УДК 004.9

ВЫБОР ОПТИМАЛЬНОГО МЕТОДА ШИФРОВАНИЯ ДАННЫХ

Пичужкина Д.Ю., Поначугин А.В.

Нижегородский государственный педагогический университет имени Козьмы Минина

Потребность в защите информации появилась ещё задолго до появления понятия «информация», но с развитием технологий всё сложнее становится её осуществлять. Одним из самых первых и известных методов шифрования являются Шифр Цезаря, Шифр Павсания, Атбаш, которые нужны были для того, чтобы враг не мог прочитать тайные послания. Современными криптографами считаются итальянский ученый Леон Альберти и немецкий аббат Иоганна Тритемия, а также Мария Стюарт, Христофор Колумб, Эрнан Кортес, Томас Джефферсон. Также говоря о защите информации и системе шифрования нельзя не сказать о создании такого изобретения как «Энигма», что и стало самым большим прорывом в данной области.

Целью статьи является рассмотреть базовые знания по методам шифрования, которые потребуется для начала работы с алгоритмами шифрования.

Задачи исследования:

- понять схему шифрование данных;
- рассмотреть основные понятия, которые характеризуют методы шифрования;
- рассмотреть основные методы шифрования (симметричный и асимметричный).

В данной статье был проведён сравнительный анализ алгоритмов шифрования как DES, IDEA, Bluwfish, так и RSA, DSA, Шифр Эль-Гамаля, а также выведены достоинства и недостатки симметричного и асимметричного метода шифрования.

Ключевые слова: шифрования, киберпреступления, симметрический метод шифрования, асимметрический метод шифрования, безопасность, программное обеспечение.

THE OPTIMUM METHOD OF DATA ENCRYPTION

Pichuzhkina D.Yu., Ponachugin A.V.

The need to protect information appeared even long before the emergence of the concept of “information”, but with the development of technology, it becomes increasingly difficult to implement it. One of the first and most well-known encryption methods is Caesar's Cipher, Pausanius's Cipher, Atbash, which were necessary so that the enemy could not read the secret messages. The modern cryptographers are the Italian scholar Leon Alberti and the German abbot Johann Trithemius, as well as Mary Stuart, Christopher Columbus, Hernan Cortes, Thomas Jefferson. Also speaking about the protection of information and the encryption system, one cannot but say about the creation of such an invention as “Enigma”, which was the biggest breakthrough in this field.

The purpose of the article is to examine the basic knowledge of the encryption methods that will be required to begin working with encryption algorithms.

Objectives of the study:

- understand the data encryption scheme;
- consider the basic concepts that characterize encryption methods;
- consider the basic encryption methods (symmetric and asymmetric).

In this article, a comparative analysis of encryption algorithms like DES, IDEA, Bluwfish, and RSA, DSA, Cipher El-Gamal was conducted, and the advantages and disadvantages of a symmetric and asymmetric encryption method were derived.

Keywords: encryption, cybercrime, symmetric encryption method, asymmetric encryption method, security, software.

В век роста киберпреступлений главной целью шифрования является сохранность информации. Система шифрования позволяет работать с данными из ненадежных источников, передавать сообщения по незащищенным каналам. Отправка информации происходит так: отправитель шифрует данные, а получатель расшифровывает их, но для прочтения полученного сообщения требуется дешифратор.

Существует два метода шифрования: симметричный и ассиметричный, а также такие понятия, как криптостойкость и ключ [2].

Криптостойкость - это способность алгоритма противостоять его взлому. Стойким считается алгоритм, атака на который потребует больших временных, умственных и материальных затрат, что после расшифровки данного защищённого алгоритма, информация потеряет всю свою значимость.

Существует два типа криптостойкости:

- Абсолютно стойкая система стойкости – характеризуется тем, то данную систему невозможно расшифровать даже, задействовав бесконечное количество вычислительных ресурсов;
- Достаточно стойкая система – характеризуется тем, что данную систему возможно расшифровать, задействовав какое-то количество вычислительных ресурсов.

Ключ - это секретная информация, которая используется криптографическим алгоритмом для зашифровки или расшифровки сообщений, а также постановке и проверке цифровой подписи, и вычислении кодов аутентичности. Для современных алгоритмов шифрования сильной криптографии утрата ключа приводит к практической невозможности расшифровать информацию.

Основной характеристикой криптостойкости является длина ключа. Так для симметричных алгоритмов шифрование с ключами длиной 128 бит и выше считается сильным, а для

асимметричных алгоритмов, минимальной надёжной длиной ключа считается 163 бит, но рекомендуются длины от 191 бит и выше [1].

Симметричный алгоритм шифрования – суть данного алгоритма заключается в том, что применяется один и тот же криптографический ключ.

Данная схема обмена информации происходит путём того, что отправитель генерирует открытый текст исходного сообщения и передаёт его получателю по незащищенному каналу. За каналом следит хакер (перехватчик) с целью перехватить и раскрыть передаваемое сообщение. Для того чтобы он не смог узнать содержание сообщения, отправитель шифрует его с помощью обратимого преобразования и получает шифртекст (или криптограмму), который отправляет получателю. Далее исходное сообщение расшифровывается и передаётся получателю [3].

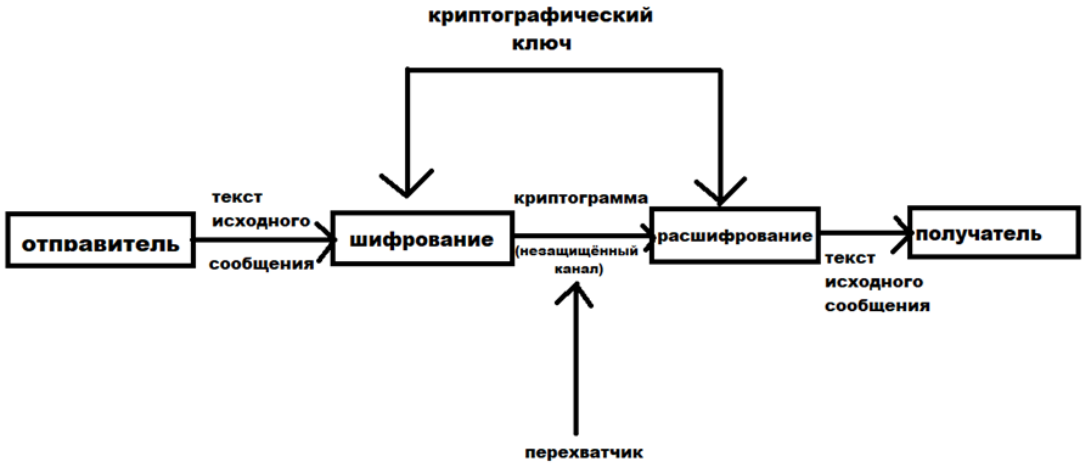

Рисунок 1. Общая схема симметрического метода шифрования

Примерами использования такого алгоритма являются DES, IDEA, blowfish.

Таблица 1. Сравнительная таблица алгоритмов симметрического метода шифрования

Алгоритм	**Размер ключа, бит**	**Длина блока, бит**	**Основные операции**	**Примечание**
DES	56	64	Подстановка, перестановка, побитовое исключающее ИЛИ	- Сеть Фейстеля; - Имеет пространство полуслабых и слабых ключей;
IDEA	128	64	Умножение по модулю $2^{16}+1$, сложение по модулю 2^{16}, побитовое исключающее ИЛИ	- Основан на смешении операций из разных алгебраических групп; - Имеет пространство слабых ключей;
BLOWFISH	32-448	64	Сложение по модулю 2^{32}, подстановка, побитовое исключающее ИЛИ	- Сеть Фейстеля; - Быстр при шифровании, медленная установка

				ключа; - Сравнительно прост; - Имеет небольшое пространство слабых ключей; - Имеет большой запас прочности;

Для сравнения выбраны IDEA, DES и Blowfish. Выбор DES обусловлен тем, что IDEA проектировался как его замена. Как видно из таблицы, размер ключа у IDEA больше, чем у DES, но меньше, чем у Blowfish. Длина блока DES, IDEA, BLOWFISH одинаковая и равна 64 бит. Также в таблице представлены основные операции, выполняющие данными и примечания алгоритмов шифрования.

Таблица 2. Применение алгоритмов симметрического метода шифрования

	DES	**IDEA**	**BLOWFISH**
Применение	- Применяется для защиты финансовой информации;	- Шифрование аудио и видео данных для кабельного телевидения, видеоконференций; - Защита коммерческой и финансовой информации; - Линии связи через модем или роутер; - Смарт-карты;	- Хеширование паролей; - Защита электронной почты и файлов GnuPG (безопасное хранение и передача); - В линиях связи: связка ElGamal; - Обеспечение безопасности в протоколах сетевого и транспортного уровня SSH;

Достоинствами симметричных алгоритмов шифрования является то, что они имеют высокую скорость обработки информации, а также их несложно модифицировать из-за относительной простоты операций, и с помощью них можно шифровать большие объемы данных при относительно небольшом размере ключа.

Недостатком симметричных алгоритмов является необходимость передать ключ для расшифровки сообщения третьему лицу, что значит данные не защищены.

Асимметрический ключ шифрования – суть данного ключа шифрования заключается в том, что используется не только открытый, но и закрытый ключ. Открытым ключом сообщение шифруется, а закрытым ключом расшифровывается, также ключи математически взаимосвязаны между собой.

Данная схема обмена информации происходит путём того, что получатель генерирует пару ключей: закрытый ключ и открытый ключ. Открытый ключ посылается отправителю, который зашифровывает сообщение с помощью открытого ключа получателя и отправляет зашифрованный текст данному получателю, который в своё время расшифровывает сообщение с помощью своего закрытого ключа и получает исходный текст сообщения.

Рисунок 2. Общая схема асимметрического метода шифрования

Примерами использования такого алгоритма являются RSA, DSA, Шифр Эль-Гамаля.

Таблица 3. Сравнительная таблица алгоритмов асимметрического метода шифрования

Алгоритм	**Размер ключа, бит**	**Примечание**	**Применение**
RSA	Max 4096	- Основан на трудности задачи факторизации больших чисел;	Шифрование и подпись
DSA	Max 1024	- Основан на трудности задачи дискретного логарифмирования в конечном поле;	Подпись
ElGamal	Max 4096	- Основан на трудной задаче вычисления дискретных логарифмов в конечном поле;	Шифрование и подпись

Для сравнения выбраны RSA, DSA и ElGamal. Как видно из таблицы, размер ключа у DSA меньше, чем у RSA и ElGamal. Также в таблице представлены основные места применения и примечания данных алгоритмов шифрования.

Достоинствами асимметричных алгоритмов шифрования является то, что для передачи ключа не нужен закрытый канал связи, а также открытый ключ может быть свободно распространён, что позволяет принимать данные от всех пользователей.

Недостатком асимметричных алгоритмов является необходимость публичной передачи ключей на этот недостаток нельзя не обратить внимание, а также алгоритмы обладают низкой скоростью выполнения операций зашифровки и расшифровки исходного текста сообщения.

Защита данных является одной из главных проблем современного мира, которую нужно постоянно держать под контролем и разрабатывать всё больше новых программных обеспечений, которые будут помогать нам её обеспечивать. Но в основе всего всегда лежит база, именно поэтому были рассмотрены симметрические и асимметрические методы шифрования, а также такие алгоритмы, как DES, IDEA, Bluwfish, так и RSA, DSA, Шифр Эль-Гамаля, которые в настоящее время также стали базовыми протоколами, помогающими обеспечивать нашу безопасность в использование разных возможностей сети Интернет.

Список литературы

1.Адаменко М. В., «Основы классической криптологии. Секреты шифров и кодов». - Москва: Машиностроение, 2014. - 256 с

2. Баричев С. Г., «Основы современной криптографии». - Москва: СИНТЕГ, 2011. - 176 с.

3. Здор С. Е., «Кодированная информация. От первых природных кодов до искусственного интеллекта». - М.: Либроком, 2012. - 168 с.