4

ISSN 1991-346X

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

NEWS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ФИЗИКА-МАТЕМАТИКА СЕРИЯСЫ

♦

СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКАЯ

♦

PHYSICO-MATHEMATICAL SERIES

5 (303)

ҚЫРКҮЙЕК – ҚАЗАН 2015 ж.
СЕНТЯБРЬ – ОКТЯБРЬ 2015 г.
SEPTEMBER – OCTOBER 2015

1963 ЖЫЛДЫҢ ҚАҢТАР АЙЫНАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С ЯНВАРЯ 1963 ГОДА
PUBLISHED SINCE JANUARY 1963

ЖЫЛЫНА 6 РЕТ ШЫҒАДЫ
ВЫХОДИТ 6 РАЗ В ГОД
PUBLISHED 6 TIMES A YEAR

АЛМАТЫ, ҚР ҰҒА
АЛМАТЫ, НАН РК
ALMATY, NAS RK

МАЗМҰНЫ

Аспан механикасының және жұлдыздар жүйесі динамикасының мәселелері

Жұлдыздарды және тұмандықтарды зерттеу

Күннің және күн жүйесіндегі денелердің физикасы

Теориялық және тәжірибелік зерттеулер

ATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
-MATHEMATICAL SERIES
-346X
Number 303 (2015), 133 – 140

ANALYSIS OF INFORMATION SECURITY TOOLS WITH PUBLIC KEY

A. M. Akhmetova[1], S.A. Nugmanova[2]

Committee of science Institute of information and computational technologies, Almaty, Kazakhstan,
[2]Kazakh National Pedagogical University named after Abai, Almaty, Kazakhstan.
E-mail: ardak_66@mail.ru, nugm_s@mail.ru

words: informative safety, confidentiality of information, open key, secret key, cryptography with the keys.

In the modern world informative safety becomes the major base element of all system of national state. It, foremost, is bound by growing like a weed technological possibilities of the modern information systems. A review and analysis of existent methods of defence of information a cryptographic method are examined.

Encipherement with the use of the symmetric key can help to keep secrets out of harm's way, but if it is necessary together to use secret information with other people, it is necessary also together to use the keys. But how to send to the keys other people? Some decisions are described in this article, including conception of cryptography with the open key.

To decide the task of distribution of the keys, it is possible to use cryptography with the open key, In an algorithm in cipher by means of the open key, can be deciphered only by means of the secret key. Safely to pass the secret key in the algorithm of Диффи-Хеллмана (DH) or Диффи-Хеллмана on elliptic curves (ECDH) it is possible to take advantage of technology of the open key, to form the together used secret. Only interactive parties create this secret value that after will be used.

16.02: 004.(574)

АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С ОТКРЫТЫМ КЛЮЧОМ

А. М. Ахметова[1], С. А. Нугманова[2]

Институт информационных и вычислительных технологии КН МОН РК, Алматы, Казахстан,
Казахский национальный педагогический университет им. Абая, Алматы, Казахстан

Ключевые слова: информационная безопасность, конфиденциальность информации, открытый ключ, секретный ключ, криптография с симметричными ключами.

Аннотация. В современном мире информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности любого государства. Это, прежде всего, связано быстро растущими технологическими возможностями современных информационных систем. В работе рассматривается обзор и анализ существующих методов защиты информации криптографическим методом.

Шифрование с использованием симметричного ключа может помочь сохранить секреты в безопасности, если нужно совместно использовать секретную информацию с другими людьми, необходимо также совместно использовать ключи. Но как безопасно отправлять ключи другим людям? В этой статье описаны возможные решения, включая концепцию криптографии с открытым ключом.

Чтобы решить задачу распределения ключей, можно использовать криптографию с открытым ключом, в алгоритме данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы только с помощью секретного ключа. Чтобы безопасно передать сеансовый ключ в алгоритме Диффи-Хеллмана (DH)

или Диффи-Хеллмана на эллиптических кривых (ECDH) можно воспользоваться технологией открытого ключа, чтобы сформировать совместно используемый секрет. Только взаимодействующие стороны могут создать это секретное значение, которое затем будет использоваться в качестве сеансового ключа.

Каждый из трех алгоритмов имеет преимущества и недостатки, поэтому нельзя сказать, какой из них лучше, чем другие, алгоритм подбирается для конкретного применения.

Введение. Современные методы накопления, обработки и передачи информации способствовали появлению угроз, связанных с возможностью потери, раскрытия, модификации данных, принадлежащих конечным пользователям. Несмотря на все возрастающие усилия по созданию технологий защиты данных, их уязвимость не только не уменьшается, но и постоянно возрастает. Человеческий ум всегда волновала проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом. Поэтому актуальность проблем, связанных с защитой потоков данных и обеспечением информационной безопасности их обработки и передачи, все более усиливается.

Под информационной безопасностью понимается состояние защищенности обрабатываемых, хранимых и передаваемых в информационно-телекоммуникационных системах данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищённости информационных ресурсов от воздействий, направленных на нарушение их работоспособности [1]. Одним из ключевых вопросов обеспечения безопасности информации, хранимой и обрабатываемой в информационных системах, а также передаваемой по линиям связи (для простоты далее по тексту будем говорить просто об информации), является защита ее от несанкционированного доступа. Для защиты информации применяются различные меры и способы, начиная с организационно-режимных и кончая применением сложных программно-аппаратных комплексов.Одним из путей решения проблемы защиты информации, а точнее - решения небольшой части вопросов из всего спектра мер защиты, является криптографическое преобразование информации, или шифрование [2]. Широкий круг применения криптографических методов в различных областях, связанных с обработкой, хранением, передачей, приемом, использованием данных и т.д.

Существует много публикации по данной теме. В исследовании [3] рассматриваются современные системы многоуровневой защиты информации, приводятся ключевые достоинства систем и обосновываются их недостатки, к таким системам предлагается комбинированный алгоритм для криптографического распределения ключей. В статье [4] описывается, разработанная в корпорации "Галактика" система ATCRYPT, предназначенная для защиты и сохранения целостности информации в распределенном хранилище данных при обменах по открытому каналу связи. В системе реализованы функции упаковки, шифрования, электронной подписи и аутентификации информации, а также предусмотрены возможности аудита, распределения и хранения ключей. В работе [5] освещаются актуальные вопросы защиты информации при создании и использовании распределенных корпоративных информационных систем и сетей масштаба предприятия. Особое внимание уделено проблемам обеспечения информационной безопасности и защите информации. Обсуждаются основные виды атак на компьютерные сети, а также методы и средства защиты локальных и корпоративных сетей от удаленных Internet-атак.

Постановка задачи. Необходимо провести обзор и анализ существующих средств защиты информации и рассмотреть решения проблем криптографии с открытым ключом.

В настоящее время криптографическое преобразование информации в форму, непонятную для посторонних, является универсальным и надежным способом ее защиты.

1. Криптографические методы. Криптографические методы традиционно используются для шифрования конфиденциальной информации, представленной в любой материальной форме в виде: письменных текстов; данных, хранящихся на гибком диске; сообщений, передаваемых в телекоммуникационных сетях; программного обеспечения, графики или речи, закодированных цифровыми последовательностями и т. п. Эти методы могут быть использованы и для многих других приложений, связанных с защитой информации, в частности, для обнаружения фактов вторжения в телекоммуникационную или компьютерную сеть и введения в нее имитирующих сообщений.

Криптографическое преобразование - это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом

и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоемкостью меньше заранее заданной.

Основным достоинством криптографических методов является обеспечение высокой гарантированной стойкости защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытиязашифрованной информации или вычисления ключей).

К числу основных недостатков криптографических методов следует отнести:

- значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
- трудности совместного использования зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределениеи т.д.);
- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

Криптография делится на два класса: криптография с симметричными ключами и криптография с открытыми ключами.

2. Криптография с симметричными ключами. В криптографии с симметричными ключами (классическая криптография) абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных.

Следует выделить следующие преимущества криптографии с симметричными ключами:

- относительно высокая производительность алгоритмов;
- высокая криптографическая стойкость алгоритмов на единицу длины ключа.

К недостаткам криптографии с симметричными ключами следует отнести:

- необходимость использования сложного механизма распределения ключей;
- технологические трудности обеспечения неотказуемости.

Для решения задач распределения ключей были использованы идеи асимметричности преобразований и открытого распределения ключей Диффи и Хеллмана.

В середине 70-х годов выпускник Стэнфорда Уитфилд Диффи и профессор Мартин Хеллман провели исследование криптографических методов вообще и проблемы распределения ключей в частности. Они предложили схему, в которой два человека могут создать совместно используемый секретный ключ путем обмена открытой информацией. Они могут связываться друг с другом по общедоступным телефонным линиям, отправляя информацию в форме, открытой для прослушивания, в то же время генерируя секретное значение, которое не делается общеизвестным. Обе стороны смогут использовать это секретное значение как симметричный сеансовый ключ. Такая схема получила название схемы Диффи–Хеллмана (DH).

Схема Диффи-Хеллмана решает проблему распределения ключей, но не шифрования. Это не делает ее непригодной; схема Диффи–Хеллмана используется и в настоящее время. Но эта схема не может быть использована для шифрования. Диффи и Хеллман опубликовали результаты своих исследований в 1976 г. В их статье обрисовывалась идея криптографии с открытым ключом (один ключ зашифровывает, другой расшифровывает). В 1977 г. Рон Ривест, Ади Щамир и Лена Эдлман разработали алгоритм, который реально мог шифровать данные. Они опубликовали алгоритм в 1978 г., и он стал известен как RSA по инициалам его авторов [6].

В 1985 г. два человека – Нил Коблиц из Вашингтонского университета и Виктор Миллер из исследовательского центра Уотсона корпорации IBM – работая независимо, сделали предположение, что малоизвестный раздел математики, посвященный так называемым эллиптическим кривым, может быть использован для реализации криптографии с открытым ключом. К концу 1990-х гг. алгоритмы этого класса начали повсеместно распространяться.

С 1977 г. (и с 1985 г.) многие исследователи разработали множество алгоритмов с открытым ключом. На сегодняшний день, тем не менее, наиболее широко используемым алгоритмом с открытым ключом для решения проблемы распределения ключей является RSA. Второе место занимает DH, а третье – алгоритмы на основе эллиптических кривых.

Шифрование с использованием симметричного ключа может помочь сохранить секреты в безопасности, но если нужно совместно использовать секретную информацию с другими людьми, необходимо также совместно использовать ключи. Но как безопасно отправлять ключи другим

людям? В этой статье мы опишем некоторые решения, включая концепцию криптографии с открытым ключом.

Менеджер компании может сохранить свои секреты путем шифрования данных с последующим хранением ключа шифрования в безопасном месте. Он хочет совместно использовать некоторые из своих секретов с другими людьми. Например, А имел встречу с потенциальным покупателем В, и хотел бы обсудить стратегию действий с Г, вице-президентом компании по продажам, боссом А. Обычно А и Г общаются по телефону, но в данном случае им нужно обмениваться документами, и они решили, что лучше всего это делать по электронной почте. Они хотели бы обезопасить обмен важными данными. Скорее всего, А для доступа в Internet придется подключать свой ноутбук к телефонной или локальной сети организации, где работает В, а кто сможет поручиться, что некие злоумышленники не подключились к телефонной сети компании.

Самым простым решением для А будет зашифровать файлы, которые он посылает Г. Таким образом, если В перехватит сообщение, она увидит лишь бессмысленный набор символов. Проблема в том, что когда сообщение дойдет до Г, она увидит тот же бессмысленный набор символов. Чтобы расшифровать сообщение, Г потребуется ключ. У А есть ключ, но как он может отправить его Г? Он не может отправить ключ в другом сообщении; если В способна перехватывать сообщение с данными, она также сможет перехватить и сообщение с ключом. Если А найдет канал, по которому можно безопасно отправить ключ, он может просто отправить свою секретную информацию по тому же каналу.

Проблема, вставшая перед А и Г, известна как проблема распределения ключей, состоящая в том, как двое или более людей могут безопасным образом передавать ключи по незащищенному каналу связи? Или, если обобщить, как могут люди безопасно передавать важную информацию по незащищенным каналам? Поскольку мы можем зашифровать данные, проблема сводится безопасной передачи ключа. Если у вас имеется 10 Мб важной информации, можно попытаться найти способ отправить эту информацию безопасным образом, либо можно зашифровать ее с использованием 128-битного симметричного ключа, а затем попытаться найти способ безопасным образом отправить ключ. Если вы решите проблему распределения ключей, то решите и проблему распространения основных данных.

Проблемы, свойственные данной схеме

А и Г теперь совместно владеют ключом. Эта схема будет работать; если атакующие не пытаются перехватить их сообщения, зашифрованные с использованием этого ключа, то они не смогут восстановить информацию. Но этому решению присущи недостатки.

Предположим, что несколько людей должны совместно использовать ключи. Чтобы безопасным образом взаимодействовать А придется посетить их и произвести обмен ключами. Каждому придется лично обменяться ключами с каждым, с кем он хочет совместно использовать конфиденциальную информацию.

Одно из решений состоит в использовании всеми сотрудниками компании одного ключа. В компании может быть «хозяин ключа», который выдаст ключ всем сотрудникам. Если же компания изменяет ключ, хозяину ключа придется повторно нанести визиты всем сотрудникам компании.

При совместном использовании ключа, если атакующие взламывают одно сообщение, они тем самым, взламывают все сообщения. Поскольку все сообщения, которыми обмениваются два человека, зашифрованы одним и тем же ключом, определение ключа для одного сообщения означает определение ключа для всех сообщений. С другой стороны, если возможно без особых затруднений использовать отдельный ключ для каждого сообщения, почему бы не воспользоваться этой дополнительной мерой безопасности? Хотя это и является недостатком, присущим подходу с совместным использованием ключа, с ним вполне можно примириться, учитывая неудобства, возникающие при попытке обмениваться ключами лично.

Проблемы безопасности

Предположим, А отправляет Г электронное сообщение с использованием цифрового конверта, а В перехватывает сообщение. Сможет ли В прочесть его? Основные данные были зашифрованы с помощью симметричного алгоритма, поэтому ей потребуется сеансовый ключ. Чтобы расшифровать данные, она может попытаться применить атаку методом прямого перебора, но если ее

битный, это займет миллиарды или даже триллионы лет. Но поскольку имеется сеансовый (он является частью самого сообщения), пй вряд ли понадобится применять эту атаку – если сеансовый ключ также не был зашифрован. Чтобы расшифровать сеансовый ключ, ей ходим ключ, парный открытому ключу, который был использован для дешифрования, по- это единственный ключ, способный расшифровать данные. Это секретный ключ, имеется только у Г.

Возможно, В сможет взломать алгоритм с открытым ключом или раскрыть секретный ключ с помощью прямого перебора. Вспомним, что существует два способа восстановить сообщения, зашифрованные с помощью шифрования с симметричным ключом: взлом алгоритма и нахождение ключа путем прямого перебора. То же самое справедливо и для шифрования открытым ключом. Если В сможет раскрыть секретный ключ, взломав алгоритм или воспользовавшись методом прямого перебора, она сможет расшифровать сеансовый ключ и использовать его для расшифровки основных данных.

Чтобы раскрыть секретный ключ, С должна найти 160-битное или 510-битное число. Если атака методом прямого перебора на 128-битное значение (симметричный ключ) представляется неосуществимой, то что говорить об атаке на 160-битный ключ? Таким образом, атаку методом прямого перебора на 160-битный или 510-битный ключ можно считать бесполезной.

Может ли быть взломан алгоритм с открытым ключом? Да, такой алгоритм может быть взломан путем определения секретного ключа на основе открытого ключа. Открытый и секретный ключи являются парой, они связаны между собой, а это соотношение является математическим. Для получения секретного ключа из открытого ключа могут быть использованы математические вычисления.

Как и для шифрования с симметричным ключом, чем длиннее открытый ключ, тем больше времени займет восстановления по нему секретного ключа. Если ключи достаточно длинные, подобные задачи займет столько же времени, сколько занимает атака методом прямого перебора при атаке на 96-битный или 28-битный ключ при симметричном шифровании.

Как работает криптография с открытым ключом

Рассмотрим как работает шифрование с симметричным ключом: используя ключ, последовательно выполняется процедура шифрования текущих данных. Чтобы расшифровать их, надо выполнять действия в обратном порядке. Если последним действием при зашифровывании был циклический сдвиг слова, первое, что делается при расшифровывании, – это циклический сдвиг зашифрованного слова в обратном направлении на то же самое число битов. Если ключ, использованный для шифрования данных, совпадает с ключом, применяемым при их расшифровании, то результат циклического сдвига будет тем же. (Если ключ неправильный, есть вероятность, что результат сдвига может остаться правильным, но все остальные дальнейшие операции, такие как XOR в одном месте и AND в другом месте, будут неверны.)

Но в криптографии с открытым ключом такая процедура не будет работать. Нельзя просто выполнить действия в обратном порядке. В то время как шифр с симметричным ключом просто оперирует данными как битами и преобразует их с помощью компьютерных операций, шифр с открытым ключом оперирует с данными как числами и выполняет действия над числами. А математические действия однонаправлены: они легко выполняются в одном направлении, но не в другом направлении. Фактически, основой любого хорошего алгоритма с открытым ключом является односторонняя функция, класс математических задач, на решении которых строится криптография с открытым ключом. Одностороннюю функцию можно сравнить с люком, который открывается лишь с одной стороны. Для всего остального мира функции являются односторонней, но секретный ключ действует как потайной люк, который дает возможность владельцу восстановить исходные данные.

Для решения задач распределения ключей и электронных цифровых подписей были использованы идеи асимметричности преобразований и открытого распределения ключей Диффи и Хеллмана [6].

В результате была создана криптография с открытыми ключами, в которой используется не один секретный, а пара ключей: открытый (публичный) ключ и секретный (личный, индивидуальный) ключ, известный только одной взаимодействующей стороне. В отличие от секретного ключа,

который должен сохраняться в тайне, открытый ключ может распространяться публично.Систе с открытыми ключами обладают с двумя свойствами, которые позволяют формировать защ рованные и аутентифицированные сообщения.

Схема шифрования данных с использованием открытого ключа состоит из двух этапов. первом из них производится обмен по несекретному каналу открытыми ключами. При этом не ходимо обеспечить подлинность передачи ключевой информации. На втором этапе, собствен реализуется шифрование сообщений, при котором отправитель зашифровывает сообще открытым ключом получателя. Зашифрованный файл может быть прочитан только владель секретного ключа, т.е. получателем. Схема расшифрования, реализуемая получателем сообще использует для этого секретный ключ получателя.

Эффективность защиты систем с помощью любых криптографических алгоритмов в зна тельной степени зависит от безопасного распределения ключей. Здесь можно выделить следую основные методы распределения ключей между участниками системы.

1) Метод базовых сеансовых ключей. Такой метод описан в стандарте ISO 8532 и испо зуется для распределения ключей симметричных алгоритмов шифрования. Для распределе ключей вводится иерархия ключей: головной ключ (так называемый мастер-ключ, или ключ ш рования ключей) и ключ шифрования данных (т.е. сеансовый ключ). Иерархия может быт двухуровневой: ключ шифрования ключей / ключ шифрования Старший ключ в этой иерар надо распространять неэлектронным способом, исключающим возможность его компромета Использование такой схемы распределения ключей требует значительного времени и зн тельных затрат.

2) Метод открытых ключей. Такой метод описан в стандарте ISO 11166 и может быть испо зован для распределения ключей как для симметричного, так и для асимметричного шифров С его помощью можно обеспечить надежное функционирование центров сертификации кл для электронной цифровой подписи на базе асимметричных алгоритмов и распреде сертификатов открытых ключей участников информационных систем. Кроме того, использов метода открытых ключей позволяет каждое сообщение шифровать отдельным кл симметричного алгоритма и передавать этот ключ с самим сообщением в зашифров асимметрическим алгоритмом.

Заключение. Надежная криптографическая система должна удовлетворять таким тр ваниям, как процедуры зашифровывания и расшифровывания должны быть "прозрачны пользователя; дешифрование закрытой информации должно быть максимально затруднено, а жание передаваемой информации не должно сказываться на эффективности криптографич алгоритма.

ЛИТЕРАТУРА

[1] Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник А государственного университета. – № 4 (108).– 2012.

[2] Аскеров Т.М. Защита информации и информационная безопасность: Учебное пособие / Под общей р К.И. Курбакова. - М.: Рос.экон. акад., 2001. 387 с.

[3] Лернер В.Д. Криптографическое распределение ключей для защиты информации в иерархических с Информационно-управляющие системы. № 5 (60), 2012

[4] Прикупец А. Защита информации в распределенном хранилище данных системы "Галактика" // «Откр темы», № 01, 1998

[5] Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и систем нистрирование и защита". – 2002.

[6] Диффи У., Хеллмен М. *Защищенность и имитостойкость. Введение в криптографию.* - ТИИЭР. *№ 3.-71-109 сс.*

[7] Фороузан Б.А. Криптография и безопасность сетей: учебное пособие / пер. с англ.; под ред. А.Н. Б Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2010. – 784 с.

[8] Нечаев В.И. Элементы криптографии (Основы теории защиты информации). – М.: Высшая школа, 1999

[9] Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – М.: Гелиос АРВ, 2002. – 240 с.

[10] Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия – Т 2002. – 175 с. – (Специальность. Для высших учебных заведений).

[11] Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – кн. 1, 2. М гоатомиздат, 1994.