УДК 004.01

Научный руководитель Катасонов Александр Игоревич,
ассистент кафедры «Защищенные системы связи»
Санкт-Петербургский государственный университет телекоммуникаций
имени профессора Михаила Александровича Бонч-Бруевича
Россия, г. Санкт-Петербург
Лянгузов Никита Алексеевич,
Студент
1 курс, факультет «Инфокоммуникационные сети и системы»
Санкт-Петербургский государственный университет
телекоммуникаций имени профессора Михаила Александровича Бонч-
Бруевича
Россия, г. Санкт-Петербург

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: *в статье рассматриваются различные методы криптографической защиты информации, их принципы работы, отличия друг от друга, преимущества и недостатки. Также в статье даны понятия хеш-функции и криптостойкости.*

Ключевые слова: *криптография, защита, информация, криптосистема, симметричная система, ассиметричная система, гибридная система, хеш-функция, криптостойкость.*

Annotation: *the article discusses various methods of cryptographic information protection, their principles of operation, differences from each other, advantages and disadvantages. The article also provides the concepts of hash functions and cryptographic strength.*

Keywords: *cryptography, security, information, cryptosystem, symmetric system, asymmetric system, hybrid system, hash function, cryptographic stability.*

Криптографический метод защиты информации — это метод шифрования информации, после применения которого ее содержание становится недоступным для лиц, не имеющих к ней доступа.

При криптографическом методе защищается информация, а не доступ к ней, что делает этот метод одним из самых надежных. Этот метод защиты реализуется в виде отдельных программ или пакетов программ.

Криптография — наука о различных методах обеспечения конфиденциальности данных, их целостности, аутентификации и невозможности отказа от авторства.

Конфиденциальность — это защита информации таким образом, чтобы доступ к ней имело только авторизированное лицо.

Целостность данных — невозможность изменения данных лицами, не имеющих на это прав.

Аутентификация — проверка подлинности пользователя. Обычно для этого пользователю нужно ввести логин и пароль.

Невозможность отказа от авторства — пользователь не может отказаться от действий, которые он совершил.

В современной криптографии можно выделить симметричные и ассиметричные криптосистемы.

1. Симметричные криптосистемы

Симметричная криптосистема — система, в которой для шифрования и расшифровки информации используется один и тот же ключ (Рисунок 1). Эта система чаще всего используется для шифрования информации, которая не должна никуда отправляться и храниться на каком-нибудь накопителе.

Ключ — информация (чаще всего определенная последовательность символов), которая используется для шифрования или расшифровки сообщений, преобразованных определенным алгоритмом.

Рисунок 1. Симметричный алгоритм шифрования

1.1. Преимущества

Симметричные криптосистемы, созданные раньше асимметричных, отличаются более глубокой изученностью. Они характеризуются простотой внедрения и высокой скоростью шифрования/расшифровки данных. Такая эффективность обусловлена использованием более коротких ключей, а также применением единого ключа для обеих операций.

1.2. Недостатки

В симметричных системах для шифрования и расшифровки данных используется один и тот же ключ. Это означает, что как отправителю, так и получателю необходимо хранить ключ в секрете и передавать его друг другу безопасным способом. Если злоумышленникам удастся получить ключ, они получат доступ к любым данным, зашифрованным с его помощью.
Поскольку в симметричных системах отсутствует закрытый ключ, их нельзя использовать для создания электронной подписи. Это ограничивает сферу их применения, особенно для передачи конфиденциальных сообщений, где критически важна конфиденциальность и безопасность.

2. Ассиметричные криптосистемы

Криптосистема с открытым ключом или ассиметричная криптосистема — система, которая использует сразу пара ключей: открытый и закрытый.

Информация, которую нужно передать, шифруется с помощью открытого ключа и расшифровывается получателем с помощью закрытого (Рисунок 2).

Открытый ключ является известным и доступен всем, в то время как закрытый ключ есть только у тех лиц, которые должны иметь доступ к зашифрованной информации.

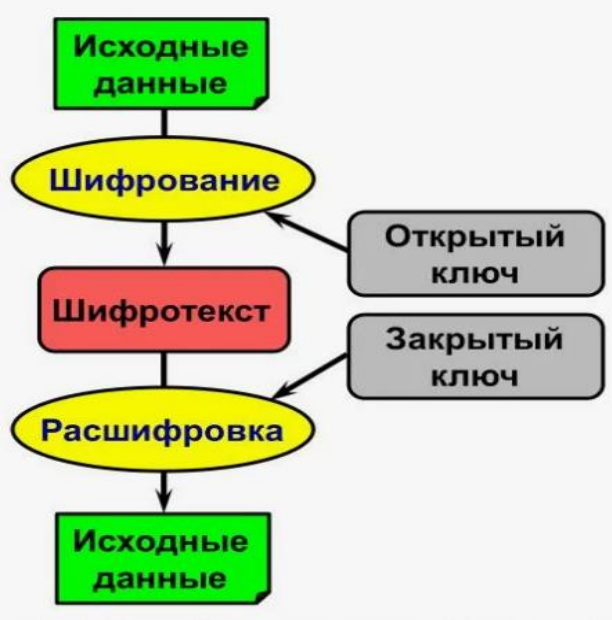

Рисунок 2. Ассиметричный алгоритм шифрования

2.1. Преимущества

В отличие от симметричных систем ассиметричные системы могут качественно обеспечить конфиденциальность и аутентификацию. Так же они имеют возможность использоваться для систем электронной подписи за счет использования разных ключей имеют более высокую надежность. Могут использоваться при создании электронной подписи.

2.2. Недостатки

Из-за наличия двух ключей ассиметричные криптосистемы имеют более сложную реализацию, так как требуют управления сразу парой ключей. Поэтому таким системам нужно больше времени на выполнение алгоритма.

В таблице 1 представлено сопоставление ключей симметричной и ассиметричной криптосистемы с одинаковой криптостойкостью — устойчивостью ко взлому.

Таблица 1. Сравнение длин ключей.

Длина ключа симметричной системы, бит	Длина ключа ассиметричной системы , бит
128	2048
192	3072
256	4096
384	6144
512	8192
768	12288
1024	16384

3. Гибридная криптосистема

Отдельного внимания в защите информации заслуживает гибридный метод, который получается при объединении симметричного и ассиметричного методов.

Гибридная криптосистема — это система шифрования, совмещающая симметричные и ассиметричные алгоритмы в собственных (Рисунок 3).

В этом случае ключ шифруется ассиметричным алгоритмом, а само сообщение — симметричным. Получателю нужно сначала расшифровать ключ, а только потом с его помощью — сообщение. Такие алгоритмы совмещают в себе скорость выполнения симметричных систем и надежность ассиметричных.

Рисунок 3. Гибридный алгоритм шифрования

4. Хеш-функции

Еще одним методом криптографической защиты являются хеш-функции. Их особенность заключается в том, что они не обратимы. Это значит, что преобразованные ими данные нельзя преобразовать обратно. В результате своей работы они выдают хеш-код — численное значение фиксированной длины. Хеш-код позволяет однозначно идентифицировать данные.

Если несколько раз преобразовать сообщение с помощью хеш-функции, то результат будет получаться одинаковый. Но если в исходное сообщение внести какое-либо изменение, то и хеш-код получится совершенно другой.

С помощью хеш-функций можно проверить, вносились ли какие-либо изменения в документ с момента его хеширования. Это очень полезно при использовании систем электронных подписей.

5. Криптостойкость

Симметричные и ассиметричные системы имеют такую характеристику, как криптостойкость. Она отвечает за сложность получения несанкционированного доступа.

По криптостойкости системы делятся на два вида: абсолютно стойкая система и достаточно стойкая система.

Абсолютно стойкая система не позволяет расшифровать сообщение без ключа даже при наличии больших вычислительных мощностей. В ней для каждого сообщения генерируется свой отдельный ключ, длина которого равна длине сообщения либо больше. Это обеспечивает дополнительную защиту.

Достаточно стойкие системы сложно взломать, но при наличии соответствующих ресурсов это становится возможно. Надежность таких систем определяется возможностями специалиста по криптоанализу.

Вывод

Криптографические технологии дают возможность кодировать и декодировать информацию, а также обеспечивают управление электронной цифровой подписью.

Криптография состоит из двух основных методов: симметричный и ассиметричный, которые чаще всего объединяются в гибридный метод, который сочетает в себе скорость и надежность симметричного и ассиметричного методов соответственно.

Используя хеш-функции можно зашифровать данные в уникальную последовательность так, чтобы их было невозможно расшифровать.

Литература

1.Что такое шифрование? [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/encryption (дата обращения: 14.07.2024)

2. Информационная безопасность. Конфиденциальность. [Электронный ресурс]. URL: https://www.geeksforgeeks.org/information-security-confidentiality/ (дата обращения: 14.07.2024)

3.Идентификация и аутентификация. [Электронный ресурс]. URL: https://brobank.ru/identifikaciya-i-autentifikaciya/ (дата обращения: 14.07.2024)

4.Недостатки симметричных криптосистем и принципы асимметричного шифрования. [Электронный ресурс]. URL: https://studopedia.org/1-29121.html (дата обращения: 14.07.2024)

5.Сравнение симметричного и асимметричного шифрования. [Электронный ресурс]. URL: https://academy.binance.com/ru/articles/symmetric-vs-asymmetric-encryption (дата обращения: 14.07.2024)

6.Что такое СКЗИ и для чего нужны средства криптографической защиты. [Электронный ресурс]. URL: https://skillbox.ru/media/code/chto-takoe-skzi-i-dlya-chego-nuzhny-sredstva-kriptograficheskoy-zashchity/ (дата обращения: 14.07.2024)

7.Симметричное и асимметричное шифрование. [Электронный ресурс]. URL: https://fb.ru/article/393115/simmetrichnoe-i-asimmetrichnoe-shifrovanie-opredelenie-ponyatiya-primenenie-primeryi (дата обращения: 14.07.2024)