ISSN 1991-346X

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Л А Р Ы

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

N E W S

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

«Известия НАН РК. Серия физико-математическая». ISSN 1991-346X
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5543-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год.
Тираж: 300 экземпляров.

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел.: 272-13-19, 272-13-18,
www:nauka-nanrk.kz / physics-mathematics.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 1991-346X
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 5543-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 300 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
www:nauka-nanrk.kz / physics-mathematics.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 5, Number 303 (2015), 133 – 140

ANALYSIS OF INFORMATION SECURITY TOOLS WITH PUBLIC KEY

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

[1]MES RK 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

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

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

An encipherement with the use of the symmetric key can help to keep secrets out of harm's way, but if it is needed together to use secret information with other people, it is necessary also together to use the keys. But how safely 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 data, in cipher by means of the open key, can be deciphered only by means of the secret key. Safely to pass the session 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 can create this secret value that after will be used.

УДК 378.016.02: 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, 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 описаны некоторые 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 90-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 попытаются 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 ключ

128-битный, это займет миллиарды или даже триллионы лет. Но поскольку имеется сеансовый ключ (он является частью самого сообщения), пй вряд ли понадобится применять эту атаку – если только сеансовый ключ также не был зашифрован. Чтобы расшифровать сеансовый ключ, ей необходим ключ, парный открытому ключу, который был использован для дешифрования, поскольку это единственный ключ, способный расшифровать данные. Это секретный ключ, имеется он 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 ключ 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, решение 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, используемый 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.Системы с открытыми ключами обладают с двумя свойствами, которые позволяют формировать зашифрованные и аутентифицированные сообщения.

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

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

1) Метод базовых сеансовых ключей. Такой метод описан в стандарте ISO 8532 и используется для распределения ключей симметричных алгоритмов шифрования. Для распределения ключей вводится иерархия ключей: головной ключ (так называемый мастер-ключ, или ключ шифрования ключей) и ключ шифрования данных (т.е. сеансовый ключ). Иерархия может быть и двухуровневой: ключ шифрования ключей / ключ шифрования Старший ключ в этой иерархии надо распространять неэлектронным способом, исключающим возможность его компрометации. Использование такой схемы распределения ключей требует значительного времени и значительных затрат.

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

Заключение. Надежная криптографическая система должна удовлетворять таким требованиям, как процедуры зашифровывания и расшифровывания должны быть "прозрачны" для пользователя; дешифрование закрытой информации должно быть максимально затруднено; содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма.

ЛИТЕРАТУРА

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

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

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

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

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

[6] Диффи У., Хеллмен М. *Защищенность и имитостойкость. Введение в криптографию. - ТИИЭР, 1976.- т. 67.- № 3.-71-109 сс.*

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

[8] Нечаев В.И. Элементы криптографии (Основы теории защиты информации). – М.: Высшая школа, 1999. – 109 с.

[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 – Телеком, 2002. – 175 с. – (Специальность. Для высших учебных заведений).

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

[12] Основы криптозащиты АСУ. Под ред. Б. П. Козлова. М.: МО, 1996.

[13] Конхейм А.Г. Основы криптографии. М.: Радио и связь, 1987.

[14] Венбо Мао. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. – М.: Вильямс, 2005. – 768 с.

[15] Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.

[16] Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.

[17] Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: «Лань», 2000.

[18] Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.

[19] Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004.

[20] Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. – 2-е изд. – М.: Горячая линия – Телеком, 2013. – 229 с.

[21] Вильям Столлингс. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001.

[22] Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1996.

[23] Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. –М.: Диалектика, 2004. – 432 с.

[24] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.

[25] Ященко В.В. Введение в криптографию. СПб.: Питер, 2001.

[26]Токарева Н.Н. Симметричная криптография. Краткий курс.

REFERENCES

[1] Aliyev M.F. Information security as an element of information *culture Bulletin of Adyghe state University,* 2012, 4 (108).

[2] Askerov T.M. data Protection and information security: the textbook Under the General editorship of K. I. Kurbatova. - M.: ROS.Econ. Acad., 2001. 387 p.

[3] Lerner V.D. distribution of Cryptographic keys to protect information in hierarchical systems *Information and control systems,* 2012, No. 5 (60)

[4] Prokopec A. Protection of information in a distributed data storage system "Galaxy" "Open systems", No. 01, 1998

[5] Shangin V.F., Sokolov A.V. Protection of information in distributed enterprise networks and systems*, "Administration and protection"*, 2002.

[6] W. Diffie, Hellman M. Safety and infotouriste. An introduction to cryptography. - TIER, 1976.- T. 67.- № 3.-71-109 SS.

[7] Forouzan B.A. Cryptography and network security: a training manual / per. s angl.; edited by A.N. Berlin. – M.: the Internet University of Information technologies: BINOM. Knowledge laboratory, 2010. – 784 p.

[8] V.I. Nechaev Elements of cryptography (fundamentals of the theory of information protection). – M.: Higher school, 1999. – 109 p.

[9] A.V. Babash, Sankin G. P. the History of cryptography. Part I. Moscow: Gelios ARV, 2002. – 240 p.

[10] Borichev S.G., Goncharov V.V., Serov, R.E. foundations of modern cryptography. – M.: Hot line – Telecom, 2002. – 175 p. – (the Specialty. For higher education institutions).

[11] Gerasimenko V.A. Protection of information in automated systems of data processing., kN. 1, 2. M.: Energoatomizdat, 1994.

[12] the Basics of encryption ACS. Ed. by B. P. Kozlov. M: MO, 1996.

[13] Konheim A.G. Fundamentals of cryptography. M.: Radio and communication, 1987.

[14] Wenbo Mao. Modern cryptography. Theory and practice = Modern Cryptography: Theory and Practice. – M.: Williams, 2005. – 768 p

[15] Mattick C. protection Mechanisms in computer networks. M.: Mir, 1993.

[16] Melnikov V.V. Protection of information in computer systems. M.: Finance and statistics, 1997.

[17] Construction Of A.A., Construction Of N.A. Advice B.Y. Cryptography. SPb.: "DOE", 2000.

[18] Y. Romanets V., Timofeev P.A., Shangin V.F. Protection of information in computer systems and networks. M.: Radio and communication, 1999.

[19] Ryabko B.Ya., Finow A.N. Basics of contemporary cryptography for specialists in information technologies. Moscow: Scientific world, 2004.

[20] Ryabko B.Ya., Finow A.N. Cryptographic methods of information protection. – 2nd ed. – M.: Hot line – Telecom, 2013. – 229 p.

[21] William Stallings. Cryptography and network security: principles and practice. M.; Williams, 2001.

[22] Uhrinov L.M. Management of information security in automated systems. M.: MEPhI, 1996.

[23] Niels Ferguson, Bruce Schneier. Practical cryptography = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. –M.: Dialectics, 2004. – 432 p.

[24] B. Schneier Applied cryptography. Protocols, algorithms, and source code in C = Applied Cryptography. Protocols, Algorithms and Source Code in C. – M.: Triumph, 2002. – 816 p.

[25] V.V. Yashchenko an Introduction to cryptography. SPb.: Piter, 2001.

[26]Tokareva N.N. Symmetric cryptography. Short course.

АШЫҚ КІЛТТІ АҚПАРАТТЫ ҚОРҒАУ ҚҰРАЛДАРЫНА ТАЛДАУ ЖАСАУ

А. М. Ахметова, С. А. Нұғманова

Ақпараттық және есептеу технологиялары институты, ҚР ҒК БҒМ, Алматы, Қазақстан,
Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан

Тірек сөздер: ақпараттық қауіпсіздік, ақпараттың конфиденциалдылығы, ашық кілт, құпия кілт, симметриялы кілті бар криптография.

Аннотация. Симметриялық кілтті пайдалану арқылы шифрлау мәліметтердің қауіпсіздігін сақтауға септігін тигізеді және ол басқа қолданушыға құпия ақпаратты білуге жол бермейді, сондай-ақ онымен қоса кілттерді пайдалануға болады. Бірақ басқа қолданушыға қалайша кілтті қауіпсіз жіберуге болады? Ашық кілттер криптографиясы осы мақалада қарастырылады.

Кілттерді үлестіру есебін шығару үшін ашық кілттер криптографиясын қарастыруға болады. Ашық кілтпен шифрлау деректер алгоритмі тек құпия кілтін пайдаланып қабылдамау мүмкін. Диффи-Хеллман (DH) немесе эллиптикалық қисықтағы Диффи-Хеллман (ECDH) алгоритміндегі қауіпсіз сессия кілтіне өту үшін, ортақ құпия қалыптастыру ашық кілт технологияларды пайдалануға болады. Тек өзара байланыс жасаушы тараптар бұл құпияның мәнін жасай алады, содан кейін сессия кілт ретінде пайдаланылуы мүмкін.

Әрбір үш алгоритмдердің артықшылықтары мен кемшіліктері бар, сондықтан бұл алгоритмдердің бір бірінен артықшылығы белгілі бір қолдану үшін таңдалады. Егер құпиясөздің кілттерін сақтайтын жоғалған құрылғыны ұмытылса криптографиялық кілттердің жоғалту мүмкіндігі бар. Сонымен қатар, ақпараттық шифрланған кілттерді қалпына келтіру керек болуы мүмін. Осы себептерге байланысты, көптеген ұйымдар қайта қалпына келтіру кілттерінің жоспарларын іске асыруда. Әдетте, қысқарту негізгі пайдалануды көздейді, ашық кілт қалпына келтіру агентті пайдаланып кілттерді шифрлайды.

Поступила 15.15.2015 г.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

http://www.physics-mathematics.kz

Редактор *М. С. Ахметова*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 25.09.2015.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
11,0 п.л. Тираж 300. Заказ 5.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19