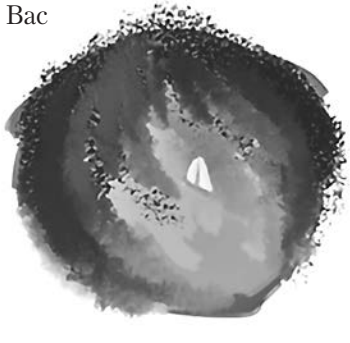
1 Введение

В этой главе

- ✓ В чем заключается криптография.
- ✓ Криптография в теории и криптография реального мира.
- ✓ О чем вы узнаете во время этого приключения.

Приветствую вас, путешественники. Погодите минутку. Вы собираетесь войти в мир, полный тайн и чудес, — в мир криптографии. *Криптография* — это древняя область знаний, ориентированная на защиту от темных сил. В этой книге собраны заклинания, необходимые для того, чтобы обезопасить себя от злого умысла. Многие пытались овладеть этим искусством, но лишь малая их часть выдержала испытания, возникшие на этом пути. Вас ждут захватывающие приключения!



Из этой книги мы узнаем, как криптографические алгоритмы защищают наши письма, идентифицируют союзников и защищают сокровища от врагов. Плавание в криптографическом море будет не самым спокойным, поскольку криптография — это основа всей безопасности и секретности в нашем мире и даже малейшая ошибка может обернуться смертельной опасностью.

ПРИМЕЧАНИЕ

Не останавливайтесь, если чего-то недопоняли. В конечном счете вы во всем разберетесь.

1.1. КРИПТОГРАФИЯ КАК ЗАЩИТА ПРОТОКОЛОВ

Наше путешествие начинается с введения в криптографию — науку, направленную на защиту протоколов от диверсантов. Но сначала определим, что такое *протокол*. Говоря простым языком, протоколом является список шагов, которые кто-то (один или несколько человек) должен выполнить для достижения какой-либо цели. Например, представьте ситуацию: вы хотите вздремнуть и для этого вам нужно оставить свой волшебный меч без присмотра на несколько часов. Протокол ваших действий может быть следующим.

1. Положить оружие на землю.
2. Вздремнуть под деревом.
3. Поднять оружие с земли.

Конечно, этот протокол далек от идеала, так как во время отдыха любой может украсть меч. Следовательно, криптография — это внимание к противникам, имеющим намерение обмануть вас.

В древние времена, когда правители и генералы только и занимались тем, что предавали друг друга и планировали перевороты, одной из самых больших проблем для них было найти способ *обмена конфиденциальной информацией с теми, кому они доверяли*. Отсюда родилась идея криптографии. Прошли столетия упорного труда, прежде чем криптография стала серьезной дисциплиной, каковой является и сегодня. Сейчас ее используют повсюду для обеспечения самых базовых услуг в нашем хаотичном, суровом мире.

Эта книга рассказывает о практической стороне криптографии. Она возьмет вас в экспедицию по всему компьютерному миру и расскажет об используемых сегодня криптографических протоколах. Она откроет вам, из каких частей состоят протоколы и каким образом все они соединяются друг с другом. Типичная книга по данной теме начинается с рассказа об открытии криптографии и ведет читателя через всю ее историю, однако не вижу смысла выстраивать здесь такую же структуру. Я хочу рассказать о применении криптографии на практике. Хочу рассказать о том, чему сам был свидетелем, работая над криптографическими программами для крупных компаний в качестве консультанта, или о криптографии, которую сам применял, будучи инженером.

Здесь не будет почти никаких страшных математических формул. Цель книги — демистификация криптографии, исследование того, что считается полезным в настоящее время, и изложение идей о том, как устроены вещи, с которыми мы работаем. Книга предназначена для любопытных людей, заинтересованных инженеров, предприимчивых разработчиков и любознательных исследователей. С главы 1 и начинается экскурс в мир криптографии. В ней мы познакомимся с различными типами криптографии, определим их важность для нас и узнаем, как мир договорился об их использовании.

1.2. СИММЕТРИЧНАЯ КРИПТОГРАФИЯ. ЧТО ТАКОЕ СИММЕТРИЧНОЕ ШИФРОВАНИЕ

Одна из фундаментальных концепций криптографии — *симметричное шифрование*. Оно используется в большинстве криптографических алгоритмов, описанных в книге, и поэтому является чрезвычайно важным понятием. Я представлю эту новую концепцию сразу через наш первый протокол.

Представим, что королеве Алисе нужно отправить письмо лорду Бобу, между владениями которого и ее королевством стоят несколько замков. Она просит преданного гонца оседлать своего верного коня и пробиться через опасные земли, чтобы доставить драгоценное послание лорду Бобу. При этом у нее есть сомнения: гонец служит ей верой и правдой уже много лет, тем не менее она желает, чтобы передаваемое послание осталось в тайне от всех посторонних лиц, включая самого гонца! Видите ли, письмо, скорее всего, содержит скандальные сплетни о королевствах, расположенных между землями королевы Алисы и лорда Боба.

Королеве Алисе нужен протокол, имитирующий передачу сообщения лорду Бобу лично, без посредников. В практическом плане данная проблема неразрешима, если мы не введем в уравнение криптографию (или телепортацию). К этому и пришли много лет назад, изобретя новый тип криптографического алгоритма — *алгоритм симметричного шифрования*, известный также как *шифр*.

ПРИМЕЧАНИЕ

Криптографический алгоритм нередко называют *примитивом*. Примитив можно рассматривать как самую маленькую полезную криптографическую конструкцию, которая часто используется в совокупности с другими примитивами для построения протокола. Этот термин не имеет особого значения, однако он так часто встречается в литературе, что о нем полезно знать.

Давайте посмотрим, как с помощью криптографического примитива скрыть сообщение королевы Алисы от гонца. Представим, что примитив — это черный ящик (мы не можем видеть, что находится или происходит внутри) с двумя функциями:

- шифрование;
- расшифрование.

Первая функция, шифрование, принимает *секретный ключ* (обычно в виде длинного числа) и сообщение, а затем выдает серию случайных чисел, или, как говорится, некоторые зашумленные данные. Этот результат и является зашифрованным сообщением (рис. 1.1).

Рис. 1.1. Функция шифрования принимает сообщение и секретный ключ и выдает зашифрованное сообщение — длинную серию цифр, которая выглядит как хаотичный шум

Вторая функция, расшифрование, является обратной по отношению к первой. Она принимает тот же секретный ключ и случайные выходные данные первой функции (зашифрованное сообщение), а затем находит исходное сообщение (рис. 1.2).

Рис. 1.2. Функция расшифрования принимает зашифрованное сообщение и секретный ключ и возвращает исходное сообщение

Прежде чем воспользоваться этим новым примитивом, королеве Алисе и лорду Бобу необходимо встретиться в реальной жизни и решить, каким будет секретный ключ. Он позволит королеве Алисе применить функцию шифрования для защиты сообщения, передать зашифрованное сообщение гонцу, который доставит его лорду Бобу. Лорд Боб, используя функцию расшифрования, с помощью того же секретного ключа сможет восстановить исходное сообщение (рис. 1.3).

При таком обмене у гонца было только то, что выглядело случайным набором символов и не давало никакого представления о содержании сообщения. По сути, благодаря криптографии мы превратили свой небезопасный протокол в безопасный. Новый протокол позволяет королеве Алисе отправить личное письмо лорду Бобу так, чтобы никто, кроме него самого, не узнал его содержания.

Использование секретного ключа для того, чтобы наполнить сообщение шумом, сделав его неотличимым от случайного набора символов, — распространенный способ защиты протокола в криптографии. В следующих главах вы увидите больше примеров его применения.

Между прочим, симметричное шифрование — это часть более широкой категории криптографических алгоритмов, называемой *симметричной криптографией* или *криптографией с секретным ключом*. Это обусловлено тем, что один и тот же ключ используют различные функции, выполняемые криптографическим примитивом. Как вы увидите позже, иногда ключей может быть несколько.

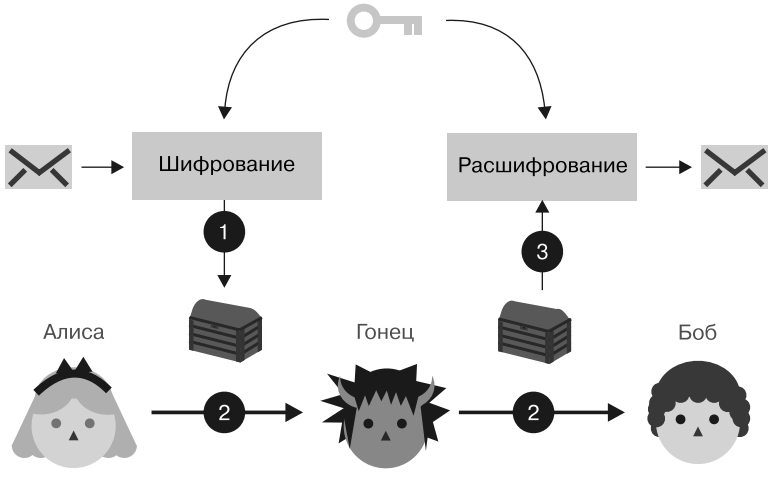


Рис. 1.3. Алиса задействует функцию шифрования с секретным ключом для преобразования своего сообщения в шум *(1)*. Она передает зашифрованное сообщение гонцу, который ничего не знает об исходном сообщении *(2)*. Получив зашифрованное сообщение, Боб может восстановить его исходное содержание с помощью функции расшифрования с тем же секретным ключом, который применила Алиса *(3)*

1.3. ПРИНЦИП КЕРКГОФФСА: СЕКРЕТОМ ЯВЛЯЕТСЯ ТОЛЬКО КЛЮЧ

Разработать криптографический алгоритм наподобие нашего криптографического примитива — просто, а вот написать *безопасный* криптографический алгоритм — задача не для слабых духом. В книге мы не станем затрагивать создание таких алгоритмов, однако *будем учиться* распознавать наиболее удачные варианты. Это не самое простое занятие, поскольку та или иная задача может иметь несколько решений. Тем не менее многочисленные неудачи в истории криптографии, а также уроки, которые сообщество извлекло из них, могут послужить хорошими подсказками. Заглянув в прошлое, мы поймем, что делает криптографический алгоритм надежным и безопасным.

Прошли сотни лет, и многие лорды и королевы покинули наш мир. С тех пор от бумаги как основного средства общения отказались в пользу более совершенных и практичных технологий. Сегодня нам доступны мощные компьютеры и Интернет. Конечно, так удобнее, но и наш подлый гонец стал намного сильнее. Он теперь повсюду: в Wi-Fi кафе Starbucks, на различных серверах, подключающих людей к Интернету и пересылающих их сообщения, и даже в машинах, на которых работают наши алгоритмы. Злоумышленники теперь могут увидеть гораздо больше сообщений, ведь каждый запрос на веб-сайт может пойти «не по тому проводу» и за считаные наносекунды его могут изменить или скопировать так, что никто этого даже не заметит.

В последние годы было много случаев, когда алгоритмы шифрования разрушались, взламывались тайными государственными организациями или независимыми исследователями, не могли защитить сообщения или соответствовать заявленным разработчиками обещаниям. Из этих неудач было извлечено много уроков, и мы постепенно пришли к пониманию того, как создать хорошую криптографическую защиту.

ПРИМЕЧАНИЕ

Криптографический алгоритм можно *взломать* разными способами. Например, возможны следующие атаки на него: секретный ключ может быть передан злоумышленнику, сообщения могут быть расшифрованы без помощи ключа, некоторые данные, касающиеся зашифрованного сообщения, могут быть раскрыты без расшифровки и т. д. Все, что каким-то образом способно снизить эффективность алгоритма, можно считать взломом.

В результате длительного процесса проб и ошибок, через который прошла криптография, сложилось устойчивое представление: получить уверенность в надежности защиты, заявленной криптографическим примитивом, можно только тогда, когда он прошел открытую проверку специалистами в этой области. В противном случае придется полагаться на *безопасность через неясность*, которая на протяжении всей истории криптографии показывала себя не с лучшей стороны. Вот почему *криптографы* (те, кто строит) обычно прибегают к помощи *криптоаналитиков* (тех, кто ломает) для проверки безопасности конструкции, хотя обычно обе функции выполняет один и тот же человек.

В качестве примера рассмотрим алгоритм шифрования Advanced Encryption Standard (AES; расширенный стандарт шифрования). Он был разработан в рамках международного конкурса, организованного Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST).

ПРИМЕЧАНИЕ

NIST — это американское агентство, которое определяет стандарты и разрабатывает руководящие принципы в области безопасности для правительственных структур и других государственных и частных организаций. Помимо AES, агентство стандартизировало большое количество широко используемых криптографических примитивов.

Конкурс длился несколько лет, в течение которых множество криптоаналитиков-добровольцев со всего мира собирались вместе, чтобы попытаться взломать различные алгоритмы шифрования. В результате признанный на конкурсе самым

безопасным шифр и стал расширенным стандартом шифрования. Сегодня большинство людей считают AES надежным алгоритмом шифрования. Его практически всегда используют для шифрования чего-либо. Например, именно он ежедневно обеспечивает вашу защиту в Интернете.

Идея открытого создания криптографических стандартов связана с концепцией, часто называемой *принципом Керкгоффса*, который трактуется примерно так: было бы глупо полагаться на то, что наши противники не узнают, какие алгоритмы мы используем, ведь они, скорее всего, узнают о них. Давайте же обеспечивать защиту в открытую.

Если недруги королевы Алисы и лорда Боба точно знали, как те шифруют свои сообщения, то каким образом их алгоритм защищает? Ответ: *секретный ключ*! Протокол безопасен не благодаря секретности алгоритма, а благодаря секретности ключа. Вот что является общей темой этой книги: почти все криптографические алгоритмы, о которых мы узнаем и которые используются в реальном мире, можно свободно изучать и задействовать в своих проектах. Скрыты только секретные ключи, применяемые в качестве входных данных для этих алгоритмов. Как сказал Жан Робер дю Карле в 1644 году, «ars ipsi secreta magistro» («секрет в искусстве есть даже для мастера»). В следующем разделе я расскажу о совершенно ином виде криптографических примитивов. А пока упорядочим то, что мы уже знаем (рис. 1.4).

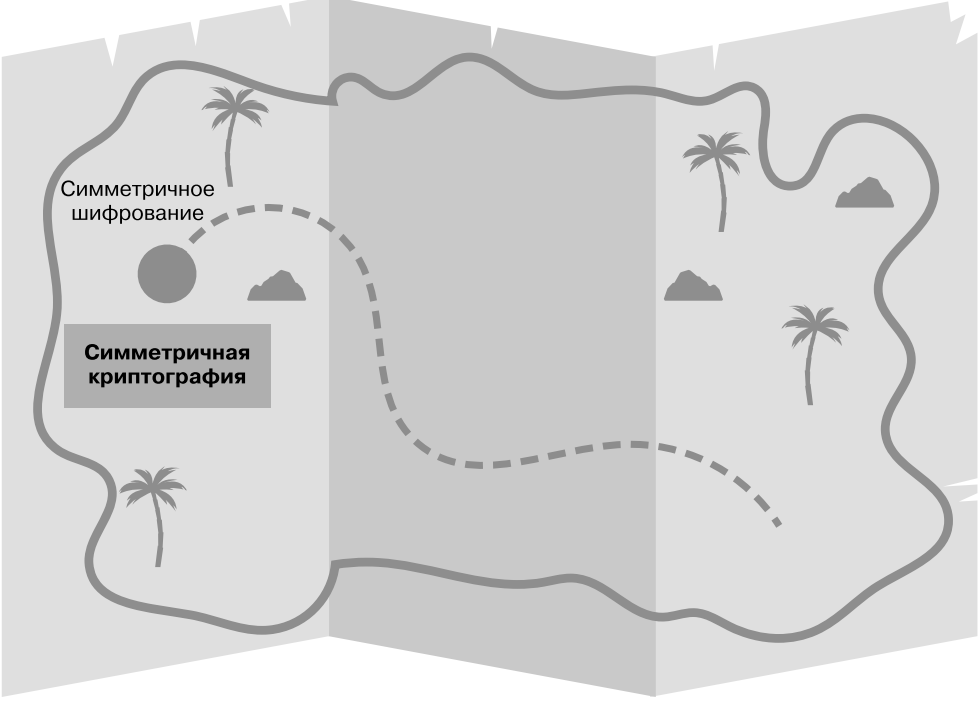


Рис. 1.4. Криптографические алгоритмы, о которых мы уже знаем.
AES — это конкретная реализация алгоритма симметричного шифрования — криптографического примитива, являющегося частью более широкого класса симметричных криптографических алгоритмов

1.4. АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ: ДВА КЛЮЧА ЛУЧШЕ ОДНОГО

В разделе про симметричное шифрование мы рассказали, как королева Алиса и лорд Боб сначала встретились и решили, каким будет симметричный ключ. Это правдоподобный сценарий, многие протоколы действительно работают именно таким образом. Но в протоколах с большим количеством участников данный способ быстро утрачивает свою практичность: нужно ли нам, чтобы наш браузер встретился с Google, Facebook, Amazon и миллиардами других веб-сайтов для обеспечения безопасного подключения?

Решение данной проблемы, которую часто обозначают как *распределение ключей*, не могли найти довольно долго — до открытия в конце 1970-х годов другой большой и полезной категории криптографических алгоритмов, именуемой *асимметричной криптографией* или *криптографией с открытым ключом*. Как правило, асимметричная криптография использует разные ключи для разных функций (в отличие от одного-единственного ключа в симметричной криптографии) или предоставляет разным участникам различный доступ к данным. В этом разделе я представлю ряд асимметричных примитивов и тем самым покажу на примерах, как криптография с открытым ключом помогает установить доверие между людьми. Обратите внимание на то, что это только краткий обзор криптографических примитивов, каждый из которых мы будем разбирать более подробно в последующих главах.

1.4.1. Обмен ключами, или Как получить общий секрет

Первый примитив асимметричной криптографии, который мы рассмотрим, — это *обмен ключами*. Названный в честь его авторов Диффи и Хеллмана (Diffie — Hellman, DH), он стал первым изобретенным и опубликованным алгоритмом с открытым ключом. Его основная задача — установление общего для двух сторон секрета, который затем может использоваться в различных целях, например в качестве ключа к примитиву симметричного шифрования.

В главе 5 я объясню работу алгоритма Диффи — Хеллмана, а сейчас ограничимся простой аналогией, чтобы понять, в чем состоит суть обмена ключами. Как и многие криптографические алгоритмы, обмен ключами обязательно начинается с того, что стороны устанавливают общий набор параметров. В нашей аналогии пусть королева Алиса и лорд Боб договорятся об использовании квадрата (■). Следующим шагом будет выбор ими личной фигуры. Оба идут в свое тайное место, и вдали от посторонних глаз королева Алиса выбирает треугольник (▲), а лорд Боб — звезду (★). Эти объекты должны оставаться в тайне любой ценой! Они представляют собой *закрытые ключи* (рис. 1.5).

После того как Алиса и Боб выбрали свои закрытые ключи, они оба по отдельности комбинируют их с общей фигурой, о которой изначально договорились, — с квадратом. В результате получаются уникальные фигуры, представляющие

собой *открытые ключи*. Теперь королева Алиса и лорд Боб могут *обмениваться* открытыми ключами (отсюда и название), поскольку те считаются публичной информацией. Данный этап изображен на рис. 1.6.

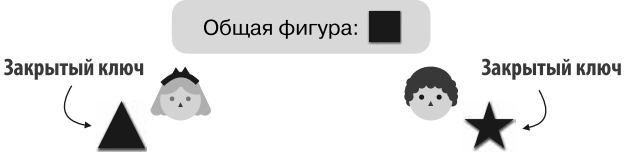


Рис. 1.5. Первый этап обмена ключами Диффи — Хеллмана: две стороны создают закрытые ключи. Королева Алиса выбирает в качестве закрытого ключа треугольник, а лорд Боб — звезду

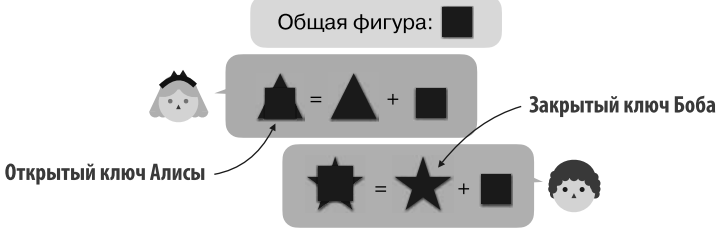


Рис. 1.6. Второй этап обмена ключами Диффи — Хеллмана: стороны обмениваются своими открытыми ключами, полученными в результате комбинирования закрытых ключей с общей фигурой

Теперь становится понятно, почему этот алгоритм называется алгоритмом с открытым ключом: он требует *пары ключей*, состоящей из закрытого и открытого ключей. Последний шаг алгоритма обмена ключами довольно прост. Королева Алиса берет открытый ключ лорда Боба и объединяет его со своим закрытым ключом. Лорд Боб делает то же самое с открытым ключом королевы Алисы. У обеих сторон должен получиться одинаковый результат. В нашем примере это фигура, сочетающая в себе звезду, квадрат и треугольник (рис. 1.7).

Рис. 1.7. Заключительный этап обмена ключами, на котором обе стороны составляют один и тот же общий секрет. Его нельзя получить, когда видны только открытые ключи

Теперь участникам протокола предстоит использовать общий секрет. Несколько примеров этого вы увидите далее в книге. Тем не менее самый очевидный сценарий — задействовать общий секрет в алгоритме, требующем его применения. Например, королева Алиса и лорд Боб могут теперь использовать общий секрет

в качестве ключа для шифрования сообщений посредством примитива симметричного шифрования. Напомню следующее.

1. Алиса и Боб обмениваются своими открытыми ключами, маскирующими их закрытые ключи.
2. Имея открытый ключ другой стороны и свой личный ключ, они могут вычислить общий секрет.
3. У противника, наблюдающего за обменом открытыми ключами, недостаточно информации для вычисления общего секрета.

ПРИМЕЧАНИЕ

В этом примере последний пункт легко обойти. Даже не зная никаких закрытых ключей, мы можем объединить открытые ключи и получить общий секрет. К счастью, это всего лишь условность нашей аналогии, которая довольно хорошо показывает принцип работы обмена ключами.

На практике обмен ключами довольно небезопасен. Немного поразмыслив, вы поймете почему.

Так как королева Алиса принимает любой отправленный ей открытый ключ за открытый ключ лорда Боба, я могу перехватить обмен и заменить этот ключ своим, что позволит мне выдать себя за лорда Боба (и то же самое можно сделать в отношении лорда Боба). Так называемый *посредник* (man-in-the-middle, MITM) может успешно атаковать данный протокол. Как это исправить? В последующих главах мы увидим, что нужно либо дополнить этот протокол другим криптографическим примитивом, либо заранее знать, каков открытый ключ лорда Боба. Но разве тогда не получается, что мы вернулись к самому началу?

Раньше королеве Алисе и лорду Бобу нужно было знать общий секрет. Теперь им требуется знать открытые ключи друг друга. Но как? Неужели это снова проблема курицы и яйца? Ну, вроде того. Как мы увидим далее, на практике криптография с открытым ключом не решает проблемы доверия, но упрощает его установление, особенно при большом количестве сторон.

Остановимся на этом и перейдем к следующему разделу, поскольку в главе 5 мы подробнее разберем обмен ключами. Нам осталось раскрыть еще несколько примитивов асимметричного шифрования (рис. 1.8), чтобы завершить экскурс в криптографию реального мира.

1.4.2. Асимметричное шифрование, не похожее на симметричное

За изобретением алгоритма обмена ключами быстро последовало изобретение *алгоритма RSA*, названного в честь Рона Ривеста, Ади Шамира и Леонарда Адлемана. RSA состоит из двух примитивов: алгоритма шифрования с открытым ключом (асимметричное шифрование) и электронной (цифровой) подписи. Оба примитива относятся к большому классу криптографических алгоритмов — *асимметричной криптографии*. В этом разделе разберем, как работают эти примитивы и в чем их польза.

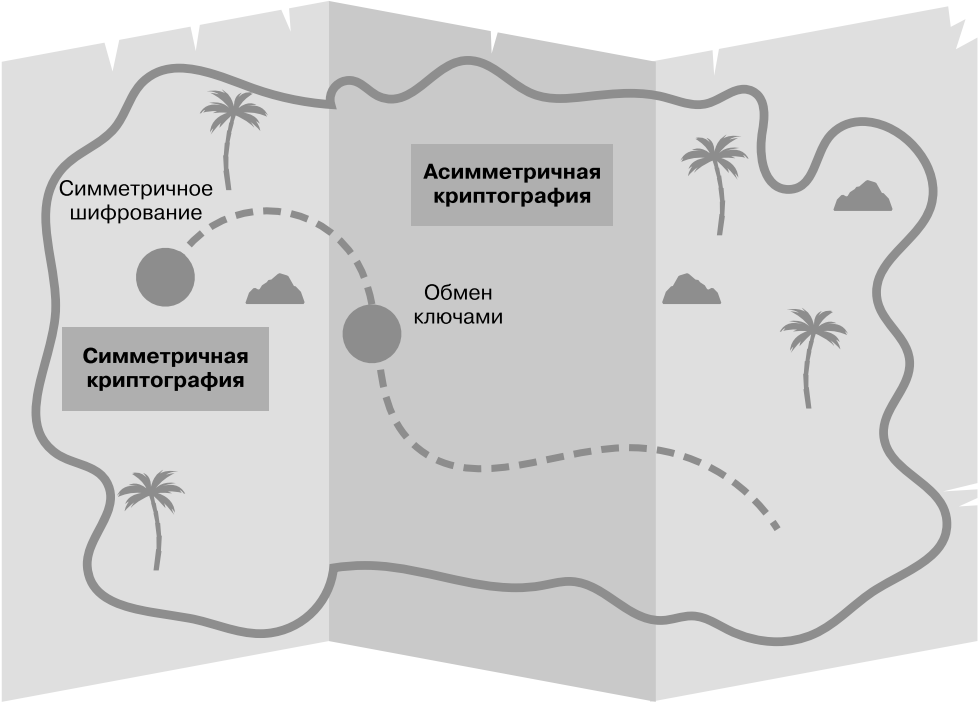


Рис. 1.8. Криптографические алгоритмы, о которых мы уже знаем. Два больших класса криптографических алгоритмов — симметричная криптография (с симметричным шифрованием) и асимметричная криптография (с обменом ключами)

Первый примитив, асимметричное шифрование, имеет ту же задачу, что и алгоритм симметричного шифрования, о котором говорилось ранее: он позволяет шифровать сообщения для обеспечения конфиденциальности. Однако, в отличие от симметричного шифрования, в котором два участника шифруют и расшифровывают сообщения с помощью одного и того же симметричного ключа, асимметричное шифрование работает совсем по-другому.

- В нем используются два разных ключа — открытый и закрытый.
- Оно предоставляет асимметричный доступ к данным: любой может шифровать с помощью открытого ключа, но расшифровывать сообщения может только владелец закрытого ключа.

Воспользуемся простой аналогией, чтобы понять, как можно применить асимметричное шифрование. Начнем с нашей подруги королевы Алисы, у которой есть закрытый ключ и соответствующий открытый ключ. Представим ее открытый ключ в виде распахнутого сундука, рыться в котором она разрешает всем желающим (рис. 1.9).