Е. Ю. Родионов

ПРИМЕНЕНИЕ ЗАПУТЫВАЮЩИХ ПРЕОБРАЗОВАНИЙ В КРИПТОГРАФИИ

Впервые задача запутывания была упомянута в работе Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии». В ней предложено использовать для построения асимметричной криптосистемы сложность задачи, заключающейся в анализе программ на низкоуровневом языке программирования (ассемблер, байт-код). В таком варианте основной упор делается на секретность алгоритма шифрования: не зная алгоритм шифрования, трудно его обратить или восстановить определенную ключевую информацию, необходимую для расшифрования. Вот основные применения запутывания в криптографии:

- преобразование симметричных криптосистем в асимметричные;
- гомоморфное шифрование.

Первое направление позволяет посредством симметричного алгоритма шифрования и применения запутывающих преобразований получить асимметричный алгоритм шифрования. Достигается это следующим образом: берется конкретный алгоритм шифрования и фиксируется ключ, затем к полученному алгоритму шифрования с фиксированным ключом применяются запутывающие преобразования так, чтобы извлечение ключевой информации из получившегося запутанного алгоритма было вычислительно трудно. Таким образом, получается открытый ключ, который абоненты могут использовать для связи, шифруя с помощью него сообщения. Преобразование симметричных криптографических систем в асимметричные позволяет получить определенные выгоды:

- маленький размер закрытого ключа;
- высокая скорость расшифрования.

Размер ключа симметричного шифра, как правило, в несколько, а то и в десятки раз меньше размера ключа асимметричного шифра. Примером может послужить криптосистема RSA, в основу которой положена задача факторизации чисел. Для обеспечения надлежащей надежности и долгосрочной секретности рекомендуется использовать ключ длиной не менее 4096 бит. Для сравнения, длина ключа в алгоритме ГОСТ 28147-89 равна 256 бит, что в 16 раз меньше, чем длина ключа в криптосистеме RSA. В то же время скорость шифрования/расшифрования алгоритма RSA примерно в тысячу раз больше, чем скорость шифрования/расшифрования алгоритма DES. То есть с таких позиций запутанная симметричная криптосистема оказывается намного быстрее, удобнее, выгоднее, чем асимметричная.

Криптосистемы подобного вида нашли применение в технологиях ТСЗАП (технические средства защиты авторских прав). На нынешнем этапе развития ТСЗАП сами по себе не в состоянии эффективно ограничить неправомерное использование произведений. Это обусловлено прежде всего тем, что применяемые ныне устройства воспроизведения (персональные компьютеры, видеомагнитофоны, DVD-проигрыватели и т. д.) являются достаточно универсальными и находятся под контролем пользователей. В таких условиях разрешить воспроизведение (просмотр) и в то же время запретить копирование представляет собой принципиально неразрешимую задачу: воспроизведение — чтение и запись на устройство вывода, копирование — чтение и запись на устройство хранения; т. е., если возможно воспроизведение, возможно и копирование. Эффективная техническая защита от копирования при разрешенном воспроизведении может быть достигнута только когда все устройство (компьютер, проигрыватель) находится целиком под контролем правообладателя.

Применение запутывающих преобразований позволяет решить данную проблему. Аудио- или видеоинформация рассылается в зашифрованном виде. Легальные пользователи

имеют специальное программное или аппаратное обеспечение, выполняющее расшифрование и воспроизведение информации. Ключ, с помощью которого выполняется расшифрование, находится на компьютере пользователя, тем самым является уязвимым звеном в описанной схеме защиты авторских прав. Здесь пользователь — потенциальный злоумышленник, который может декомпилировать программу и извлечь ключ расшифрования. Применение запутывающих преобразований позволяет предотвратить извлечение ключа расшифрования из программного обеспечения, которое используется для воспроизведения. Данные преобразования делают задачу извлечения ключа шифрования из программного обеспечения вычислительно трудной.

Как было замечено выше, асимметричные криптографические алгоритмы, в основе которых лежит алгоритмически трудно разрешимая задача, проигрывают симметричным алгоритмам по скорости шифрования/расшифрования, что ограничивает их применение в некоторых приложениях. К таким приложениям относятся программные продукты, работающие в условиях дефицита аппаратных ресурсов, например такие, как программное обеспечение электронных ключей. Электронные ключи представляют собой небольшие устройства, подсоединяемые к параллельному (LPT) или USB-порту компьютера, и являются на сегодняшний день наиболее эффективным инструментом защиты коммерческого программного обеспечения от незаконного копирования. Защищаемое программное обеспечение привязывается программным способом к аппаратному ключу и корректно работает только в случае наличия в системе электронного ключа. Данная схема защиты имеет определенные уязвимые места, в частности протокол обмена информацией между ключом и приложением, который подвержен атакам типа «человек посередине». Для предотвращения подобных атак производители электронных ключей прибегают к использованию криптографии, в результате чего и сталкиваются с вышеописанными трудностями. При использовании симметричных криптографических протоколов разработчики и пользователи должны решать проблему распространения ключей шифрования и ЭЦП, использование асимметричных криптографических протоколов на сегодняшний день является нерациональным в силу приведенных выше аргументов. Криптографические алгоритмы, построенные по принципу запутывания симметричных алгоритмов шифрования данных, позволят избежать таких трудностей.

Вторым направлением применения запутывающих преобразований в области криптографии является создание гомоморфных криптосистем. Под гомоморфным шифрованием, или, как еще говорят, вычислениями над зашифрованными данными, понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо операций над открытыми текстами: предположим $E(k,m)$ — функция шифрования, где m — открытый текст, k — ключ шифрования. Функция E гомоморфна относительно операции $o\rho$, если существует эффективный алгоритм (требующий полиномиального числа ресурсов и работающий за полиномиальное время) M, такой, который, получив на вход любую пару криптограмм вида $E(k,m_1)$ и $E(k,m_2)$, выдает криптограмму c, при расшифровании которой будет получен открытый текст $m_1\ o\rho\ m_2$. В криптографии очень часто рассматривается частный случай: для данной функции шифрования E и операции $o\rho_1$ над открытыми текстами существует операция $o\rho_2$ над криптограммами, такая, что при расшифровании криптограммы $E(k,m_1)\ o\rho_2\ E(k,m_2)$ получится открытый текст $m_1\ o\rho\ m_2$. Гомоморфное шифрование может найти широкое применение в криптографии. Прежде всего, следует выделить такую задачу, как вычисление над зашифрованными данными, наиболее интересную с прикладной точки зрения. Конфиденциальные и секретные данные хранятся в зашифрованном виде. Предположим, что требуется выполнить какую-либо операцию над ними. Для этого необходимо расшифровать данные, затем выполнить требуемую операцию,

а затем вновь зашифровать результат. Данная последовательность действий выполняется на произвольном компьютере, в частности в окружении злоумышленника, который полностью контролирует вычислительное устройство и фактически может в любой момент вмешаться в выполнение программы и извлечь секретные данные. Для решения подобной задачи необходима защищенная аппаратура и организационные меры по хранению секретных ключей. Вычисления над зашифрованными данными позволяют избежать всех этих проблем, так как секретная информация не расшифровывается.

В данной статье автор рассмотрел области применения запутывающих преобразований, такие как программное обеспечение электронных ключей и технологии ТСЗАП. Актуальность данного направления обусловлена стремительным развитием ТСЗАП, предназначенных для ограничения доступа к информации в недоверенном программно-аппаратном окружении. В настоящее время данное направление развивается достаточно быстрыми темпами, разрабатываются методы, позволяющие запутать такие алгоритмы шифрования, как AES, DES, ГОСТ 28147-89, проводятся исследовательские работы в области изучения запутывающих преобразований.

СПИСОК ЛИТЕРАТУРЫ:

1. *Boaz Barak*. On the (Im)possibility of Obfuscating Programs. URL: http://www.iacr.org/archive/crypto2001/21390001.pdf.
2. *Dennis Hofheinz*. Obfuscation for Cryptographic Purposes. URL: http://eprint.iacr.org/2006/463.pdf.
3. *S. Chow*. A White-Box DES Implementation. URL: http://crypto.stanford.edu/DRM2002/whitebox.pdf.