Основы криптографии

Юлий Цезарь не доверял гонцам. Поэтому, отправляя письма своим генералам, он заменял каждую букву A в своём сообщении на D, каждую B на E, и т.д. Только тот, кто знал правило «сдвига на 3» мог расшифровать его послание.

Итак, приступим.

Зашифрование и расшифрование

Информация, которая может быть прочитана, осмыслена и понята без каких-либо специальных мер, называется *открытым текстом* (plaintext, clear text). Метод искажения открытого текста таким образом, чтобы скрыть его суть, называется *зашифрованием* [1] (encryption или enciphering). Зашифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую *шифртекстом* (ciphertext). Шифрование позволяет скрыть информацию от тех, для кого она не предназначается, несмотря на то, что они могут видеть сам шифртекст. Противоположный процесс по обращению шифртекста в его исходный вид называется *расшифрованием* (decryption или deciphering). [2]

Рисунок 1 иллюстрирует это.

Рис. 1

[1] В большинстве случаев русский термин *шифрование* является синонимом *зашифрования*, но иногда обозначает криптографический процесс в целом, – *здесь и далее прим. пер.*

[2] Не следует путать *расшифрование* с *дешифрованием*: первое обозначает обращение шифртекста в открытый текст при помощи ключа, второе – без знания ключа путём криптоанализа.

Что такое криптография

Криптография – это наука об использовании математики для зашифрования и расшифрования данных. Криптография позволяет хранить важную информацию или передавать её по ненадёжным каналам связи (таким как Интернет) так, что она не может быть прочитана никем, кроме легитимного получателя.

В то время как криптография – это наука о защите данных, *криптоанализ* – это наука об анализировании и взломе зашифрованной связи. Классический криптоанализ предствляет собой смесь аналитики, математических и статистических расчётов, а также спокойствия, решительности и удачи. Криптоаналитиков также называют взломщиками.

Криптология объединяет криптографию и криптоанализ.

Стеганография является смежной дисциплиной. Вместо того, чтобы делать сообщения нечитаемыми, она использует техники сокрытия самих сообщений. Стеганография – это не криптография, это лишь частный случай *кодирования*, чья надёжность опирается на секретность механизма сокрытия сообщений. Скажем, если вы решите спрятать сообщение А, используя для этого первые буквы первых слов в каждом предложении сообщения Б, это будет секретом, пока кто-то не обнаружит, где искать А, и тогда механизм более не будет предоставлять никакой защиты.

Стойкая криптография

«В мире различают два типа критографии: криптография, которая помешает вашей младшей сестре читать ваши файлы, и криптография, которая помешает читать ваши файлы правительствам могучих держав. Эта книга посвящена криптографии второго типа»

– Брюс Шнайер, «Прикладная криптография:
протоколы, алгоритмы, исходные тексты на языке С»

PGP основан на том же типе криптографии.

Криптография может быть *стойкой*, а может быть *слабой*, как описано в приведённом примере. Криптографическая стойкость измеряется тем, сколько понадобится времени и ресурсов, чтобы из шифртекста восстановить исходный открытый текст. Результатом стойкой криптографии является шифртекст, который исключительно сложно взломать без обладания определёнными инструментами по дешифрованию. Но насколько сложно? Используя весь вычислительный потенциал современной цивилизации – даже миллиард компьютеров, выполняющих миллиард операций в секунду – невозможно дешифровать результат стойкой криптографии до конца существования Вселенной.

Кто-то может решить, что стойкая криптография сможет устоять даже против самого серьёзного криптоаналитика. Но кто об этом говорит? Никем не доказано, что лучшее шифрование, доступное сегодня, сможет выстоять против вычислительных возможностей компьютеров, доступных завтра. Тем не менее, стойкая криптография, задействованная в PGP, – лучшая на сегодняшний день. Бдительность и консерватизм сберегут вас лучше заявлений о совершенной защите.

Как действует криптография

Криптографический алгоритм, или *шифр*, – это математическая формула, описывающая процессы зашифрования и расшифрования. Чтобы зашифровать открытый текст, криптоалгоритм работает в сочетании с *ключом* – словом, числом или фразой. Одно и то же сообщение одним алгоритмом, но разными ключами будет преобразовываться в разный шифртекст. Защищённость шифртекста целиком зависит от двух вещей: стойкости криптоалгоритма и секретности ключа.

Криптоалгоритм плюс всевозможные ключи и протоколы, приводящие их в действие, составляют *криптосистему*. PGP – это криптосистема.

Обычная криптография

В традиционной криптографии, также называемой шифрованием *тайным*, или *симметричным*, ключом, один и тот же ключ используется как для зашифрования, так и для расшифрования данных. Data Encryption Standart (DES) – пример симметричного алгоритма, широко применявшегося на Западе с 70-х годов в банковской и коммерческой сферах. В настоящее время его сменяет Advanced Encryption Standard (AES). Рисунок 2 иллюстрирует процесс симметричного шифрования.

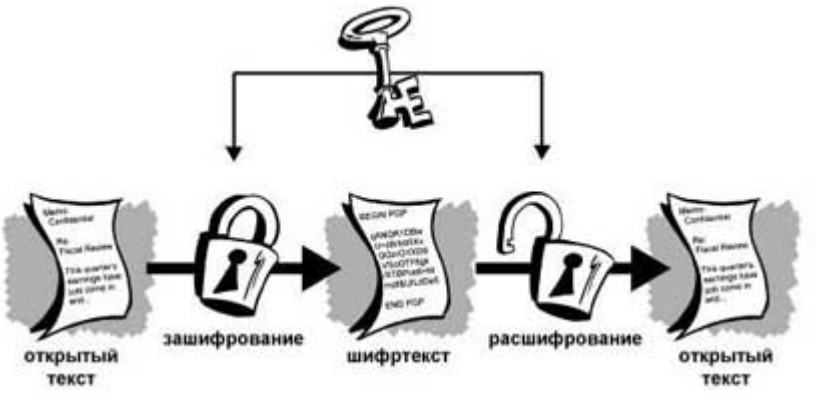

Рис. 2

Шифр Цезаря

Крайне простой пример симметричного шифрования – это *подстановочный шифр*. Подстановочный шифр заменяет каждую часть информации другой информацией. Чаще всего это достигается смещением букв алфавита. Пара примеров – это Секретное кольцо-декодер капитана Миднайта, которое могло быть у вас в детстве, и шифр Юлия Цезаря. В обоих случаях алгоритм состоит в том, чтобы сдвинуть алфавит, а ключ – это число букв, на которое произведено смещение.

Допустим, если мы решим зашифровать слово «SECRET», используя ключ Цезаря, равный 3, то сдвинем латинский алфавит так, чтобы он начинался с третьей буквы (D).

Итак, беря исходный вариант

ABCDEFGHIJKLMNOPQRSTUVWXYZ,

и смещая всё на 3, получаем

DEFGHIJKLMNOPQRSTUVWXYZABC,

где D=A, E=B, F=C и т.д.

Используя эту схему, открытый текст «SECRET» превращается в «VHFUHW». Чтобы кто-то мог восстановить исходный текст, вы сообщаете ему, что ключ – 3.

Очевидно, что по сегодняшним меркам это чрезвычайно слабый алгоритм, тем не менее, даже он помогал Цезарю! И прекрасно демонстрирует, как действует симметричное шифрование.

Симметричное шифрование и управление ключами

Симметричное шифрование имеет ряд преимуществ. Первое – скорость криптографических операций. Оно особенно полезно для шифрования данных, которые остаются у вас. Однако, симметричное шифрование, применяемое само по себе как средство защиты пересылаемых ценных данных, может оказаться весьма затратным просто из-за сложности передачи тайного ключа.

Вспомните персонажа из вашего любимого шпионского фильма: человек с запечатанным кейсом, пристёгнутым наручником к руке. Как вы считаете, что в этом кейсе? Едва ли в нём коды запуска ракет / формула химического оружия / планы вторжения, как таковые. Вероятнее, там – ключ, который расшифрует секретную информацию.

Для установления шифрованной связи с помощью симметричного алгоритма, отправителю и получателю нужно предварительно согласовать ключ и держать его в тайне. Если они находятся в географически удалённых местах, то должны прибегнуть к помощи доверенного посредника, например, надёжного курьера, чтобы избежать компрометации ключа в ходе транспортировки. Злоумышленник, перехвативший ключ в пути, сможет позднее читать, изменять и подделывать любую информацию, зашифрованную или заверенную этим ключом. Глобальная проблема симметричных шифров (от Кольца-декодера капитана Миднайта до DES и AES) состоит в сложности управления ключами: как вы доставите ключ получателю без риска, что его перехватят?

Криптография с открытым ключом

Проблема управления ключами была решена *криптографией с открытым*, или *асимметричным*, *ключом*, концепция которой была предложена Уитфилдом Диффи и Мартином Хеллманом в 1975 году. [1]

Криптография с открытым ключом – это асимметричная схема, в которой применяются *пары ключей*: *открытый* (public key), который зашифровывает данные, и соответствующий ему *закрытый* (private key), который их расшифровывает. Вы распространяете свой открытый ключ по всему свету, в то время как закрытый держите в тайне. Любой человек с копией вашего открытого ключа может зашифровать информацию, которую только вы сможете прочитать. Кто угодно. Даже люди, с которыми вы прежде никогда не встречались.

Хотя ключевая пара математически связана, вычисление закрытого ключа из открытого в практическом плане невыполнимо. Каждый, у кого есть ваш открытый ключ, сможет зашифровать данные, но не сможет их расшифровать. Только человек, обладающим соответствующим закрытым ключом может расшифровать информацию.

Рис. 3

Главное достижение асимметричного шифрования в том, что оно позволяет людям, не имеющим существующей договорённости о безопасности, обмениваться секретными сообщениями. Необходимость отправителю и получателю согласовывать тайный ключ по специальному защищённому каналу полностью отпала. Все коммуникации затрагивают только открытые ключи, тогда как закрытые хранятся в безопасности. Примерами криптосистем с открытым ключом являются *Elgamal* (названная в честь автора, Тахира Эльгамаля), *RSA* (названная в честь изобретателей: Рона Ривеста, Ади Шамира и Леонарда Адлмана), *Diffie-Hellman* (названная, правильно, в честь её создателей) и *DSA*, Digital Signature Algorithm (изобретённый Дэвидом Кравицом).

Поскольку симметричная криптография была некогда единственным способом пересылки секретной информации, цена надёжных каналов для обмена ключами ограничивала её применение только узким кругом организаций, которые могли её себе позволить, в частности, правительствами и крупными банковскими учреждениями (или маленькими детьми с Секретными кольцами-декодерами). Появление шифрования с открытым ключом стало технологической революцией, предоставившей стойкую криптографию массам. Помните курьера с кейсом, пристёгнутым к руке? Шифрование с открытым ключом отправило его на покой (к его же счастью, вероятно).

[1] Теперь есть доказательства в пользу того, что Британская Секретная Служба изобрела его несколькими годами раньше Диффи и Хеллмана, но хранила под грифом «сов. секретно» и никак не использовала. *J. H. Ellis, The Possibility of Secure Non-Secret Digital Encryption*, CESG Report, январь 1970. (CESG – Национальный Центр Объединённого Королевства по официальному применению криптографии.), – *прим. автора*.

Первой гражданской реализацией криптографии с открытым ключом было изобретение Ральфа Меркла, получившее название *«Головоломок Меркла»* (было описано им в качестве курсовой работы в 1974 году), но к практическим целям эта схемы была неприменима, – *прим. пер.*

Как действует PGP

PGP объединяет в себе лучшие стороны симметричной криптографии и криптографии с открытым ключом. PGP – это *гибридная криптосистема*.

Когда пользователь зашифровывает данные с помощью PGP, программа для начала их сжимает. Сжатие сокращает время модемной передачи и экономит дисковое пространство, а также, что более важно, повышает криптографическую стойкость. Большинство криптоаналитических техник основано на статистическом анализе шифртекста в поисках признаков открытого текста. Сжатие уменьшает число таких признаков (снижает избыточность данных), чем существенно усиливает сопротивляемость криптоанализу. (Слишком короткие файлы и файлы, которые не сжимаются достаточно хорошо, не сжимаются вовсе.)

Затем, PGP создаёт *сеансовый ключ*, т.е. одноразовый симметричный ключ, применяемый только для одной операции. Этот сеансовый ключ представляет собой псевдослучайное число, сгенерированное от случайных движений мышки и нажатий клавиш. Сеансовый ключ работает на основе очень надёжного, быстрого симметричного алгоритма, которым PGP зашифровывает сжатое сообщение; в результате получается шифртекст. Как только данные зашифрованы, сеансовый ключ также шифруется, но уже открытым ключом получателя.

Этот зашифрованный открытым ключом сеансовый ключ прикрепляется к шифртексту и передаётся вместе с ним получателю.

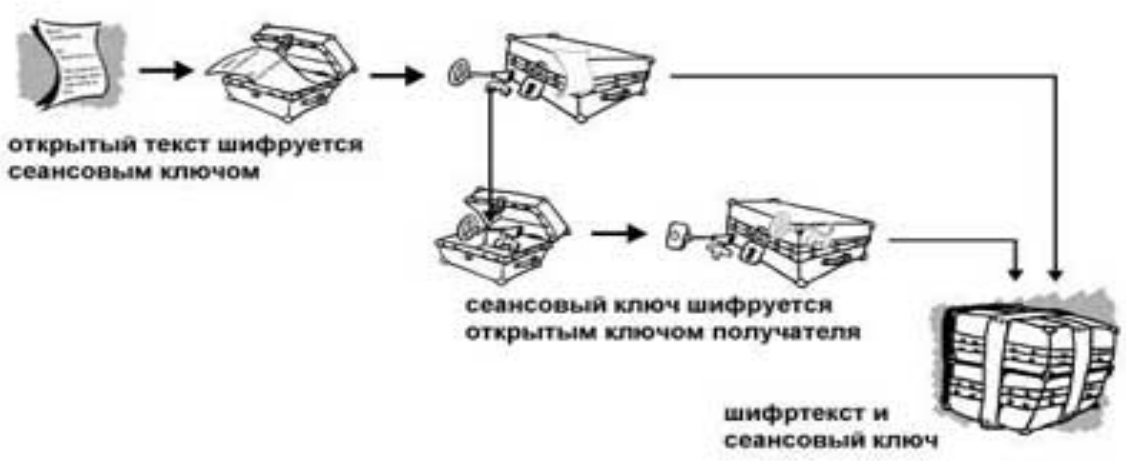

Рис. 4

Расшифрование происходит в обратном порядке. PGP получателя использует его закрытый ключ для извлечения сеансового ключа из сообщения, которым шифртекст исходного послания восстанавливается в открытый текст.

Рис. 5

Таким образом, комбинация этих двух криптографических методов объединяет удобство шифрования открытым ключом со скоростью работы симметричного алгоритма. Симметричное шифрование в тысячи раз быстрее асимметричного. Шифрование открытым ключом, в свою очередь, предоставляет простое решение проблемы управления ключами и передачи данных. Используемые совместно, скорость исполнения и управление ключами взаимно дополняются и улучшаются без какого-либо ущерба для безопасности.

Ключи

Ключ – это некоторая величина, которая, работая в сочетании с криптоалгоритмом, производит определённый шифртекст. Ключи, как правило, – это очень-очень-очень большие числа. Размер ключа измеряется в битах; число, представляющее 2048-битовый ключ, чертовски большое. В асимметричной криптографии, чем больше ключ, тем защищённей полученный шифртекст.

Однако, размер асимметричного ключа и размер симметричного тайного ключа, абсолютно несопоставимы. Симметричный 80-битовый ключ эквивалентен в стойкости 1024-битовому открытому ключу. Симметричный 128-битовый ключ примерно равен 3000-битовому открытому. Опять же, больше ключ – выше надёжность, но механизмы, лежащие в основе каждого из типов криптографии совершенно различны, и сравнивать их ключи в абсолютных величинах недопустимо.

Несмотря на то, что ключевая пара математически связана, практически невозможно из открытого вычислить закрытый; в то же время, вычисление закрытого ключа всегда остаётся возможным, если располагать достаточным временем и вычислительными мощностями. Вот почему критически важно создавать ключ верной длины: достаточно крупный, чтобы был надёжным, но достаточно малый, чтобы оставался быстрым в работе. Для этого подумайте и оцените, кто может попытаться «прочитать ваши файлы», насколько они могут быть упорны, скольким временем располагают, каковы их ресурсы.

Более крупные ключи будут криптографически защищены больший промежуток времени. Если то, что вы хотите зашифровать, должно храниться в тайне многие-многие годы, вам, возможно, следует воспользоваться очень большим ключом. Кто знает, сколько потребуется времени, чтобы вскрыть ваш ключ, используя завтрашние более быстрые, более эффективные компьютеры? Было время, когда 56-битовый симметричный ключ DES считался крайне надёжным.

По современным представлениям 128-битовые симметричные ключи совершенно надёжны и не подвержены взлому, по крайней мере до тех пор, пока кто-то не построит функционирующий квантовый суперкомпьютер. 256-битовые ключи по оценкам криптологов не могут быть взломаны даже теоретически и даже на гипотетическом квантовом компьютере. Именно по этой причине алгоритм AES поддерживает ключи длиной 128 и 256 бит. Однако история учит нас тому, что все эти заверения спустя пару десятилетий могут оказаться пустой болтовнёй.

PGP хранит ключи в зашифрованном виде. Они содержатся в двух файлах на жёстком диске; один файл для открытых ключей, другой – для закрытых. Эти файлы называются *связками* (keyrings). Используя PGP, вы, время от времени, будете добавлять открытые ключи своих корреспондентов на связку открытых. Ваши закрытые ключи находятся на связке закрытых. **Если вы потеряете (удалите) связку закрытых ключей, то уже никаким образом не сможете расшифровать информацию, зашифрованную для ключей с этой связки.** Следовательно, сохранение пары резервных копий этого файла является полезной практикой.

Цифровые подписи

Дополнительное преимущество от использования криптосистем с открытым ключом состоит в том, что они предоставляют возможность создания *электронных цифровых подписей* (ЭЦП). Цифровая подпись позволяет получателю сообщения убедиться в аутентичности источника информации (иными словами, в том, кто является автором информации), а также проверить, была ли информация изменена (искажена), пока находилась в пути. Таким образом, цифровая подпись является средством *аутентификации* и *контроля целостности данных*. Кроме того, ЭЦП несёт принцип *неотречения*, который означает, что отправитель не может отказаться от факта своего авторства подписанной им информации. Эти возможности столь же важны для криптографии, как и секретность.

ЭЦП служит той же цели, что печать или собственноручный автограф на бумажном листе. Однако вследствие своей цифровой природы ЭЦП превосходит ручную подпись и печать в ряде очень важных аспектов. Цифровая подпись не только подтверждает личность подписавшего, но также помогает определить, было ли содержание подписанной информации изменено. Собственноручная подпись и печать не обладают подобным качеством, кроме того, их гораздо легче подделать. В то же время, ЭЦП аналогична физической печати или факсимиле в том плане, что, как печать может быть проставлена любым человеком, получившим в распоряжение печатку, так и цифровая подпись может быть сгенерирована кем угодно с копией нужного закрытого ключа. [1]

Некоторые люди используют цифровую подпись гораздо чаще шифрования. Например, вы можете не волноваться, если кто-то узнает, что вы только что поместили $1000 на свой банковский счёт, но вы должны быть абсолютно уверены, что производили транзакцию через банковского кассира.

Простой способ генерации цифровых подписей показан на рисунке 6. Вместо зашифрования информации чужим открытым ключом, вы шифруете её своим собственным закрытым. Если информация может быть расшифрована вашим открытым ключом, значит её источником являетесь вы.

Рис. 6

Хэш-функция

Однако описанная выше схема имеет ряд существенных недостатков. Она крайне медлительна и производит слишком большой объём данных – по меньшей мере вдвое больше объёма исходной информации. Улучшением такой схемы становится введение в процесс преобразования нового компонента – *односторонней хэш-функции*. Одностороняя хэш-функция берёт ввод произвольной длины, называемый *прообразом*, – в данном случае, сообщение любого размера, хоть тысячи или миллионы бит – и генерирует строго зависящий от прообраза вывод фиксированной длины, допустим, 160 бит. Хэш-функция гарантирует, что если информация будет любым образом изменена – даже на один бит, – в результате получится совершенно иное хэш-значение.

В процессе цифрового подписания PGP обрабатывает сообщение криптографически стойким односторонним хэш-алгоритмом. Эта операция приводит к генерации строки

ограниченной длины, называемой *дайджестом сообщения* (message digest). [2] (Опять же, любое изменение прообраза приведёт к абсолютно иному дайджесту.)

Затем PGP зашифровывает полученный дайджест закрытым ключом отправителя, создавая «электронную подпись», и прикрепляет её к прообразу. PGP передаёт ЭЦП вместе с исходным сообщением. По получении сообщения, адресат при помощи PGP заново вычисляет дайджест подписанных данных, расшифровывает ЭЦП открытым ключом отправителя, тем самым сверяя, соответственно, целостность данных и их источник; если вычисленный адресатом и полученный с сообщением дайджесты совпадают, значит информация после подписания не была изменена. PGP может как зашифровать само подписываемое сообщение, так и не делать этого; подписание открытого текста без зашифрования полезно в том случае, если кто-либо из получателей не заинтересован или не имеет возможности сверить подпись (допустим, не имеет PGP).

Если в механизме формирования ЭЦП применяется стойкая односторонняя хэш-функция, нет никакого способа взять чью-либо подпись с одного документа и прикрепить её к другому, или же любым образом изменить подписанное сообщение. Малейшее изменение в подписанном документе будет обнаружено в процессе сверки ЭЦП.

Рис. 7

ЭЦП играют важнейшую роль в удостоверении и заверении ключей других пользователей PGP.

[1] Таким образом, цифровая подпись, в отличие от собственноручной, свидетельствует не о том, что конкретный индивидуум (физическое лицо) заверил информацию, а что конкретный криптографический ключ заверил информацию. Цели "связывания" криптографического ключа и физического лица служат цифровые сертификаты и механизмы защиты ключа, основанные на личностных (биометрических) данных его владельца.

[2] Синонимы – хэш-значение, свёртка, сигнатура, контрольная сумма, код аутентичности сообщения.