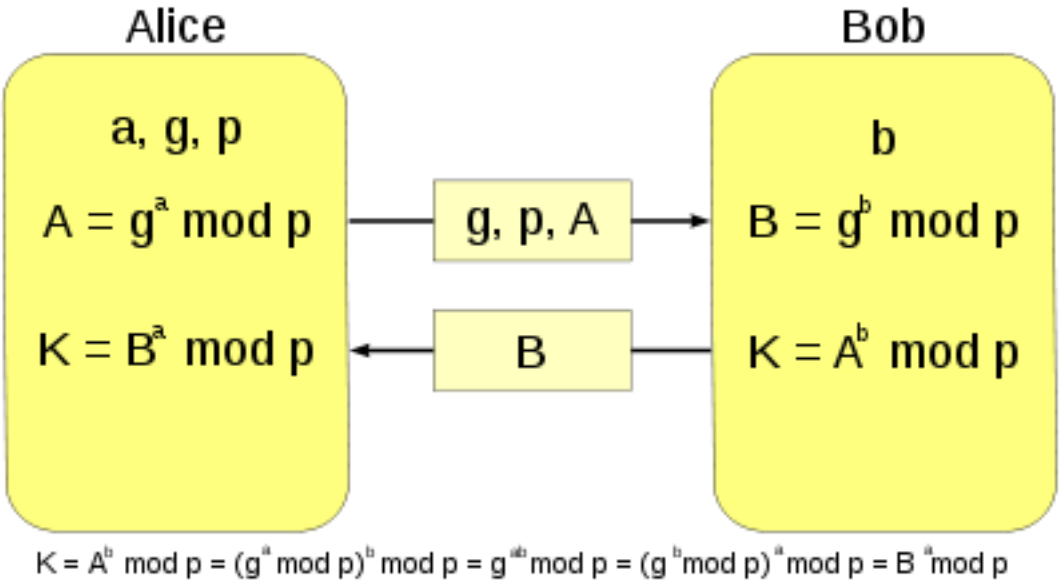

Рисунок 1 – Алгоритм Диффи-Хллмана, где K – итоговый общий секретный ключ

При работе алгоритма каждая сторона:

1. генерирует случайное натуральное число a – закрытый ключ
2. 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)
   - g является первообразным корнем по модулю p (также является простым числом)
3. вычисляет открытый ключ A, используя преобразование над закрытым ключом

- $A = g^a \bmod p$

4. обменивается открытыми ключами с удалённой стороной
5. вычисляет общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a
   - $K = B^a \bmod p$
   - K получается равным с обеих сторон, потому что:
   - $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$

В практических реализациях для a и b используются числа порядка 10^{100} и p порядка 10^{300}. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

Аутентификация

Стороны, используя криптоалгоритм с открытым ключом RSA, шифруют получившийся общий секретный ключ K (сессионный ключ). Далее они обмениваются своими открытыми ключами RSA и зашифрованными секретными ключами K'. Каждая сторона расшифровывает полученный зашифрованный ключ, используя свой закрытый ключ RSA, и сверяют, совпадает ли полученный ключ с сессионным ключом, сгенерированным данной стороной. Если сессионные ключи совпадают, то аутентификация прошла успешна, и стороны могут обмениваться зашифрованными с помощью этого сессионного ключа сообщениями. Иначе аутентификация не прошла.

Инструкция по использованию приложения

WEB

Аутентификация

1. При запуске создаются ключи и отображаются в двух полях (“Ваш публичный ключ” и “Ваш публичный ключ RSA”).
2. В следующих двух полях нужно ввести публичный ключ собеседника и публичный ключ RSA собеседника, на основе которых будет создан сессионный ключ
3. Нажать кнопку “Зашифровать сессионный ключ”. Откроется новая страница
4. В поле “Ваш зашифрованный сессионный ключ” будет отображаться ваш сессионный ключ, который нужно сообщить собеседнику.
5. В поле ниже нужно ввести зашифрованный сессионный ключ собеседника
6. Нажать на кнопку “Аутентифицировать”. Если после расшифровки сессионные ключ совпадут, то отобразится уведомление, что аутентификация прошла успешно.

Шифрование сообщения

1. Открыть сайт https://vyatsu.maxeem.ru/diffie-hellman или запустить index.html в браузере
2. Автоматически будет создан приватный и публичный ключ (публичный будет показан в интерфейсе)
3. Ввести публичный ключ собеседника в соответствующее поле
4. Ввести сообщение, которое нужно зашифровать
5. Нажать на кнопку "Расшифровать"
6. Зашифрованное сообщение будет выведено ниже

Расшифровка сообщения

1. Открыть сайт https://vyatsu.maxeem.ru/diffie-hellman или запустить index.html в браузере

2. Автоматически будет создан приватный и публичный ключ (публичный будет показан в интерфейсе)
3. Ввести публичный ключ собеседника в соответствующее поле
4. Ввести сообщение, которое нужно расшифровать
5. Нажать на кнопку "Расшифровать"
6. Расшифрованное сообщение будет выведено ниже

Вопросы для самопроверки

1) Какую проблему решает протокол Диффи-Хеллмана?
    a) распределение ключей
    b) конфиденциальность
    c) целостность
    d) аутентификация

2) Что такое аутентификация?
    a) процедура проверки роли
    b) процедура получения биометрии
    c) процедура проверки подлинности
    d) процедура чипирования

3) Диффи и Хеллман предложили использовать одностороннюю функцию с секретом для:
    a) Цифрового сообщения.
    b) Цифровой подписи.
    c) Цифрового ключа.
    d) Логина и пароля

4) Алгоритм Диффи-Хеллмана основан на трудности
    a) Возведения целых чисел в степень по модулю.
    b) Разложения больших чисел на множители.
    c) Решения задачи факторизации.
    d) Вычисления дискретных логарифмов.

5) Какой из следующих протоколов использует алгоритм Диффи-Хеллмана для установления защищенного соединения между клиентом и сервером?
    a) SSL/TLS
    b) SSH
    c) IPsec
    d) Все вышеперечисленные

6) Алгоритмы шифрования с открытым ключом по-другому называются
    a) симметричными алгоритмами шифрования
    b) односторонними алгоритмами шифрования
    c) помехоустойчивыми алгоритмами шифрования
    d) асимметричными алгоритмами шифрования

7) Какие два числа являются общедоступными параметрами алгоритма Диффи-Хеллмана?
    a) Основание и модуль
    b) Закрытый и открытый ключ
    c) Секретный ключ и хеш-функция
    d) Закрытый ключ и хэш-функция

8) Какой из следующих утверждений верен относительно алгоритма Диффи-Хеллмана?
    a) Он является симметричным алгоритмом шифрования
    b) Он является асимметричным алгоритмом шифрования
    c) Он является протоколом обмена ключами
    d) Он является протоколом цифровой подписи

Ответы

Номер вопроса	Правильный ответ
1	a

2	c
3	d
4	d
5	a
6	c
7	b
8	d