Федюшина Е.О.

ЗАДАЧА ДИФФИ-ХЕЛЛМАНА. Россия, Екатеринбург, УрГУПС

eleno4ka45@mail.ru

Безопасность систем шифрования зависит от конфиденциальности ключа, используемого в алгоритме шифрования, а не от хранения в тайне самого алгоритма. Многие алгоритмы шифрования общедоступны и были хорошо проверены благодаря этому. Цель данной работы: изучить алгоритм обмена ключей Диффи-Хеллмана, как пример шифрования с открытым ключом, и выявить его уязвимость.

Алгоритм Диффи­-Хеллмана (Diffie-Hellman, DH) – алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования.

Уитфилд Диффи и Мартин Хеллман разработали свою систему шифрования с открытым ключом в 1976 г. Система Диффи-Хеллмана разрабатывалась для решения проблемы распространения ключей при использовании систем шифрования с секретными ключами. Идея заключалась в том, чтобы применять безопасный метод согласования секретного ключа без передачи ключа каким-либо другим способом. Следовательно, необходимо было найти безопасный способ получения секретного ключа с помощью того же метода связи, для которого разрабатывалась защита. Алгоритм Диффи-Хеллмана нельзя использовать для шифрования или дешифрования информации.

Определим круг возможностей алгоритма. Предположим, что двум абонентам необходимо провести конфиденциальную переписку, а в их распоряжении нет первоначально оговоренного секретного ключа. Однако между ними существует канал, защищенный от модификации, то есть данные, передаваемые по нему, могут быть прослушаны, но не изменены. В этом случае две стороны могут создать одинаковый секретный ключ, ни разу не передав его по сети, по следующему алгоритму.

Предположим, что обоим абонентам известны некоторые два числа g и p (при этом p – простое число, а g – первообразный корень числа p). Они, впрочем, известны и всем остальным заинтересованным лицам. Например, они могут быть просто фиксированно "зашиты" в программное обеспечение. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют случайные или псевдослучайные простые числа: первый абонент – число a, второй абонент – число b. Затем первый абонент вычисляет значение и пересылает его второму, а второй вычисляет и передает первому. Злоумышленник получает оба этих значения, но модифицировать их (вмешаться в процесс передачи) не может. На втором этапе первый абонент на основе имеющегося у него a и полученного по сети y вычисляет значение ), а второй абонент на основе имеющегося у него b и полученного по сети x вычисляет значение . На самом деле операция возведения в степень переносима через операцию взятия модуля по простому числу (то есть коммутативна в конечном поле), то есть у обоих абонентов получилось одно и то же число: . Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник снова встретится с проблемой дискретного логарифмирования при попытке выяснить по перехваченным x и y сами числа a и b – это очень и очень ресурсоемкая операция, если числа g, n, a, b выбраны достаточно большими.

Необходимо еще раз отметить, что алгоритм Диффи-Хеллмана работает только на линиях связи, надежно защищенных от модификации. Если бы он был применим на любых открытых каналах, то давно снял бы проблему распространения ключей и, возможно, заменил собой всю асимметричную криптографию.

Следует заметить, что данный алгоритм уязвим для атак типа "man-in-the-middle". Если противник может осуществить активную атаку, т.е. имеет возможность не только перехватывать сообщения, но и заменять их другими, он может перехватить открытые ключи участников x и y, создать свою пару открытого и закрытого ключа и послать каждому из участников свой открытый ключ. После этого каждый участник вычислит ключ, который будет общим с противником, а не с другим участником. Если нет контроля целостности, то участники не смогут обнаружить подобную подмену. Осуществление такой атаки требует большого объема ресурсов, и в реальном мире такие атаки происходят редко.

Рассмотрим на примере алгоритм обмена ключей Диффи-Хеллмана и еще одну его уязвимость.

В качестве пользователей, которым нужно обменяться ключами выступают Алиса и Боб. Ева – криптоаналитик. Она читает пересылку Алисы и Боба, но не изменяет содержимого их сообщений.

Вначале Алиса и Боб публично определяют p и g. Например, p = 997 и g = 7 (7 – первообразный корень 997). Потом Алиса выбирает приватное число a = 221 и вычисляет и посылает этот результат публично Бобу. Боб выбирает свое приватное число b = 313 и вычисляет , и посылает результат публично Алисе. Алиса берет публичный результат Боба и возводит его в степень своего приватного числа, получает – общий секретный ключ. Боб берет публичный результат Алисы и возводит его в степень своего приватного числа – тот же самый общий ключ.

Итак, приватной является информация a = 221, b = 313 и k = 46. Публичная информация, которую может перехватить Ева: p = 997, g = 7, x = 652 и y = 661. Задача Евы узнать общий секретный ключ k. Если Ева определит a или b, она беспрепятственно сможет найти k. Определим, например a.

Для начала рассмотрим задачу дискретного логарифмирования:

, так как алгоритм Диффи-Хеллмана основан именно на нем. Так как во всех необходимых формулах присутствует mod – остаток от деления, необходима формула, раскрывающая его, то есть обратная mod. Выведем эту формулу. Например, возьмем n = 17 и a = 3 (3 – первообразный корень 17). И найдем степень 3, при которой остаток от деления на 17 будет равен, например, 13, т. е. . Зная смысл данного сравнения, сделаем вывод, что число 3b делится на 17 так, что получается некоторое количество целых частей (обозначим их s) и остаток c = 13. Тогда получаем новую формулу: . Для общего случая формула примет вид: . Отсюда b можно найти при помощи обычного логарифмирования: . И теперь остается найти такое s, при котором b будет целым числом.



|  |  |
| --- | --- |
| s | b |
| 1 | 3,095 |
| 2 | 3,505 |
| 3 | 3,786 |
| 4 | 4 |
| 5 | 4,173 |

Получаем b= 4 при s = 4. Проверим результат, составив таблицу всех степеней 3, и найдя остатки от деления на 17.

|  |  |  |  |
| --- | --- | --- | --- |
| b | c | b | c |
| 1 | 3 | 9 | 14 |
| 2 | 9 | 10 | 8 |
| 3 | 10 | 11 | 7 |
| 4 | 13 | 12 | 4 |
| 5 | 5 | 13 | 12 |
| 6 | 15 | 14 | 2 |
| 7 | 11 | 15 | 6 |
| 8 | 16 | 16 | 1 |

Действительно, при b= 4 остаток с = 13, т.е. .

Вернемся к задаче Диффи-Хеллмана и применим выведенные формулы в нашем случае. Заменим aна g и b на a, тем самым ab на ga, c на x, n на p. Получим . Отсюда . И выразим по уже известной формуле искомое a: .

Что касается переменной s. От чего зависит ее длина? Так как s – это число целых частей при делении ga на p (или gb на p), то чем меньше степени a и b, и соответственно ga или gb ближе к p, то тем меньше получится s. Рассмотрим пример, используя в качестве делимого произвольную переменную h, с дополнительным условием h1-p > h2-p:

p = 103, h1 = 13, тогда 7 целых частей и 12 в остатке.

p = 703, h2 = 13, тогда 54 целых часть и 1 в остатке.

Таким образом чем меньше ga -p (или gb-p) – тем меньше s.

Все необходимые формулы у нас есть, теперь можно вернуться к задаче нахождения a по известным p, g, x и y. Для этого составляем таблицу степеней g от 1 до n, при n ≤ p-1. Для каждого ga из этой таблицы находим s по формуле .Ответом окажется та степень а, при которой s – целое. В нашем случае s = 586099950684229201345256120579:: 364198169865551062770052620404291021600302359519520224669077237:: 486807350277769530967800344763226725491218205917157093115968811:: 86957846546597299763113697215. В данном примере s получилось очень большим, так как разница между ga и p довольно большая (ga = 7221, p = 997).

Подставим найденное s в формулу и получим а = 221.

Алисой в качестве a было выбрано число 221, с помощью данного алгоритма мы получили это же число. Зная a и y Ева может вычислить k. Аналогично можно вычислить b и найти k по b и x.

Распишем алгоритм нахождения a пошагово:

1. Составление таблицы степеней g от 1 до n при n ≤ p-1;
2. Нахождение s по формуле ;

1. Проверка целостности;
2. Нахождение a по формуле .

Какой бы ни была длина используемого ключа, количество операций останется равным 3.

Недостаток алгоритма: необходимость в калькуляторах, способных оперировать с большими числами, т.к. в алгоритме Диффи-Хеллмана считается надежным использовать 1024-битные ключи.

На практике алгоритм Диффи-Хеллмана применяется в совокупности с цифровой подписью, дабы обезопасить данные от подмены, которая может возникнуть при атаке «человек посредине», но в рассмотренном алгоритме это не играет важной роли, так как атака идет не при помощи подмены, а нахождения секретного ключа, при имеющейся публичной информации.

Список литературы:

1. Википедия, свободная энциклопедия / Дискретое логарифмирование. 7.08.2012. URL: [http://ru.wikipedia.org/wiki/Дискретное\_логарифмирование](http://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B5_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) (дата обращения: 15.10.2012)
2. Википедия, свободная энциклопедия / Алгоритм Диффи-Хеллмана. 9.10.2012. URL: [http://ru.wikipedia.org/wiki/Алгоритм\_Диффи\_—\_Хеллмана](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0) (дата обращения: 15.10.2012)
3. IT-сектор / Шифрование. 2010. URL: <http://it-sektor.ru/shifrovanie.html> (дата обращения: 24.10.2012)
4. Интернет университет информационных технологий / 7 лекция: Криптография с открытым ключом. 2011. URL: [http://www.intuit.ru/department/security/networksec/7/3.html](http://www.intuit.ru/department/security/networksec%20/7/3.html) (дата обращения: 21.10.2012)
5. Сайт Ильи Кантора. Алгоритмы. Методы. Исходники / Защита информации и ее взлом / Атаки / Временная атака. 2000 – 2012. URL: <http://algolist.manual.ru/defence/attack/timing.php> (дата обращения: 25.10.2012)
6. Беляев А.В. Курс лекций: «Методы и средства защиты информации» / Обмен ключами по алгоритму Диффи-Хеллмана. 30.11.2000. URL: <http://scanner.narod.ru/link/Safe/miszi/miszi9.htm> (дата обращения: 25.10.2012)
7. Учи IT! Коллекция учебников по IT / Криптография с открытым ключом. 2009. URL: <http://ychit.ru/2/2/7.html> (дата обращения: 25.10.2012)
8. Персональный компьютер / Алгоритм Диффи-Хеллмана. URL: <http://dammlab.com/bezopasnost-pk/kriptografiya/algoritmy-i-standarty-shifrovaniya/asimmetrichnoe-shifrovanie/algoritm-diffi-xellmana.html> (дата обращения: 25.10.2012)
9. Wolfram Alpha LLC – A Wolfram Research Company. 2012. URL: <http://www.wolframalpha.com> (дата обращения: 2.11.2012)