ОСНОВЫ КРИПТОГРАФИИ: ПОДГОТОВКА К CISSP

Марков Алексей Сергеевич, *кандидат технических наук, старший научный сотрудник., CISSP, SBCI, г. Москва*
Цирлов Валентин Леонидович, *кандидат технических наук, CISSP, CISM, AMBCI, г. Москва*

Публикация продолжает серию статей для специалистов по информационной безопасности, готовящихся сдать экзамен на получение статуса CISSP (Certified Information Systems Security Professional). В статье рассмотрены базовые понятия домена «Криптография», основные криптографические примитивы, в том числе симметричные и асимметричные криптосистемы, криптографические хэш–функции, цифровые подписи.

Ключевые слова*: сертификация специалистов, CISSP, криптография, шифрование, хэш, цифровая подпись, AES, Rijndael.*

CRYPTOGRAPHY BASICS: BECOMING A CISSP

Alexey Markov, *Ph.D., CISSP, Moscow*
Valentin Tsirlov, *Ph.D., CISSP, CISM, AMBCI, Moscow*

This publication continues our series of articles for information security specialists, preparing to take an exam for CISSP (Certified Information Systems Security Professional) certification. The basic concepts of Cryptography domain are described.

Keywords*: specialist certification, CISSP, cryptography, encryption, hash, digital signature, AES, Rijndael.*

Введение

Данная публикация является продолжением цикла статей по подготовке к сдаче экзамена по CISSP (Certified Information Systems Security Professional) [1-6] и касается домена, посвященного тематике криптографии. При изучении домена соискателям CISSP следует разобраться в методах и алгоритмах шифрования, симметричных и ассиметричных системах, криптографических методах обеспечения целостности, управлении ключами, стандартах и базовых криптографических протоколах, атаках на криптографические системы, а также иметь навыки работы со средствами криптографической защиты информации. Рассмотрим наиболее важные моменты.

Общие сведения

Задача передачи важной информации определённому адресату в тайне от всех остальных может быть решена, в общем случае, тремя способами [8]:

1. За счёт создания абсолютно надёжного канала передачи информации между адресатами.

Данный вариант является, безусловно, самым надёжным, однако обычно не может быть реализован на практике.

2. За счёт сокрытия самого факта передачи информации.

Такой подход получил достаточно широкое распространения и является предметом изучения ***стеганографии*** (**steganography**). Примером стеганографического канала передачи информации может служить встраивание текстового сообщения в аудио-файл. При определённых условиях данная операция не приведёт к появлению заметных изменений в звучании файла, позволяя в то же время осуществить скрытую передачу значительного объёма информации.

3. За счёт преобразования информации таким образом, чтобы восстановить её мог только законный получатель.

Именно последний вариант составляет предмет изучения криптографии.

Итак, изначально ***криптография*** (**cryptography**) возникла как наука, изучающая методы преобразования информации с целью сокрытия её смысла от нежелательных получателей. Сейчас задачи криптографии значительно шире: как минимум можно говорить о том, что она является основой для обеспечения:

- конфиденциальности информации;
- целостности информации;
- аутентификации;
- неотказуемости.

Конфиденциальность информации (**confidentiality**) означает, что она остаётся недоступной для всех, кроме легальных пользователей. Конфиден-

циальность достигается за счёт использования симметричных и асимметричных криптосистем.

Целостность информации (**integrity**) рассматривается как подтверждение её неизменности при хранении или передачи. Механизмы контроля целостности позволяют получателю сообщения убедиться в том, что оно осталось неизменным в процессе передачи. Контроль целостности реализуется с использованием криптографических хэш-функций и цифровых подписей.

Аутентификация (**authentication**) представляет собой процесс подтверждения подлинности предъявленного идентификатора и используется преимущественно для обеспечения контроля доступа к определённым ресурсам или сервисам. В протоколах аутентификации используются все без исключения криптографические примитивы.

Неотказуемость (**nonrepudiation**) защищает получателя сообщения от возможной попытки отравителя отказаться от авторства отправленного ранее сообщения. Неотказуемость может быть реализована только средствами криптографии с открытым ключом.

Перечисленные задачи криптографии реализуются с использованием следующих ***криптографических примитивов*** (**cryptographic primitives**):

- симметричные криптосистемы;
- криптосистемы с открытым ключом;
- криптографические хэш-функции;
- цифровые подписи.

Для успешной сдачи экзамена необходимо понимать основные принципы функционирования всех перечисленных примитивов, а также знать общий порядок их использования в реальной жизни.

Немного истории

Безусловно, древние криптосистемы не используются сегодня на практике. В то же время, в вопросах экзамена иногда упоминаются отдельные моменты из истории криптографии.

Мы не преувеличим, сказав, что криптография является ровесницей письменности: простейшей криптосистемой явилась сама возможность сохранения информации в виде надписи, недоступной для непосвящённых – не владеющих чтением. В дальнейшем, чтобы скрыть смысл написанного от нежелательных получателей, приходилось придумывать более сложные методы преобразования текста: использование нестандартных обозначений для букв (иероглифов, клинописных знаков), употребление чисел вместо некоторых слов и т.п.

Стоит отметить, что для многих древних цивилизаций криптография не была чем-то экзотическим [*10*]. Так, в Древней Индии было известно порядка 60 способов письма (считалось, что большинством из них владел в своё время и сам Будда), а в Камасутре среди искусств, которыми должна была в обязательном порядке владеть женщина, упоминается и криптография. Древнееврейский ***шифр «Атбаш»*** (ивр. אתב"ש) известен с VI века до н.э.

Первым документированным европейским шифром является ***шифр Цезаря*** (**Caesar Cipher**, I век н.э.). Цезарь использовал следующее преобразование: первая буква латинского алфавита заменялась на четвёртую, вторая – на пятую и т.д. Для современного латинского алфавита (справедливости ради отметим, что он отличается от того, которым пользовался Цезарь!) такое преобразование можно проиллюстрировать следующим образом:

↕	A	B	C	D	E	F	G	H	I	J
	D	E	F	G	H	I	J	K	L	M

↕	K	L	M	N	O	P	Q	R	S	T
	N	O	P	Q	R	S	T	U	V	W

↕	U	V	W	X	Y	Z
	X	Y	Z	A	B	C

Так, сообщение **VICTORY** преобразовывалось в малопонятное **YLFWRUB**. Для расшифрования достаточно найти каждый из символов шифрованного текста в нижней строке таблицы и взять вместо него символ из верхней строки.

В более строгих терминах, шифр Цезаря представляет собой циклический сдвиг алфавита на 3 позиции, и реализуемое им преобразование можно обозначить следующим образом:

$$Z_i = C_3(P_i),$$

где Z_i – ***шифртекст*** (**ciphertext**), P_i – исходный ***открытый текст*** (**plaintext**).

Очевидно, что шифр Цезаря можно обобщить, осуществляя сдвиг алфавита не на 3, а на произвольное количество позиций. Тем не менее, даже такой усовершенствованный шифр вскрывается перебором всего лишь 26 вариантов.

В общем случае преобразование, которому подвергается алфавит, не обязательно должно быть циклическим сдвигом. Если переставить символы алфавита в нижней строке подстановочной таблицы произвольным образом, мы получим простейший ***шифр простой замены***, который является примером ***подстановочного шифра*** (**substitution cipher**).

Несмотря на то, что в случае использования произвольной подстановки шифр трудно вскрыть полным перебором, подобные криптосистемы допускают тривиальное дешифрование статистическими методами. Одним из способов усложнения шифра простой замены является ***шифр Виженера*** (**Vigenere's cipher**, XVI в).

Шифр реализуется следующим образом: под сообщением подписывается ключевое слово (или фраза), которое повторяется столько раз, чтобы под каждым символом исходного сообщения был символ ключевого слова. Далее, символ открытого текста сдвигается на число позиций, соответствующее номеру расположенной под ним буквы ключевого слова. В качестве примера зашифруем сообщение **KILL THEM ALL** ключевым словом **CAB**:

K	I	L	L	T	H	E	M	A	L	L
C	A	B	C	A	B	C	A	B	C	A
N	J	N	O	U	J	H	N	C	O	M

В результате получаем фразу **NJNO OUJH COM**. Как видно, в данном случае одни и те же символы открытого текста могут перейти в разные символы шифртекста, и наоборот, одинаковые символы шифртекста могут соответствовать разным символам исходного сообщения. Всё это несколько затрудняет криптоанализ.

Обобщением шифра Виженера можно считать ***книжный шифр*** (**book cipher**). Шифрование осуществляется аналогичным образом, но в качестве ключевой фразы используется текст некоторой книги, начиная с определённой условленной позиции. Отметим, что подобный процесс наложения символов из двух источников друг на друга путём сложения их по определённому правилу называется ***гаммированием***.

Рассмотрим ***шифр Вернама*** (**Vernam cipher**), известный также как ***одноразовый блокнот*** (**one-time pad**). Шифрование в нём осуществляется аналогично книжному шифру, но в качестве ключа используется одноразовая последовательность случайных символов, длина которой равна длине открытого текста. Доказано, что данный шифр является абсолютно стойким, однако использование его на практике затруднительно из-за указанных жёстких ограничений, накладываемых на ключ. В то же время данный шифр может быть использован для передачи коротких сообщений чрезвычайной важности.

Принципиально иным классом шифров являются ***перестановочные шифры*** (**transposition/permutation ciphers**). Здесь символы сообщения переставляются по определённому закону. В качестве примера зашифруем фразу **HE IS THE ONE**, переставив буквы в порядке, указанном во второй строке таблицы:

H	E	I	S	T	H	E	O	N	E
9	7	10	1	6	2	4	3	5	8
S	H	O	E	N	T	E	E	H	I

В результате получим: **SHOENTEEHI**.

Историческая справка была бы неполной без упоминания ***дисковых шифраторов*** (**cipher disk systems**). Первый шифрдиск был разработан Леоном Баттистой Альберти (Alberti) в 1460 г. Устройство состояло из двух концентрических дисков, по периметру каждого был нанесён алфавит. Вращая диски друг относительно друга, можно было менять соответствие между символами алфавитов.

В дальнейшем дисковые шифраторы развивались в сторону усложнения: используемые в XX веке системы представляли собой сложные механические и электромеханические устройства, содержащие несколько взаимосвязанных дисков. Пожалуй, наибольшую известность из всех дисковых шифровальных машин получила ***Энигма*** (**Enigma**), использованная немецкими военными в годы Второй мировой войны. Криптоанализ Энигмы, выполненный британцами в 1940-1943 гг., является одной из интереснейших страниц в истории криптографии. Отметим, что первые прототипы ЭВМ были разработаны именно как средства автоматизации криптоанализа дисковых шифраторов.

Современная криптография ориентирована в первую очередь на использование в цифровых коммуникационных системах, для которых классические криптосистемы непригодны. В то же время современные симметричные криптосистемы являются наследниками традиционных подстановочных и перестановочных шифров.

Современные криптосистемы

Прежде чем перейти к рассмотрению современных криптографических алгоритмов, уточним основные термины, используемые в дальнейшем изложении.

Итак, ***алфавитом*** (**alphabet**) мы будем называть конечное множество знаков, используемых для представления информации. В приведённых выше примерах исторических шифров в качестве алфавита мы использовали латинские прописные буквы: A..Z. Чаще всего (хотя далеко не всегда) в современных криптосистемах используется ***двоичный***, или ***бинарный*** (**binary**), ***алфавит***, состоящий всего из двух символов: {0, 1}. ***Текст***, или ***сообщение*** (**text**, **message**) представляет собой упорядоченный набор из элементов алфавита. ***Открытый текст*** (**plaintext**) – это исходное сообщение, предназначенное для зашифрования. ***Шифртекст*** (**ciphertext**) – это результат зашифрования открытого текста.

Тем самым, ***зашифрование*** (**encryption**, **enciphering**) – это процесс преобразования открытого текста в шифртекст, а ***расшифрование*** (**decryption**, **deciphering**) – обратный процесс преобразования шифртекста в открытый текст. ***Дешифрование*** (**breaking**) – это процесс восстановления открытого текста по шифртексту без знания ключа. Подчеркнём разницу между расшифрованием и дешифрованием: если расшифрование является стандартной штатной процедурой при использовании криптографического алгоритма, то дешифрование – это взлом криптосистемы, имеющий отношение скорее к криптоанализу. Общий термин ***шифрование*** означает процесс зашифрования или расшифрования.

Предметом изучения ***криптоанализа*** (**cryptanalysis**) являются методы взлома криптосистем. Поскольку криптография и криптоанализ тесно связаны, их часто рассматривают в совокупности как единую науку – ***криптологию*** (**cryptology**).

Под ***криптосистемой*** (**cryptosystem**) мы будем понимать семейство обратимых преобразований открытого текста в шифртекст, каждое из которых определяется соответствующим алгоритмом и значением ключа.

Ключ (**key**), или ***криптопеременная*** (**cryptovariable**) – это конкретное значение некоторых параме-

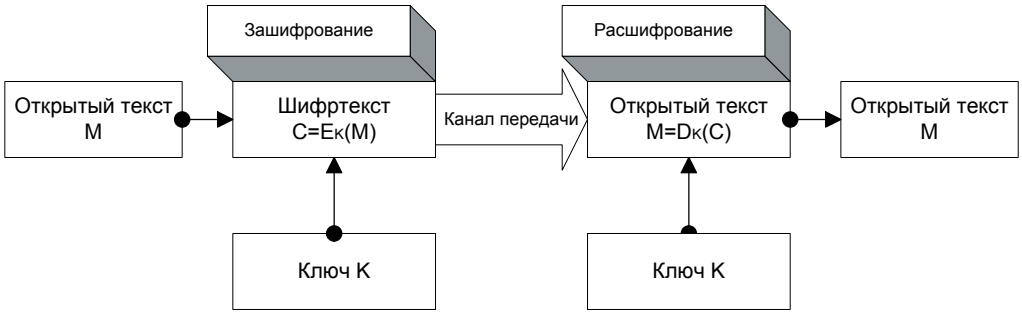
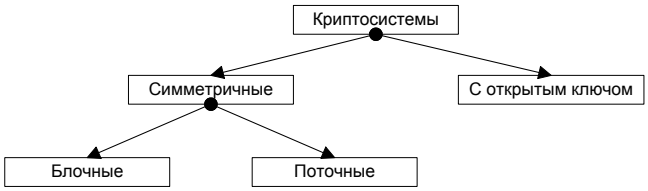


***Рис. 1** – Порядок использования симметричного шифра.*

тров криптографического алгоритма, обеспечивающее выбор одного преобразования из семейства.

Современные криптосистемы можно классифицировать следующим образом:



Характерной особенностью ***симметричных криптосистем*** (**symmetric key cryptosystems**), или ***криптосистем с секретным ключом*** (**secret key cryptosystems**), является то, что для зашифрования и расшифрования информации используется один и тот же ключ. Порядок использования симметричного шифра представлен на рисунке 1.

При этом предполагается, что взаимодействующие стороны осуществили обмен ключевой информацией по некоему надёжному каналу связи и обладают секретным ключом **K**.

Блочные шифры (**block ciphers**) по сути являются подстановочными шифрами, информация в них преобразуется блоками одинакового размера, причём одинаковые блоки исходного текста дают в результате одинаковые блоки шифртекста.

В ***поточных шифрах*** (**stream ciphers**) преобразование, которому подвергаются знаки открытого текста, изменяется с каждым моментом времени.

Криптосистемы с открытым ключом (**public key cryptosystems**), или ***асимметричные криптосистемы*** (**asymmetric key cryptosystems**) характерны тем, что в них используются различные ключи для зашифрования и расшифрования информации. Ключ для зашифрования (***открытый ключ***, **public key**) можно сделать общедоступным, с тем чтобы любой желающий мог зашифровать сообщение для некоторого получателя. Получатель же, являясь единственным обладателем ключа для расшифрования (***секретный ключ***, **private key**), будет единственным, кто сможет расшифровать зашифрованные для него сообщения. Данный механизм проиллюстрирован на рисунке 2.

Идеологию использования криптосистем с открытым ключом можно наглядно представить на следующем примере. Возьмём ящик с кодовым замком и оставим его открытым в общедоступном месте. В этом случае любой желающий сможет положить в ящик некоторое сообщение и захлопнуть его, однако открыть захлопнувшийся ящик сможет только тот, кто знает комбинацию кодового замка – т.е. законный получатель.

Безусловное преимущество данного подхода состоит в том, что отпадает необходимость организации защищённого канала для распределения ключей. К недостаткам можно отнести более низкую по сравнению с симметричными криптосистемами скорость шифрования, а также отсутствие строгого математического обоснования стойкости ряда используемых конструкций. Часто используются гибридные криптографические системы, когда обмен ключевой информацией производится с использованием асимметричной криптографии, а шифрование передаваемых данных – более быстрыми и не менее стойкими симметричными алгоритмами.

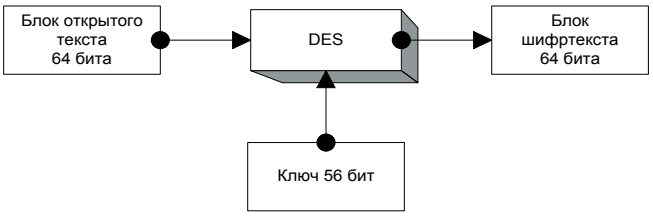
Примеры криптографических алгоритмов

Data Encryption Standard (DES)

DES (Data Encryption Standard – Стандарт Шифрования Данных) был разработан в 1972 году специалистами IBM и в течение без малого тридцати лет оставался стандартом де-факто для коммерческих приложений [7]. Алгоритм, определяемый данным стандартом, носит название ***DEA*** – Data Encryption Algorithm, Алгоритм Шифрования данных. Стандарт был утверждён в США под номером FIPS PUB 46-1 в 1977 году.

DES является блочным шифром, информация в нём преобразуется блоками по 64 бита, длина ключа составляет 56 бит. Каждый блок подвергается преобразованию, состоящему из 16 раундов. При реализуются как подстановочные, так и перестановочные преобразования.

В наиболее общем виде преобразование можно представить себе следующим образом:



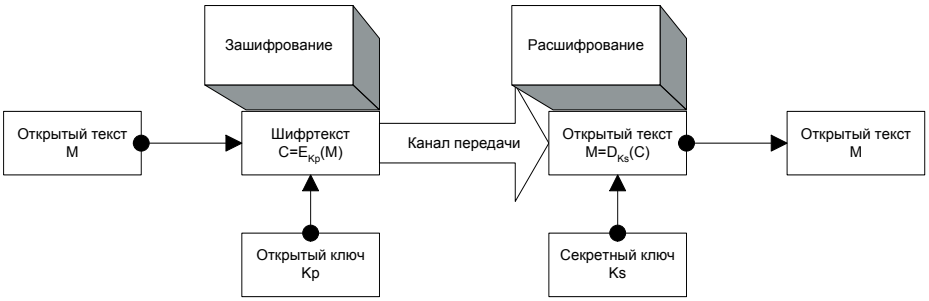


Рис. 2

Легко заметить, что при использовании данной схемы одинаковые блоки исходного текста преобразуются в одинаковые блоки шифртекста.

В настоящее время криптографическая стойкость данного стандарта считается недостаточной для большинства областей, и использование его в качестве стойкого шифра запрещено – однако, в силу своей популярности, он иногда попадает в вопросы экзамена. Изредка используется модификация ***Triple DES*** (FIPS PUB 46-1), позволяющая повысить длину ключа шифрования.

Advanced Encryption Standard (AES)

AES был принят в 2000 году в качестве замены DES по результатам открытого конкурса. Победителем стал блочный алгоритм Rijndael. Rijndael представляет собой целое семейство блочных шифров, в зависимости от требуемого уровня криптографической стойкости могут быть выбраны следующие значения параметров:

1. 128-битный ключ, 10 раундов шифрования.
2. 192-битный ключ, 12 раундов шифрования.
3. 256-битный ключ, 14 раундов шифрования.

В настоящее время наиболее распространённым (хотя и наименее стойким) является первый вариант. Стоит отметить, что алгоритм допускает достаточно простую реализацию и является сейчас стандартом де-факто во всём мире.

Другие блочные шифры

Существование криптографических стандартов ни в коей мере не ограничивает использование других алгоритмов. Так, среди популярных блочных шифров можно отметить, прежде всего, следующие: IDEA, BLOWFISH, RC5, RC6, FEAL, CAST и др. Из отечественных блочных шифров единственным реально используемым является ГОСТ 28147-89, не получивший распространения за пределами России.

Сравнение блочных шифров

Наиболее общим критерием выбора того или иного алгоритма блочного шифрования является его стойкость – однако оценить её зачастую достаточно сложно. На практике одним из наиболее простых критериев оценки стойкости криптографических алгоритмов (хотя далеко не всегда корректным!) является длина ключа. Другие параметры, такие как число раундов шифрования, также могут косвенно свидетельствовать о стойкости алгоритма.

В таблице 1 приведены некоторые параметры для наиболее распространённых блочных криптосистем [7].

Криптография с открытым ключом

Схема распределения ключей Диффи-Хеллмана

Напомним, что одним из принципиальных ограничений симметричной криптографии является необходимость организации защищённого канала для передачи секретного ключа. Криптография с открытым ключом предлагает возможное решение данной проблемы.

Итак, схема распределения ключей Диффи-Хеллмана позволяет двум участвующим сторонам совершить обмен ключевой информацией по незащищённому каналу связи.

Схема реализуется следующим образом. На первоначальном, подготовительном этапе выбираются два параметра: простое число **p** и число **g,** меньшее **p**, такое что для всех целых **n**, меньших или равных **p-1**, существует такая степень **k**, что $g^k=n \pmod p$ [1]. Оба параметра можно сделать общедоступными.

Далее, обмен ключевой информацией между участниками ***A*** и ***B*** осуществляется следующим образом:

A	B
1. Выбирает секретное число **a** и вычисляет: $y_a=g^a \pmod p$	1. Выбирает секретное число **b** и вычисляет $y_b=g^b \pmod p$
2. Пересылает B вычисленное значение y_a.	2. Пересылает A вычисленное значение y_b.
3. Используя своё секретное число **a** и полученное y_b вычисляет: $c=y_b^a=g^{ab} \pmod p$	3. Используя своё секретное число **b** и полученное y_a вычисляет: $c=y_a^b=g^{ab} \pmod p$
4. В результате как A, так и B получают общий секретный ключ **c**.	

Заметим, что сам ключ **c**, которым по окончании обмена обладают оба участника схемы, в явном виде не передаётся по каналу связи. Более того,

1 Запись (mod p) означает необходимость взять остаток от деления результата на p

Таблица 1

Алгоритм	Длина ключа	Количество раундов шифрования	Длина блока
DES	56	16	64
IDEA	128	8	64
AES (Rijndael)	128	10	128
	192	12	128
	256	14	128

можно доказать, что по тем данным, которые по каналу всё-таки передаются, практически невозможно восстановить общий секретный ключ.

Однонаправленные функции.

Прежде чем перейти к рассмотрению криптосистем с открытым ключом, необходимо остановиться на ***однонаправленных функциях*** (**one-way functions**) – своеобразных математических конструкциях, которые лежат в основе современной криптографии.

Однонаправленная функция должна обладать следующим основным свойством: просто вычисляться в прямом направлении и принципиально более сложно – в обратном [9]. Иначе говоря, для однонаправленной функции **y=f(x)** должно быть очень просто вычислить значение **y** по имеющемуся **x**, и очень трудно – определить **x** по имеющемуся **y**. Проиллюстрировать понятие однонаправленной функции можно на примере отсортированного в алфавитном порядке и напечатанного на бумаге телефонного справочника. По такому справочнику, зная фамилию абонента, очень просто найти его телефон, и наоборот, определить фамилию по имеющемуся телефону достаточно трудно (а именно, это можно сделать только полным перебором всех имеющихся вариантов!).

Практический интерес представляют так называемые ***однонаправленные функции с лазейкой*** (**trapdoor one-way functions**). Лазейка однонаправленной функции представляет собой нечто, позволяющее легко вычислить значение однонаправленной функции в обратном направлении: определить **x** по **y**. Так, для рассмотренного выше примера с телефонным справочником лазейкой мог бы быть перечень абонентов, упорядоченный не по алфавиту, а по возрастанию их телефонных номеров.

Применительно к криптографии, последнее свойство однонаправленных функций можно использовать следующим образом: секретный ключ должно быть очень трудно получить из открытого ключа без знания лазейки.

Криптосистема RSA

Первой реализованная на практике, криптографическая система RSA получила своё название как аббревиатура фамилий её разработчиков: Рона Ривеста (R. L. Rivest), Ади Шамира (A. Shamir) и Леонарда Эдлмана (L.M. Addleman). Вплоть до настоящего времени криптосистема RSA является одной из самых распространённых в своём классе.

В основе стойкости RSA лежит следующая однонаправленная функция. Возьмём два больших простых числа[2] **a** и **b** и вычислим их произведение: **c=ab**. Вычисление произведения является очень простой задачей, в то время как обратный процесс – ***факторизация*** (**factoring**) числа **c**, т.е. разложение его на простые множители, не имеет эффективных способов решения.

Алгоритм RSA реализуется следующим образом. Для генерации открытого и секретного ключей выбираются два больших простых числа, **p** и **q**. Вычисляется произведение **n=pq.**

Ключ зашифрования **e** выбирается произвольно с единственным условием: **e** и **(p-1)(q-1)** должны быть взаимно простыми числами (это означает, что у них не должно быть общих делителей, кроме единицы).

Ключ расшифрования вычисляется следующим образом:

$$d=e^{-1} \bmod ((p-1)(q-1))$$

(для вычисления можно использовать, например, алгоритм Евклида). В результате получаем:

параметры, составляющие открытый ключ: **(n, e),**

секретный ключ: **d**.

Числа **p** и **q** в дальнейшем не используются и могут быть уничтожены.

Зашифрование осуществляется блоками $\mathbf{m}_i$ длины, меньшей **n**, по следующей формуле:

$$c_i = m_i^e \bmod n$$

Расшифрование блока шифртекста $\mathbf{c}_i$ производится аналогично:

$$m_i = c_i^d \bmod n$$

Параметры e и d являются взаимозаменяемыми: любой из них можно использовать в открытом ключе, тогда другой будет секретным ключом.

Безусловным достоинством криптосистемы RSA, как и всех криптосистем с открытым ключом, является изначальное отсутствие проблемы распределения ключей. В то же время можно выделить ряд принципиальных недостатков, а именно:

крайне низкая скорость шифрования (на несколько порядков меньше, чем у традиционных криптосистем);

2 Простым называется целое число, которое делится только на само себя и на единицу

отсутствие строгого математического обоснования стойкости алгоритма[3].

Криптосистема Эль-Гамаля

Непосредственным конкурентом криптосистемы RSA является криптосистема Эль-Гамаля (T. El Gamal). В определённой степени она является обобщением рассмотренной выше схемы распределения ключей Диффи-Хеллмана.

Покажем, как с использованием схемы Эль-Гамаля осуществляется шифрование. Выбираются простое число **p** и два числа **g** и **x**, каждое из которых меньше **p**. Используется также вспомогательная величина $y=g^x \bmod p$.

В качестве ключа зашифрования выбирается число **k**, взаимно простое с **p-1**. Шифртекст для сообщения **M** будет состоять из двух чисел:

$$a=g^k \bmod p$$
$$b=y^k M \bmod p$$

Расшифрование производится с использованием следующего соотношения:

$$M=b/a^x \bmod p$$

Заметим, что в отличие от криптосистемы RSA, криптосистема Эль-Гамаля основывается на другой однонаправленной функции, связанной с вычислением дискретного логарифма.

Другие криптосистемы с открытым ключом

Помимо рассмотренных выше двух крипосистем (каждая из которых имеет несколько разновидностей), существует целый ряд менее распространённых алгоритмов. Это, в первую очередь, криптосистемы, основанные на использовании свойств эллиптических кривых.

Цифровые подписи и криптографические хэш-функции

Цифровые подписи

Цифровая подпись **(digital signature)**, точно так же как и традиционная, представляет собой механизм подтверждения подлинности документов и позволяет доказать, что именно законный автор, и никто другой, сознательно подписал документ. При этом выполняются следующие свойства цифровой подписи:

- Подпись является неотъемлемой частью документа. Невозможно отделить подпись от документа и использовать её для других документов.
- Подписанный документ невозможно изменить (в том числе и автору документа).
- От подписи невозможно отказаться. Более того, факт подписывания документа является доказуемым.

Все перечисленные свойства успешно реализуются за счёт применения аппарата асимметричной криптографии.

Действительно, если зашифровать документ не открытым, а закрытым ключом, и зашифрованную копию распространять вместе с оригиналом документа в качестве цифровой подписи, то получатель, используя общедоступный открытый ключ, может расшифровать подпись, сличить её с оригиналом и убедиться, что подпись верна.

Использование хэш-функций в цифровых подписях

Определённым недостатком рассмотренного выше способа реализации цифровой подписи является значительное увеличение объёма передаваемых сообщений: действительно, к открытому сообщению добавляется его зашифрованная копия, используемая в качестве цифровой подписи.

Чтобы избавиться от данного недостатка, можно использовать следующий подход. Назовём ***криптографической хэш-функцией*** **(hash function)** однонаправленную функцию, которая удовлетворяет следующим дополнительным свойствам:

1. На вход хэш-функции может поступать последовательность данных произвольной длины, однако результат (называемый ***хэшем***, или ***дайджестом*** **(digest)**) имеет фиксированную длину.
2. Различные входные последовательности должны давать различные дайджесты (ситуация, когда двум различным входным значениям соответствует один и тот же хэш, называется ***коллизией*** **(collision)**).
3. По имеющимся входному значению и дайджесту должно быть невозможно найти другое входное значение, дающее тот же дайджест.
4. При вычислении дайджеста должна использоваться вся информация входной последовательности (это означает, что даже незначительное изменение входной последовательности должно приводить к значительному изменению дайджеста).

Поясним второе требование. Безусловно, поскольку хэш, как правило, короче входной последовательности, число возможных значений хэша значительно меньше числа возможных входных последовательностей, и коллизии существуют по определению. Однако принципиальное требование к хэш-функции состоит в том, что целенаправленно найти коллизию должно быть невозможно.

Итак, если в рассмотренных ранее алгоритмах цифровой подписи подписывать не само сообщение, а его хэш, то тем самым можно значительно уменьшить объём передаваемых сообщений, сохранив все свойства цифровой подписи. Именно такой подход используется на практике.

Стандарты на цифровые подписи и криптографические хэш-функции

Основными международными стандартами на механизм цифровой функции и на криптографиче-

3 Обоснование стойкости RSA основано на одной из недоказанных теорем теории сложности вычислений.

скую хэш-функцию являются, соответственно, **DSS** (Digital Signature Standard) и **SHS** (Secure Hash Standard) [*9*].

DSS предусматривает возможность использования двух алгоритмов цифровой подписи: RSA и **DSA** (представляющий собой модификацию цифровой подписи Эль-Гамаля).

SHS регламентирует использование в качестве криптографической хэш-функции **SHA-1** (Secure hash Algorithm-1). SHA-1 получает на вход произвольную последовательность двоичных символов и получает хэш длиной 160 символов.

Очень популярен алгоритм хэширования **MD5** , разработанный Рональдом Ривестом (R. Rivest). MD5 вычисляет хэш длиной 128 бит.

Коды проверки подлинности сообщения

Коды проверки подлинности сообщения (**Message Authentication Codes, MAC-codes**) представляет собой криптографическую хэш-функцию, зависящую от ключа. Это означает, что вычислить значение дайджеста может только обладатель секретного ключа.

Подобные функции часто используются для контроля целостности пересылаемых файлов. Отправитель, подав на вход такой функции пересылаемый файл и свой секретный ключ, получает контрольную сумму и прилагает её к файлу. Злоумышленник, изменивший передаваемый файл, не сможет пересчитать значение MAC-кода, поскольку не знает секретного ключа. По лучатель по тому же алгоритму, что и отправитель, повторно вычисляет значение MAC-кода, и в случае совпадения его с полученным делает однозначный вывод о том, что сообщение не было изменено в процессе передачи.

Очевидно, что в качестве кода проверки подлинности сообщения можно использовать любую криптографическую хэш-функцию, дайджест которой шифруется с использованием некоторого симметричного алгоритма шифрования. Другой вариант – шифровать сообщение симметричным криптоалгоритмом в режиме CBC или CFB и использовать в качестве хэша последний блок шифртекста.

Криптографические атаки

Ранее мы отмечали, что изучением методов взлома криптографических систем занимается криптоанализ. В общем случае задача криптоанализа состоит, как правило, в получении криптографического ключа. Коротко перечислим основные методы криптоанализа [11-14].

1. ***Атака полным перебором***, или «***грубой силой***» (**brute force**). Заключается в подборе криптографического ключа путём полного перебора всех возможных вариантов. Очевидно, что сложность такой атаки значительно возрастает с увеличением длины ключа.
2. ***Атака по известному открытому тексту*** (**known plaintext attack**). Предполагает, что у криптоаналитика имеются в наличии как шифртекст, так и соответствующий открытый текст.
3. ***Атака по выбранному открытому тексту*** (**chosen plaintext attack**). Означает, что криптоаналитик может произвольно выбирать открытый текст и получать соответствующий шифртекст. Подобное возможно, например, если криптоаналитик получил доступ к устройству как к чёрному ящику.
4. ***Атака по шифртексту*** (**ciphertext only attack**). В этом случае у криптоаналитику приходится довольствоваться исключительно шифртекстом (и, возможно, некоторой общей информацией, такой, например, как предполагаемый язык сообщения).
5. ***Атака по выбранному шифртексту (*chosen ciphertext attack*).*** Криптоаналитик может выбирать произвольный шифртекст и получать соответствующий открытый текст.
6. ***Дифференциальный (*differential*) и линейный (*linear*) криптоанализ.*** Специфические методы, применяемые в отношении симметричных криптосистем.

Инфраструктура открытых ключей

Рассмотренные нами механизмы криптографии с открытым ключом позволяют решить проблему распределения ключей: для зашифрования сообщения любой желающий может использовать общедоступный открытый ключ, и расшифровать такое сообщение при помощи секретного ключа сможет только законный получатель. При этом мы не акцентировали внимание на серьёзной проблеме, а именно: как удостовериться в том, что тот или иной открытый ключ принадлежит именно желаемому адресату? Рассмотренные нами до этого методы решить данную проблему не позволяют.

Тем самым, чтобы обеспечить возможность практического использования методов криптографии с открытым ключом, необходимо реализовать некоторый механизм, который б обеспечил однозначную привязку пользователей к их открытым ключам. В качестве такого механизма используются ***цифровые сертификаты*** (**digital certificates**). В общем случае цифровой сертификат представляет собой подписанную некой авторитетной организацией – ***удостоверяющим центром*** (**certificate authority**) совокупность открытого ключа и идентификационной информации его владельца.

Структуру цифровых сертификатов определяет группа международных стандартов **X.509**. В соответствии с этим стандартом, сертификат должен включать:

- конкретную версию стандарта X.509, которой соответствует данный сертификат;
- серийный номер сертификата;
- идентификатор алгоритма цифровой подписи, который используется для подписания сертификата;

– идентификатор удостоверяющего центра, выдавшего сертификат;
– срок действия сертификата;
– идентификатор держателя сертификата;
– открытый ключ держателя сертификата.

Среди наиболее известных удостоверяющих центров можно отметить, например, VeriSign или GlobalSign.

Удостоверяющий центр выполняет следующие основные операции:

– ***Выдача сертификатов*** (**enrollment**). Процедуре выдачи предшествует проверка подлинности субъекта, запросившего сертификат.
– ***Проверка сертификатов*** (**verification**). Помимо проверки цифровой подписи сертификата необходимо убедиться в том, что сертификат не был отозван и не закончился его срок действия.
– ***Отзыв сертификатов*** (**revocation**)**.** Отзыв может потребоваться в случае, если сертификат каким-либо образом скомпрометирован или изменилась содержащаяся в нём информация. Отзыв проводится путём занесения сертификата в ***список отозванных сертификатов*** (**revocation list**).

Совокупность всех средств, реализующих описанные механизмы, получила название ***инфраструктуры открытых ключей*** (**PKI – Public Key Infrastructure**). Аспекты практической реализации и правовой статус инфраструктуры открытых ключей определяются законодательством и нормативными документами.

Литература

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С.66-73.
4. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С.69-73.
5. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4(7). С. 69-74.
6. Барабанов А.В. Подготовка к сдаче CISSP: модели информационной безопасности // // Вопросы кибербезопасности. 2014. № 5(8). С. 59-67.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: «Издательство ТРИУМФ», 2002. 816 с.
8. Введение в криптографию / Под. общей ред. В.В.Ященко. – 3-е изд. М.: МЦНМО, 2000. 288 с.
9. Столлингс В. Криптография и защита сетей. Принципы и практика. – М.: «Вильямс», 2001. 698 с.
10. Бабаш А.В., Шанкин Г.П. История криптографии. Часть 1. – М.: Гелиос АРВ, 2002. 240 с.
11. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. 2-е изд. М.: Гелиос АРВ, 2002, 480 с.
12. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография - СПб.: Издательство «Лань», 2001. - 224 с.
13. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
14. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012. 1216 p.

References

1. Dorofeev A.V. Status CISSP: kak poluchit' i ne poteryat'? Voprosy kiberbezopasnosti, 2013, N 1(1), pp.65-68.
2. Dorofeev A.V., Markov A.S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii, Voprosy kiberbezopasnosti, 2014, N 1 (2), pp. 67-73.
3. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: upravlenie riskami, Voprosy kiberbezopasnosti, 2014, N 2(3), pp.66-73.
4. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: perekhod na ISO 27001:2013, Voprosy kiberbezopasnosti, 2014, N 3(4), pp.69-73.
5. Dorofeev A.V. Podgotovka k CISSP: telekommunikatsii i setevaya bezopasnost', Voprosy kiberbezopasnosti, 2014, N 4(7), pp. 69-74.
6. Barabanov A.V. Podgotovka k sdache CISSP: modeli informatsionnoy bezopasnosti,, Voprosy kiberbezopasnosti, 2014, N 5(8), pp. 59-67.
7. Shnayer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si. - M.: Izdatel'stvo TRIUMF, 2002, 816 p.
8. Vvedenie v kriptografiyu, Pod. obshchey red. V.V.Yashchenko, 3-e izd. M.: MTsNMO, 2000. 288 s.
9. Stollings V. Kriptografiya i zashchita setey. Printsipy i praktika. M.: Vil'yams, 2001, 698 p.
10. Babash A.V., Shankin G.P. Istoriya kriptografii. Chast' 1. – M.: Gelios ARV, 2002. 240 p.
11. Alferov A.P., Zubov A.Yu., Kuz'min A.S., Cheremushkin A.V. Osnovy kriptografii: Uchebnoe posobie. 2-e izd. M.: Gelios ARV, 2002, 480 p.
12. Moldovyan A.A., Moldovyan N.A., Sovetov B.Ya. Kriptografiya - SPb.: Izdatel'stvo "Lan'", 2001, 224 p.
13. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
14. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition -McGrawHill, 2012. 1216 p.