УДК 004.4 **Информационные технологии**

Палаш Борис Викторович, *студент,*
Хакасский государственный университет им. Н.Ф. Катанова
Голубничий Артем Александрович, *научный руководитель,*
старший преподаватель кафедры программного обеспечения
вычислительной техники и автоматизированных систем
Хакасский государственный университет им. Н.Ф. Катанова

ОСНОВНЫЕ ПРИНЦИПЫ РАБОТЫ СИСТЕМ ШИФРОВАНИЯ

Аннотация: Информация, важнейший ресурс современного мира, защита которой стоит на лидирующих позициях списка современных проблем. Самым простым способом обеспечения целостности и безопасности данных является применение современных методов шифрования, но для правильного их использования необходимо точно знать принципы работы данных систем.

Ключевые слова: шифрование, ключи, образование, защита.

Abstract: Information, the most important resource of the modern world, the protection of which is at the top of the list of modern problems. The easiest way to ensure data integrity and security is to use modern encryption methods, but to use them correctly, you need to know exactly how these systems work.

Keywords: encryption, keys, education, security.

С развитием информационных технологий информация стала главной ценностью современного мира. С каждым годом вопрос защиты данных становится все актуальнее, самым простым и надежным способом обеспечения безопасности информации является ее шифрование.

Шифрование – это обратимое искажение данных с целью ограничения доступа для не авторизованных пользователей. Главной целью применения

шифрования является соблюдение конфиденциальности передаваемых данных. Еще одним важным условием шифрования является соблюдение целостности данных, это означает что данные до шифрования и после расшифровки должны быть полностью идентичны. Во всех видах шифрования важную роль занимают так называемые «ключи шифрования». Ключ — это информация, которая использовалась в процессе шифрования.

На текущий момент существует большое количество различных методов шифрования информации, однако все они разделяются на два основных вида:

1. Симметричное шифрование – это метод, в котором для шифрования и расшифровывания данных используется один и тот же ключ. В таком алгоритме ключ должен быть заранее известен обеим сторонам [1]. Принцип работы данного алгоритма представлен на рисунке 1.

2. Ассиметричное шифрование – метод, в котором для шифровки и расшифровки используются разные ключи. При таком подходе передается лишь один публичный ключ [1].

Рисунок 1 – принцип работы симметричного шифрования.

Самым наглядным примером использования симметричного шифрования является «Энигма», это шифровальная машина, используемая нацисткой Германией с декабря 1932 года. В работе машины использовался самый простой метод шифрования «метод замены» [2]. Данный метод является одним из видов симметричного шифрования в его основе лежит символьная таблица, пример которой представлен на рисунке 2. В примере буквы алфавита заменены числовыми значениями. Используя аналогичную таблицу замены «Энигма»

осуществляла шифрование сообщения, для дешифровки которого необходима исходная таблица.

А	Б	В	г	д	Е	Ж	З	и	Й	К	Л	м	Н	О	П	Р
09	23	01	04	07	02	14	13	21	31	17	25	29	06	22	11	26
С	Т	У	Ф	Х	Ц	Ч	ш	Щ	ъ	Ы	Ь	Э	Ю	Я		
00	19	30	08	18	16	28	03	27	32	15	10	20	24	12	05	

Рисунок 2 – Пример ключа для метода «замена».

Сам по себе такой метод шифрования довольно ненадежен, однако с увеличением количества роторов машина сильно повышала сложность шифрования. В современных реалиях, вычислительные мощности даже персональных компьютеров позволяют произвести дешифровку таких сообщений за довольно короткий промежуток времени.

Ассиметричное же шифрование в отличии от своего предшественнике является довольно сложным в реализации. Принцип работы данной системы показан на рисунке 3.

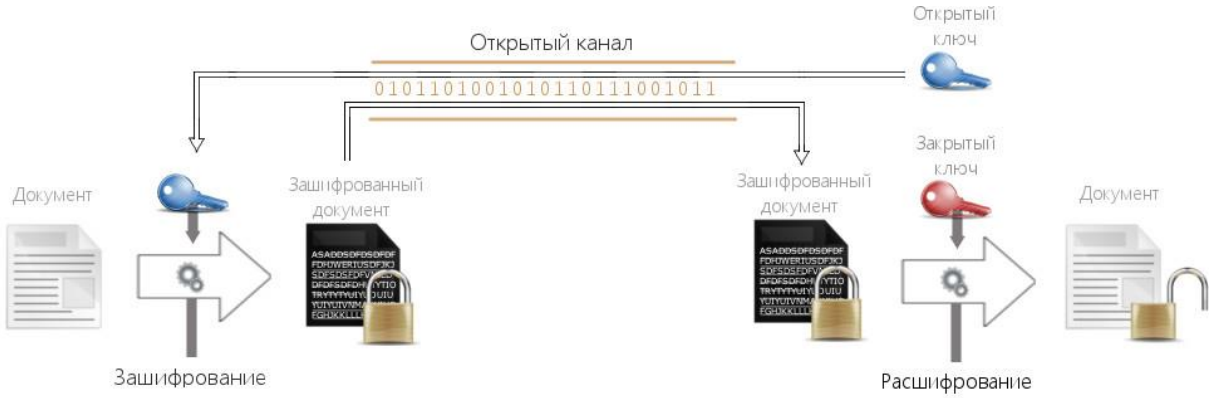

Рисунок 3 – принцип работы асимметричного шифрования.

При реализации такой системы создаются два ключа связанные между собой математическим способом. Один из ключей является публичным и используется для шифрования сообщения и проверки электронной подписи шифровальщика. Довольно часто такой ключ передается напрямую через открытый канал связи, так как не представляет сильной ценности при перехвате.

Второй же ключ представляет наибольшую ценность, так как используется при расшифровке сообщения. Такой подход решает главную уязвимость симметричного шифрования, а именно зная алгоритм шифрования злоумышленник может как просматривать информацию, так и вносить в нее правки. В системе же асимметричного шифрования зная метод шифрования возможно только зашифровать сообщение, но не расшифровать его. Применение такого вида шифрования довольно обширно, от менеджеров паролей до военного применения.

Обеспечение безопасности информации является важнейшей задачей. Незащищенная информация может привести к серьезным проблемам в повседневной жизни людей. Незащищенные банковские переводы или отсутствие электронных подписей могут существенно подорвать как работу крупных компаний, так и целых стран. Рассмотрев основные типы реализации шифрования, можно сделать вывод о целесообразности использования каждой из них в зависимости от ситуации. В случае реализации единичных шифровании и существовании способа безопасной передачи ключей возможно использование простого в реализации метода симметричного шифрования. Если отсутствует безопасная возможность передачи и система должна соответствовать высочайшему классу надежности, то единственным вариантом для использования становится ассиметричная система шифрования. Которая при достаточном наборе шифрования способна защитить информацию на десятки и сотни лет вперед, даже с учетом, постоянно растущих вычислительных мощностей.

Библиографический список:

1. Криптография и главные способы шифрования информации – URL: https://proglib.io/p/methods-of-encryption (дата обращения: 10.01.2020).

2. Криптография от папируса до компьютера – URL: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 12.01.2020).