УДК 004.056.5

ПРИНЦИПЫ КРИПТОГРАФИИ И МЕТОДЫ КРИПТОАНАЛИЗА В СОВРЕМЕННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ

М.А. Чарыева

Государственный энергетический институт Туркменистана, Мары, Туркменистан

Аннотация. Данная работа посвящена основам криптографии и криптоанализа, а также их применению для защиты информации в современных цифровых системах. В первой части рассматриваются основные понятия криптографии, включая цифровые подписи и криптографические хэш-функции, которые играют ключевую роль в обеспечении безопасности данных. Особое внимание уделяется алгоритмам цифровых подписей и методам создания хэш-значений, обеспечивающим целостность и подлинность сообщений. Вторая часть работы фокусируется на криптоанализе и различных типах атак на криптосистемы, таких как атака с подставкой, атака с использованием таймера и атака с знанием зашифрованного текста. Описываются способы защиты от этих атак, а также примеры использования криптографических методов в реальных приложениях, таких как электронные подписи и системы аутентификации. Работа направлена на освещение теоретических основ криптографии и практических методов защиты информации, актуальных в условиях современного цифрового мира.

Ключевые слова: цифровые подписи; криптоанализ; криптосистемы; атака.

PRINCIPLES OF CRYPTOGRAPHY AND METHODS OF CRYPTOANALYSIS IN MODERN SECURITY SYSTEMS

M.A. Charyyeva

The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Abstract. This work is dedicated to the fundamentals of cryptography and cryptanalysis, as well as their application for information protection in modern digital systems. The first part discusses the basic concepts of cryptography, including digital signatures and cryptographic hash functions, which play a key role in ensuring data security. Special attention is given to digital signature algorithms and methods of creating hash values, which ensure the integrity and authenticity of messages. The second part of the work focuses on cryptanalysis and various types of attacks on cryptosystems, such as man-in-the-middle attacks, timing attacks, and ciphertext-only attacks. Methods of defense against these attacks are described, as well as examples of using cryptographic methods in real applications, such as digital signatures and authentication systems. The work aims to highlight

the theoretical foundations of cryptography and practical methods of information protection relevant in the modern digital world.
Keywords: digital signatures; cryptanalysis; cryptosystems; attack.

Введение

Криптография – это наука о том, как обеспечить секретность сообщения. Криптоанализ – это наука о том, как вскрыть шифрованное сообщение, то есть как извлечь открытый текст не зная ключа. Криптографией занимаются криптографы, а криптоанализом занимаются криптоаналитики.

Криптография покрывает все практические аспекты секретного обмена сообщениями, включая аутенфикацию, цифровые подписи, электронные деньги и многое другое. Криптология - это раздел математики, изучающий математические основы криптографических методов.

Цифровые подписи

Некоторые из асимметричных алгоритмов могут использоваться для генерирования цифровой подписи. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу). Также подписи используются для проставления штампа времени (timestamp) на документах: сторона, которой мы доверяем, подписывает документ со штампом времени с помошью своего секретного ключа и, таким образом, подтверждает, что документ уже существовал в момент, объявленный в штампе времени.

Цифровые подписи также можно использовать для удостоверения (сертификации – to certify) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим a-priori, что ему можно доверять). В централизованной инфраструктуре ключей имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агенства; их также называют сертификационными агенствами - certification authorities). В распределенной инфраструктуре нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название сети доверия (web of trust) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый дайджест (message digest) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или

иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA.

Криптографические хэш-функции

Криптографические хэш-функции используются обычно для генерации дайджеста сообщения при создании цифровой подписи. Хэш-функции отображают сообщение в имеющее фиксированный размер хэш-значение (hash value) таким образом, что все множество возможных сообщений распределяется равномерно по множеству хэш-значений. При этом криптографическая хэш-функция делает это таким образом, что практически невозможно подогнать документ к заданному хэш-значению.

Криптографические хэш-функции обычно производят значения длиной в 128 и более бит. Это число значительно больше, чем количество собщений, которые когда-либо будут существовать в мире.

Много хороших криптографических хэш-функций доступно бесплатно. Широко известные включают MD5 и SHA.

Криптоанализ и атаки на криптосистемы

Криптоанализ – это наука о дешифровке закодированных сообщений не зная ключей. Имеется много криптоаналитических подходов. Некоторые из наиболее важных для разработчиков приведены ниже.

Атака со знанием лишь шифрованного текста (ciphertext-only attack). Это ситуация, когда атакующий не знает ничего о содержании сообщения, и ему приходтся работать лишь с самим шифрованным текстом. На практике, часто можно сделать правдоподобные предположения о структуре текста, поскольку многие сообщения имеют стандартные заголовки. Даже обычные письма и документы начинаются с легко предсказумой информации. Также часто можно предположить, что некоторый блок информации содержит заданное слово.

Атака со знанием содержимого шифровки (known-plaintext attack): Атакующий знает или может угадать содержимое всего или части зашифрованного текста. Задача заключается в расшифровке остального сообщения. Это можно сделать либо путем вычисления ключа шифровки, либо минуя это.

Атака с заданным текстом (chosen-plaintext attack): Атакующий имеет возможнот получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Некоторые методы шифрования и, в частности, RSA, весьма уязвимы для атак этого типа. При использовании таких алгоритмов надо тщательно следить, чтобы атакующий не мог зашифровать заданный им текст.

Атака с подставкой (Man-in-the-middle attack): Атака направлена на обмен шифрованными сообщениями и, в особенности, на протокол обмена ключами. Идея заключается в том, что когда две стороны обмениваются ключами для секретной коммуникации (например, используя шифр Диффи-Хелмана, Diffie-Hellman), противник внедряется между ними на линии обмена сообщениями. Далее противник

выдает каждой стороне свои ключи. В результате, каждая из сторон будет иметь разные ключи, каждый из которых известен противнику. Теперь противник будет расшифровывать каждое сообщение своим ключом и затем зашифровывать его с помощью другого ключа перед отправкой адресату. Стороны будут иметь иллюзию секретной переписки, в то время как на самом деле противник читает все сообщения.

Одним из способов предотвратить такой тип атак заключается в том, что стороны при обмене ключами вычисляют криптографическую хэш-функцию значения протокола обмена (или по меньшей мере значения ключей), подписывают ее алгоритмом цифровой подписи и посылают подпись другой стороне. Получатель проверит подпись и то, что значение хэш-функции совпадает с вычисленным значением. Такой метод используется, в частности, в системе Фотурис (Photuris).

Атака с помощью таймера (timing attack): Этот новый тип атак основан на последовательном измерении времен, затрачиваемых на выполнение операции возведения в степень по модулю целого числа. Ей подвержены по крайней мере следующие шифры: RSA, Диффи-Хеллман и метод эллиптических кривых.

Имеется множество других криптографических атак и криптоаналитических подходов.

Заключение

На сегодняшний день криптоанализ играет ключевую роль в обеспечении безопасности данных. С развитием технологий и криптографических алгоритмов, таких как RSA и AES, появляются новые методы взлома и атаки. Криптоанализ помогает выявлять уязвимости в системах и улучшать их защиту. Современные криптографические исследования направлены на создание более устойчивых алгоритмов, способных противостоять сложным методам анализа и атакам, обеспечивая высокую степень безопасности в цифровом мире.

Список использованных источников

1. Кауфман, Ч. "Криптография и безопасность компьютерных систем". – М.: Издательство «Наука», 2018.

2. Шиффман, Д. "Введение в криптографию". – М.: Издательство «Речи», 2017.

3. Меркель, П. «Цифровые подписи и защита данных». – М.: Издательство «Диалектика», 2015.

4. Цицилин, М. В., Кузнецов, В. В. "Современные методы криптографического анализа". – СПб.: Издательство «Питер», 2020.

References

1. Kaufman, C. "Cryptography and Computer System Security." – Moscow: "Nauka" Publishing House, 2018.

2. Shiffman, D. "Introduction to Cryptography." – Moscow: "Rechi" Publishing House. 2017.

3. Merkel, P. "Digital Signatures and Data Protection." – Moscow: "Dialektika" Publishing House. 2015.

4. Ttsitsilin, M. V., Kuznetsov, V. V. "Modern Methods of Cryptographic Analysis." – St. Petersburg: "Piter" Publishing House. 2020.

Сведения об авторах

Чарыева М.А., преподаватель, Государственный энергетический институт Туркменистана, annageldievamaysa@gmail.com.

Information about the authors

Charyyeva M., Teacher, The State Energy Institute of Turkmenistan, annageldievamaysa@gmail.com.