**Криптографические протоколы**

Протокол - это последовательность шагов, которые предпринимают две или большее количество сторон для совместного решения некоторой задачи. Следует обратить внимание на то, что все шаги предпринимаются в порядке строгой очередности и ни один из них не может быть сделан прежде, чем закончится предыдущий.

Кроме того, любой протокол подразумевает участие двух сторон. В одиночку можно смешать и выпить коктейль, но к протоколу эти действия не будут иметь никакого отношения. Поэтому придется угостить кого-нибудь сделанным коктейлем, чтобы его приготовление и дегустация стали настоящим протоколом. И наконец, протокол обязательно предназначен для достижения какой-то цели, иначе это не протокол, а пустое времяпрепровождение.

У протоколов есть также и другие отличительные черты:

• каждый участник протокола должен быть заранее оповещен о шагах, которые ему предстоит предпринять;

• все участники протокола должны следовать его правилам добровольно, без принуждения;

• необходимо, чтобы протокол допускал только однозначное толкование, а его шаги были совершенно четко определены и не допускали возможности их неправильного понимания;

• протокол должен описывать реакцию участников на любые ситуации, которые могут возникнуть в ходе его реализации. Иными словами, недопустимым является положение, при котором для возникшей ситуации протоколом не определено соответствующее действие.

Криптографическим протоколом называется протокол, в основе которого лежит криптографический алгоритм. Однако целью криптографического протокола зачастую является не только сохранение информации в тайне от посторонних. Участники криптографического протокола могут быть близкими друзьями, у которых нет друг от друга секретов, а могут являться и непримиримыми врагами, каждый из которых отказывается сообщить другому, какое сегодня число. Тем не менее им может понадобиться поставить свои подписи под совместным договором или удостоверить свою личность. В этом случае криптография нужна, чтобы предотвратить или обнаружить подслушивание посторонними лицами, а также не допустить мошенничества. Поэтому часто криптографический протокол требуется там, где его участники не должны сделать или узнать больше того, что определено этим протоколом.

Зачем нужны криптографические протоколы

В повседневной жизни нам приходится сталкиваться с протоколами буквально на каждом шагу - играя в любые игры, или делая покупки в магазинах, или голосуя на выборах. Многими протоколами нас научили пользоваться родители, школьные учителя и друзья. Остальные мы сумели узнать самостоятельно.

В настоящее время люди все чаще контактируют друг с другом при помощи компьютеров. Компьютеры же, в отличие от большинства людей, в школу не ходили, у них не было родителей, да и учиться без помощи человека они не в состоянии. Поэтому компьютеры приходится снабжать формализованными протоколами, чтобы они смогли делать то, что люди выполняют не задумываясь. Например, если в магазине не окажется кассового аппарата, вы все равно окажетесь в состоянии купить в нем необходимую для себя вещь. Компьютер же такое кардинальное изменение протокола может поставить в полный тупик.

Большинство протоколов, которые люди используют при общении друг с другом с глазу на глаз, хорошо себя зарекомендовали только потому, что их участники имеют возможность вступить в непосредственный контакт. Взаимодействие с другими людьми через компьютерную сеть, наоборот, подразумевает анонимность. Будете ли вы играть с незнакомцем в преферанс, не видя, как он тасует колоду и раздает карты? Доверите ли вы свои деньги совершенно постороннему человеку, чтобы он купил вам что-нибудь в магазине? Пошлете ли вы свой бюллетень голосования по почте, зная, что с ним сможет ознакомиться кто-то из почтовых работников и потом рассказать всем о ваших нетрадиционных политических пристрастиях? Думаю, что нет.

Глупо считать, что компьютерные пользователи ведут себя более честно, чем абсолютно случайные люди. То же самое касается и сетевых администраторов, и проектировщиков компьютерных сетей. Большинство из них и в самом деле достаточно честны, однако остальные могут причинить вам слишком большие неприятности. Поэтому так нужны криптографические протоколы, использование которых позволяет защититься от непорядочных людей.

Распределение ролей

Чтобы описание протоколов было более наглядным, их участники будут носить имена, которые однозначно определяют роли, им уготованные (см. таблицу). Антон и Борис принимают участие во всех двухсторонних протоколах. Как правило, начинает выполнение шагов, предусмотренных протоколом, Антон, а ответные действия предпринимает Борис. Если протокол является трех- или четырехсторонним, исполнение соответствующих ролей берут на себя Владимир и Георгий.

Об остальных персонажах подробнее будет рассказано несколько позже.

**Протоколы с арбитражем**

Арбитр является незаинтересованным участником протокола, которому остальные участники полностью доверяют, предпринимая соответствующие действия для завершения очередного шага протокола. Это значит, что у арбитра нет личной заинтересованности в достижении тех или иных целей, преследуемых участниками протокола, и он не может выступить на стороне одного из них. Участники протокола также принимают на веру все, что скажет арбитр, и беспрекословно следуют всем его рекомендациям.

В протоколах, которым мы следуем в повседневной жизни, роль арбитра чаще всего играет адвокат. Однако попытки перенести протоколы с адвокатом в качестве арбитра из повседневной жизни в компьютерные сети наталкиваются на существенные препятствия:

• Легко довериться адвокату, про которого известно, что у него незапятнанная репутация и с которым можно установить личный контакт. Однако если два участника протокола не доверяют друг другу, арбитр, не облаченный в телесную оболочку и существующий где-то в недрах компьютерной сети, вряд ли будет пользоваться у них большим доверием.

• Расценки на услуги, оказываемые адвокатом, известны. Кто и каким образом будет оплачивать аналогичные услуги арбитра в компьютерной сети?

• Введение арбитра в любой протокол увеличивает время, затрачиваемое на реализацию этого протокола.

• Поскольку арбитр контролирует каждый шаг протокола, его участие в очень сложных протоколах может стать узким местом при реализации таких протоколов. Соответствующее увеличение числа арбитров позволяет избавиться от данного узкого места, однако одновременно увеличиваются и расходы на реализацию протокола.

• В силу того, что все участники протокола должны пользоваться услугами одного и того же арбитра, действия злоумышленника, который решит нанести им ущерб, будут направлены, в первую очередь, против этого арбитра. Следовательно, арбитр представляет собой слабое звено в цепи участников любого протокола с арбитражем.

Несмотря на отмеченные препятствия, протоколы с арбитражем находят широкое применение на практике.

**Протокол с судейством**

Чтобы снизить накладные расходы на арбитраж, протокол, в котором участвует арбитр, часто делится на две части. Первая полностью совпадает с обычным протоколом без арбитража, а ко второй прибегают только в случае возникновения разногласий между участниками. Для разрешения конфликтов между ними используется особый тип арбитра - судья.

Подобно арбитру, судья является незаинтересованным участником протокола, которому остальные его участники доверяют при принятии решений. Однако в отличие от арбитра, судья участвует отнюдь не в каждом шаге протокола. Услугами судьи пользуются, только если требуется разрешить сомнения относительно правильности действий участников протокола. Если таких сомнений ни у кого не возникает, судейство не понадобится.

В компьютерных протоколах с судейством предусматривается наличие данных, проверив которые доверенное третье лицо может решить, не смошенничал ли кто-либо из участников этого протокола. Хороший протокол с судейством также позволяет выяснить, кто именно ведет себя нечестно. Это служит прекрасным превентивным средством против мошенничества со стороны участников такого протокола.

**Самоутверждающийся протокол**

Самоутверждающийся протокол не требует присутствия арбитра для завершения каждого шага протокола. Он также не предусматривает наличие судьи для разрешения конфликтных ситуаций. Самоутверждающийся протокол устроен так, что если один из его участников мошенничает, другие смогут моментально распознать нечестность, проявленную этим участником, и прекратить выполнение последующих шагов протокола.

Конечно же, хочется, чтобы существовал универсальный самоутверждающийся протокол на все случаи жизни. Однако на практике в каждом конкретном случае приходится конструировать свой специальный самоутверждающийся протокол.

Разновидности атак на протоколы

Атаки на протоколы бывают направлены против криптографических алгоритмов, которые в них задействованы, против криптографических методов, применяемых для их реализации, а также против самих протоколов. Для начала предположим, что используемые криптографические алгоритмы и методы являются достаточно стойкими, и рассмотрим атаки собственно на протоколы.

Лицо, не являющееся участником протокола, может попытаться подслушать информацию, которой обмениваются его участники. Это пассивная атака на протокол, которая названа так потому, что атакующий (будем именовать его Петром) может только накапливать данные и наблюдать за ходом событий, но не в состоянии влиять на него. Пассивная атака подобна криптоаналитической атаке со знанием только шифртекста. Поскольку участники протокола не обладают надежными средствами, позволяющими им определить, что они стали объектом пассивной атаки, для защиты от нее используются протоколы, дающие возможность предотвращать возможные неблагоприятные последствия пассивной атаки, а не распознавать ее.

Атакующий может попытаться внести изменения в протокол ради собственной выгоды. Он может выдать себя за участника протокола, внести изменения в сообщения, которыми обмениваются участники протокола, подменить информацию, которая хранится в компьютере и используется участниками протокола для принятия решений. Это активная атака на протокол, поскольку атакующий (назовем его Зиновием) может вмешиваться в процесс выполнения шагов протокола его участниками.

Итак, Петр пытается собрать максимум информации об участниках протокола и об их действиях. У Зиновия же совсем другие интересы - ухудшение производительности компьютерной сети, получение несанкционированного доступа к ее ресурсам, внесение искажений в базы данных. При этом и Петр, и Зиновий не обязательно являются совершенно посторонними лицами. Среди них могут быть легальные пользователи, системные и сетевые администраторы, разработчики программного обеспечения и даже участники протокола, которые ведут себя непорядочно или даже вовсе не соблюдают этот протокол.

В последнем случае атакующий называется мошенником. Пассивный мошенник следует всем правилам, которые определены протоколом, но при этом еще и пытается узнать о других участниках больше, чем предусмотрено этим протоколом. Активный мошенник вносит произвольные изменения в протокол, чтобы нечестным путем добиться для себя наибольшей выгоды.

Защита протокола от действий нескольких активных мошенников представляет собой весьма нетривиальную проблему. Тем не менее при некоторых условиях эту проблему удается решить, предоставив участникам протокола возможность вовремя распознать признаки активного мошенничества. А защиту от пассивного мошенничества должен предоставлять любой протокол вне зависимости от условий, в которые поставлены его участники.

**Доказательство с нулевым разглашением конфиденциальной информации**

Антон: "Я знаю пароль для входа в компьютерную сеть Центробанка и рецепт приготовления „Байкала"".

Борис: "Нет, не знаешь!"

Антон: "Нет, знаю!"

Борис: "Чем докажешь?"

Антон: "Хорошо, я тебе все расскажу".

Антон долго шепчет что-то на ухо Борису.

Борис: "Действительно интересно! Надо сообщить об этом газетчикам!"

Антон: "Ё-моё..."

К сожалению, в обычных условиях Антон может доказать Борису, что знает какую-либо тайну, единственным способом - рассказав, в чем состоит ее суть. Но тогда Борис автоматически узнает эту тайну и сможет поведать о ней первому встречному. Есть ли у Антона возможность помешать Борису это сделать?

Конечно, есть. В первую очередь, Антону не следует доверять свою тайну Борису. Но как тогда Антон сможет убедить Бориса в том, что действительно входит в число посвященных?

Антону надо воспользоваться протоколом доказательства с нулевым разглашением конфиденциальной информации. С помощью этого протокола Антон окажется в состоянии доказать Борису, что он обладает некой секретной информацией, однако разглашать данную информацию перед Борисом будет совсем не обязательно.

Доказательство носит интерактивный характер. Борис задает Антону серию вопросов. Если Антон знает секрет, то ответит правильно на все заданные ему вопросы. Если не знает, вероятность правильного ответа на каждый из вопросов будет невелика. После примерно 10 вопросов Борис будет точно знать, обманывает ли его Антон. При этом шансы Бориса извлечь для себя какую-либо полезную информацию о сути самого секрета практически равны нулю.

Протокол доказательства с нулевым разглашением конфиденциальной информации

Использование доказательства с нулевым разглашением конфиденциальной информации можно пояснить на конкретном примере.

Предположим, что имеется пещера, точка входа в пещеру обозначена буквой A, в точке B пещера разветвляется на две половины - C и D (см. рисунок). У пещеры есть секрет: только тот, кто знает волшебные слова, может открыть дверь, расположенную между C и D.

Антону волшебные слова известны, Борису - нет. Антон хочет доказать Борису, что знает волшебные слова, но так, чтобы Борис по-прежнему оставался в неведении относительно этих слов. Тогда Антон может воспользоваться следующим протоколом:

1. Борис стоит в точке A.

2. По своему выбору Антон подходит к двери либо со стороны точки C, либо со стороны точки D.

3. Борис перемещается в точку B.

4. Борис приказывает Антону появиться или (а) - через левый проход к двери, или (б) - через правый проход к двери.

5. Антон подчиняется приказу Бориса, в случае необходимости используя волшебные слова, чтобы пройти через дверь.

6. Шаги 1-5 повторяются n раз, где n - параметр протокола.

Допустим, что у Бориса есть видеокамера, с помощью которой он фиксирует все исчезновения Антона в недрах пещеры и все его последующие появления с той или иной стороны. Если Борис покажет записи всех n экспериментов, произведенных им совместно с Антоном, смогут ли эти записи послужить доказательством знания Антоном волшебных слов для другого человека (например, для Владимира)?

Вряд ли. Владимир никогда не сможет полностью удостовериться в том, что Антон каждый раз предварительно не сообщал Борису, с какой стороны он направится к двери, чтобы потом Борис приказывал ему выходить именно с той стороны, с какой Антон зашел. Или что из сделанной видеозаписи не вырезаны все неудачные эксперименты, в ходе которых Антон появлялся совсем не с той стороны, с какой ему приказывал Борис.

Это означает, что Борис не в состоянии убедить Владимира, лично не присутствовавшего при проведении экспериментов в пещере, в том, что Антон действительно подтвердил там свое знание секрета. А значит, использованный Антоном протокол доказательства характеризуется именно нулевым разглашением конфиденциальной информации. Если Антон не знает волшебные слова, открывающие дверь в пещере, то, наблюдая за Антоном, не сможет ничего узнать и Борис. Если Антону известны волшебные слова, то Борису не поможет даже подробная видеозапись проведенных экспериментов. Во-первых, поскольку при ее просмотре Борис увидит только то, что уже видел живьем. А во-вторых, потому что практически невозможно отличить сфальсифицированную Борисом видеозапись от подлинной.

Протокол доказательства с нулевым разглашением срабатывает в силу того, что, не зная волшебных слов, Антон может выходить только с той стороны, с которой зашел. Следовательно, только в 50 % всех случаев Антон сумеет обмануть Бориса, сумев выйти именно с той стороны, с которой тот попросит. Если количество экспериментов равно n, то Антон успешно пройдет все испытания только в одном случае из 2n. На практике можно ограничиться n=16. Если Антон правильно исполнит приказ Бориса во всех 16 случаях, значит, он и вправду знает волшебные слова.

Пример с пещерой является очень наглядным, но имеет существенный изъян. Борису будет значительно проще проследить, как в точке B Антон поворачивает в одну сторону, а потом появляется с противоположной стороны. Протокол доказательства с нулевым разглашением здесь попросту не нужен.

Поэтому предположим, что Антону известны не какие-то там волшебные слова типа "Сезам, откройся". Нет, Антон владеет более интересной информацией - он первым сумел справиться с труднорешаемой задачей. Чтобы доказать этот факт Борису, Антону совсем не обязательно публично демонстрировать свое решение. Ему достаточно применить следующий протокол доказательства с нулевым разглашением конфиденциальной информации:

1. Антон использует имеющуюся у него информацию и сгенерированное случайное число, чтобы свести труднорешаемую задачу к другой труднорешаемой задаче, изоморфной исходной задаче. Затем Антон решает эту новую задачу.

2. Антон задействует протокол предсказания бита для найденного на шаге 1 решения, чтобы впоследствии, если у Бориса возникнет необходимость ознакомиться с этим решением, Борис мог бы достоверно убедиться, что предъявленное Антоном решение действительно было получено им на шаге 1.

3. Антон показывает новую труднорешаемую задачу Борису.

4. Борис просит Антона

или (а) - доказать, что две труднорешаемые задачи (старая и новая) изоморфны,

или (б) - предоставить решение, которое Антон должен был найти на шаге 1, и доказать, что это действительно решение задачи, к которой Антон свел исходную задачу на том же шаге.

5. Антон выполняет просьбу Бориса.

6. Антон и Борис повторяют шаги 1-6 n раз, где n - параметр протокола.

Труднорешаемые задачи, способ сведения одной задачи к другой, а также случайные числа должны по возможности выбираться так, чтобы у Бориса не появилось никакой информации относительно решения исходной задачи даже после многократного выполнения шагов протокола.

Не все труднорешаемые задачи могут быть использованы при доказательстве с нулевым разглашением конфиденциальной информации, однако большинство из них вполне пригодны для таких целей. Примерами могут служить отыскание в связном графе цикла Гамильтона (замкнутого пути, проходящего через все вершины графа только один раз) и определение изоморфизма графов (два графа изоморфны, если они отличаются только названиями своих вершин).

**Параллельные доказательства с нулевым разглашением конфиденциальной информации**

Обычный протокол доказательства с нулевым разглашением конфиденциальной информации требует, чтобы Антон и Борис последовательно повторили его шаги n раз. Можно попробовать выполнять действия, предусмотренные этим протоколом, одновременно:

1. Антон использует имеющуюся у него информацию и n сгенерированных случайных чисел, чтобы свести труднорешаемую задачу к n другим труднорешаемым задачам, изоморфным исходной задаче. Затем Антон решает эти n новых задач.

2. Антон задействует протокол предсказания бита для найденных на шаге 1 n решений, чтобы впоследствии, если у Бориса возникнет необходимость ознакомиться с этими решениями, Борис мог бы достоверно убедиться, что предъявленные Антоном решения действительно были получены им на шаге 1.

3. Антон показывает n новых труднорешаемых задач Борису.

4. Для каждой из n новых труднорешаемых задач Борис просит Антона

или (а) - доказать, что она изоморфна исходной труднорешаемой задаче,

или (б) - предоставить решение этой задачи, которое Антон должен был найти на шаге 1, и доказать, что оно действительно является ее решением.

5. Антон выполняет все просьбы Бориса.

На первый взгляд параллельный протокол обладает тем же свойством нулевого разглашения конфиденциальной информации, что и обычный. Однако строгого доказательства этого факта еще не найдено. А пока с полной определенностью можно сказать лишь одно: некоторые интерактивные протоколы доказательства с нулевым разглашением в некоторых ситуациях можно выполнять параллельно, и от этого они не утрачивают свойство нулевого разглашения конфиденциальной информации.

**Неинтерактивные протоколы доказательства с нулевым разглашением конфиденциальной информации**

Постороннее лицо, не участвующее в выполнении шагов интерактивного протокола доказательства с нулевым разглашением конфиденциальной информации, невозможно убедить в том, в чем в ходе реализации протокола убеждается Борис, а именно - что Антон действительно владеет конфиденциальной информацией. Чтобы преодолеть этот недостаток, потребуется применить неинтерактивный протокол, в котором вместо Бориса используется однонаправленная функция:

1. Антон использует имеющуюся у него информацию и n сгенерированных случайных чисел, чтобы свести труднорешаемую задачу к n другим труднорешаемым задачам, изоморфным исходной задаче. Затем Антон решает эти n новых задач.

2. Антон задействует протокол предсказания бита для найденных на шаге 1 n решений.

3. Антон подает n обязательств, полученных им на шаге 2, на вход однонаправленной функции.

4. Для каждой i-й труднорешаемой задачи, к которой Антон свел исходную задачу на шаге 1, он берет i-й бит значения, вычисленного с помощью однонаправленной функции, и

(а) если этот бит равен 1, то Антон доказывает, что исходная и i-я задачи изоморфны, или

(б) если этот бит равен 0, то Антон помещает в общедоступную базу данных решение i-й задачи, вычисленное на шаге 1.

5. Антон передает в общедоступную базу данных все обязательства, которые были получены им на шаге 2.

6. Борис, Владимир или любое другое заинтересованное лицо могут проверить правильность выполнения шагов 1-5 Антоном.

Удивительно, но факт: Антон предоставляет в общее пользование данные, которые позволяют любому убедиться в том, что он владеет некоторым секретом, и в то же время не содержат никакой информации о сути самого секрета.

Роль Бориса в этом протоколе исполняет однонаправленная функция. Если Антон не знает решения труднорешаемой задачи, он все равно может выполнить действия, предусмотренные или пунктом (а), или пунктом (б) шага 4 протокола, но отнюдь не обоими пунктами сразу. Поэтому, чтобы смошенничать, Антону придется научиться предсказывать значения однонаправленной функции. Однако, если функция действительно является однонаправленной, Антон не сможет ни догадаться, какими будут ее значения, ни повлиять на нее с тем, чтобы на ее выходе получилась нужная Антону битовая последовательность.

В отличие от интерактивного протокола, здесь требуется большее количество итераций. Поскольку генерация случайных чисел возложена на Антона, подбором этих чисел он может попытаться добиться, чтобы на выходе однонаправленной функции получилась битовая последовательность нужного ему вида. Ведь даже если Антон не знает решения исходной труднорешаемой задачи, он всегда в состоянии выполнить требования или пункта (а), или пункта (б) шага 4 протокола.

Тогда Антон может попытаться догадаться, на какой из этих пунктов падет выбор, и выполнить шаги 1-3 протокола. А если его догадка неверна, он повторит все сначала. Именно поэтому в неинтерактивных протоколах необходим больший запас прочности, чем в интерактивных. Рекомендуется выбирать n=64 или даже n=128.

Доказано, что в общем случае любое математическое доказательство может быть соответствующим образом преобразовано в доказательство с нулевым разглашением конфиденциальной информации. А это означает, что теперь математику вовсе не обязательно публиковать результаты своих научных исследований. Он может доказать своим коллегам, что нашел решение какой-то математической проблемы, не раскрывая перед ними сути найденного решения.

**Удостоверение личности с нулевым разглашением конфиденциальной информации**

В повседневной жизни людям регулярно приходится удостоверять свою личность. Обычно они делают это путем предъявления паспортов, водительских прав, студенческих билетов и других подобных документов. Такой документ обычно имеет некоторую индивидуальную отличительную особенность, которая позволяет однозначно связать его с определенным лицом. Чаще всего это фотография, иногда - подпись, реже - отпечатки пальцев или рентгеновский снимок зубов. Можно ли делать то же самое с помощью криптографии?

Конечно. В этом случае для удостоверения личности Антона используется его тайный криптографический ключ. Применяя доказательство с нулевым разглашением конфиденциальной информации, Антон может продемонстрировать любому, что знает свой тайный ключ, и тем самым однозначно идентифицировать себя. Идея цифровой идентификации весьма заманчива и таит в себе массу разнообразных возможностей, однако у нее есть ряд существенных недостатков.

Во-первых, злоумышленник Зиновий под фальшивым предлогом может попросить Антона предъявить свое цифровое удостоверение личности. Одновременно с помощью современных средств связи Зиновий инициализирует процесс идентификации Антона совсем в другом месте и будет переадресовывать все запросы из этого места Антону, а данные им ответы - пересылать обратно. Например, Зиновий может связаться с ювелирным магазином и, выдав себя за Антона, оплатить из его кармана весьма дорогую покупку.

Во-вторых, Зиновий может запросто обзавестись несколькими тайными ключами, а следовательно, и заиметь соответствующее число цифровых удостоверений личности. Одно из них он использует единственный раз для финансовой аферы и больше им пользоваться не будет. Свидетелем преступления станет лицо, которому Зиновий предъявит свое "одноразовое" удостоверение личности, однако доказать, что это был именно Зиновий, не удастся. Ведь предусмотрительный Зиновий никогда не удостоверял таким образом свою личность прежде. Не станет он делать этого и впредь. А свидетель сможет только показать, какое удостоверение личности было предъявлено преступником. Однозначно связать это удостоверение с личностью Зиновия будет нельзя.

В-третьих, Антон может попросить Зиновия одолжить на время его цифровое удостоверение личности. Мол, Антону надо съездить в Соединенные Штаты, а поскольку он - бывший сотрудник советской разведки, работавший против США, американское правительство наотрез отказывает ему во въездной визе. Зиновий с радостью соглашается: после отъезда Антона он может пойти практически на любое преступление, поскольку обзавелся "железным" алиби. С другой стороны, ничто не мешает совершить преступление Антону. Кто поверит лепету Зиновия о том, что он одолжил свое цифровое удостоверение личности какому-то другому человеку?

Избавиться от перечисленных недостатков помогают дополнительные меры предосторожности. В первом случае мошенничество стало возможным, поскольку Зиновий, проверяя цифровое удостоверение личности Антона, мог одновременно общаться с внешним миром по телефону или радио. Если Зиновия поместить в экранированную комнату без всяких средств связи, никакого мошенничества не было бы.

Чтобы исключить вторую форму мошенничества, необходимо ввести ограничение на количество ключей, которые человеку разрешается использовать, чтобы удостоверить свою личность (как правило, такой ключ должен существовать в единственном числе).

И наконец, чтобы не допустить третий вид мошенничества, требуется либо заставить всех граждан удостоверять свою личность как можно чаще (например, у каждого фонарного столба, как это делается в тоталитарных государствах), либо дополнить средства цифровой идентификации другими идентификационными методами (например, проверкой отпечатков пальцев).

**Неосознанная передача информации**

Предположим, что Борис безуспешно пытается разложить на простые множители 700-битовое число. При этом ему известно, что данное число является произведением семи 100-битовых множителей. На помощь Борису приходит Антон, который случайно знает один из множителей. Антон предлагает Борису продать этот множитель за 1000 рублей - по 10 рублей за бит. Однако у Бориса имеются в наличии лишь 500 рублей. Тогда Антон выражает желание отдать Борису 50 бит за половину цены. Борис сомневается, поскольку даже купив эти 50 бит, он все равно не сможет убедиться, что они действительно являются частью искомого множителя, пока не узнает все его биты целиком.

Чтобы выйти из тупика, Антон и Борис должны воспользоваться протоколом неосознанной передачи информации. В соответствии с ним Антон передает Борису несколько шифрованных сообщений. Борис выбирает одно из них и отсылает все сообщения обратно. Антон расшифровывает выбранное Борисом сообщение и снова отсылает Борису. При этом Антон остается в неведении относительно того, какое именно сообщение выбрал для себя Борис.

Протокол неосознанной передачи информации не решает всех проблем, которые стоят перед Антоном и Борисом, желающими заключить сделку о купле-продаже одного из множителей 700-битового числа. Чтобы сделка стала честной, Антон должен будет доказать Борису, что проданные 50 бит действительно являются частью одного из простых множителей, на которые раскладывается это число. Поэтому Антону скорее всего придется дополнительно воспользоваться еще и протоколом доказательства с нулевым разглашением информации.

Следующий протокол позволяет Антону послать два сообщения, одно из которых будет принято Борисом, но какое именно, Антон так и не узнает.

1. Антон генерирует две пары ключей, состоящих из открытого и тайного ключа, и отсылает оба открытых ключа Борису.

2. Борис генерирует ключ для симметричного алгоритма (например, для DES-алгоритма), шифрует этот ключ при помощи одного из открытых ключей, присланных Антоном, и отсылает обратно Антону.

3. Антон расшифровывает ключ Бориса с помощью каждого из двух своих тайных ключей, сгенерированных им на шаге 1, и получает две битовых последовательности. Одна из них является подлинным ключом для DES-алгоритма, а другая содержит произвольный набор битов.

4. Антон шифрует два сообщения по DES-алгоритму, используя в качестве ключей обе битовые последовательности, которые были получены им на шаге 3, и отсылает результаты шифрования Борису.

5. Борис расшифровывает оба присланных Антоном сообщения на ключе, сгенерированном на шаге 2, и обретает два открытых текста сообщения, один из которых представляет собой настоящую тарабарщину, а второй - содержательное послание.

Теперь у Бориса имеется одно из двух сообщений Антона, однако последний не может со всей определенностью сказать, какое именно. К сожалению, если в протоколе не предусмотреть дополнительный проверочный шаг, у Антона будет возможность смошенничать (например, зашифровать на шаге 4 два идентичных сообщения). Поэтому необходим еще один, заключительный шаг протокола:

6. После того как отпала надобность хранить в секрете второе сообщение (к примеру, у Бориса нашлись еще 500 рублей, чтобы выкупить у Антона оставшуюся половину множителя), Антон предоставляет Борису свои тайные ключи, чтобы тот мог убедиться в честности Антона.

Протокол защищен от атаки со стороны Антона, поскольку на шаге 3 Антон не в состоянии отличить произвольную битовую последовательность от подлинного ключа DES-алгоритма, сгенерированного Борисом. Протокол также обеспечивает защиту от атаки со стороны Бориса, так как у того нет тайных ключей Антона, чтобы определить битовую последовательность, использованную Антоном в качестве ключа DES-алгоритма для шифрования второго сообщения.

Конечно, протокол неосознанной передачи информации отнюдь не гарантирует, что Антон не пошлет Борису какие-нибудь бессмысленные послания (типа "Борис - лох" или "Мяу-мяу") вместо битов одного из семи простых множителей, на которые раскладывается исходное 700-битовое число. Или что Борис вообще захочет с ними ознакомиться и примет участие в выполнении шагов этого протокола.

На практике протокол неосознанной передачи информации используется довольно редко. Обычно он служит в качестве одного из строительных блоков для построения других протоколов.

**Анонимные совместные вычисления**

Иногда бывает так, что группе людей требуется совместно вычислить некоторую функцию от многих переменных. Каждый участник вычислительного процесса является источником значений одной или нескольких переменных этой функции. Результат вычислений становится известен всем членам группы, однако ни один из них не в состоянии выяснить что-либо о значениях, поданных на вход функции другим членом группы.

**Вычисление средней зарплаты**

Допустим, что начальник отдела приказал своим подчиненным подсчитать среднюю зарплату в отделе. Начальник осведомлен о зарплате любого сотрудника, но слишком занят более важными делами, чтобы отвлекаться на подобные пустяки. Каждый сотрудник прекрасно знает собственную зарплату, но категорически не желает сообщать о ней сослуживцам. Чтобы сотрудники отдела могли просуммировать свои оклады, сохранив их в тайне от других, им следует воспользоваться следующим протоколом:

1. Антон генерирует случайное число, прибавляет его к своей зарплате, шифрует полученную сумму при помощи открытого ключа Бориса и затем передает то, что у него получилось, Борису.

2. На своем тайном ключе Борис расшифровывает результат, вычисленный Антоном, прибавляет к нему свою зарплату, шифрует полученную сумму при помощи открытого ключа Владимира и затем передает то, что у него получилось, Владимиру.

3. На своем тайном ключе Владимир расшифровывает результат, вычисленный Борисом, прибавляет к нему свою зарплату, шифрует полученную сумму при помощи открытого ключа Георгия и затем передает то, что у него получилось, Георгию.

4. На своем тайном ключе Георгий расшифровывает результат, вычисленный Владимиром, прибавляет к нему свою зарплату, шифрует полученную сумму при помощи открытого ключа Антона и затем передает то, что у него получилось, Антону.

5. На своем тайном ключе Антон расшифровывает результат, вычисленный Георгием, вычитает из него случайное число, сгенерированное на шаге 1, делит на количество сотрудников отдела и получает искомую среднюю зарплату в отделе.

Точность вычисления средней зарплаты зависит от честности каждого сотрудника. Если хотя бы один из участников протокола соврет относительно своего жалованья, итоговое значение будет неверным. Особенно большими потенциальными возможностями для злоупотреблений обладает Антон. На шаге 5 он может вычесть любое число, какое только придет ему в голову, и никто не заметит подделки. Поэтому необходимо обязать Антона воспользоваться какой-либо из схем предсказания бита. Однако если от Антона потребуется раскрыть перед всеми случайное число, сгенерированное им на шаге 1, зарплату Антона узнает Борис. Это значит, что начальнику отдела все же придется отвлечься и выполнить вычисления, предусмотренные шагом 2 протокола, самому. Ведь он и так в курсе размера оплаты труда Антона.

**Как найти себе подобного**

Антон любит играть с резиновыми куклами, изготовители которых потрудились на славу, тщательно скопировав в натуральную величину определенные особенности анатомического строения женщины. А Борису нравится во всех красочных подробностях наблюдать за жизнью соседей из многоквартирного дома напротив при помощи современных оптических приспособлений. Оба тщательно скрывают свои пристрастия от родственников, друзей и коллег по работе, но очень хотели бы найти людей, которые разделяют их интересы.

Фирма "Совместные анонимные вычисления" готова оказать необходимую помощь Антону, Борису и им подобным в подборе таких же чудаков, как они сами. Сотрудники фирмы составили всеобъемлющий список всех человеческих чудачеств, каждое из которых снабжено уникальным идентификатором из семи цифр. Обратившись в фирму, Антон и Борис принимают участие в выполнении шагов некоторого протокола, после чего узнают, испытывают ли они склонность к одним и тем же чудачествам. При положительном ответе они смогут связаться друг с другом и слиться во взаимном экстазе. Если ответ будет отрицательным, об их необычных пристрастиях не узнает никто, включая сотрудников фирмы.

Протокол выглядит так:

1. Используя однонаправленную функцию, Антон преобразует 7-значный идентификатор своего чудачества в другое 7-значное число.

2. Трактуя полученное на шаге 1 число как телефонный номер, Борис набирает этот номер и оставляет его абоненту свои координаты. Если на вызов никто не отвечает или такого телефонного номера не существует, Антон применяет к нему однонаправленную функцию и получает новое семизначное число. Так продолжается до тех пор, пока кто-нибудь не ответит на телефонный звонок Антона.

3. Антон сообщает в фирму, сколько раз Борис должен применять однонаправленную функцию, чтобы получить искомый телефонный номер.

4. С помощью однонаправленной функции Борис преобразует 7-значный идентификатор своего чудачества столько раз, сколько это делал Антон, и получает 7-значное число, которое трактует как телефонный номер. Борис звонит по полученному им номеру и спрашивает, нет ли для него какой-либо информации.

Следует отметить, что Борис может предпринять атаку с выбранным открытым текстом. Узнав идентификаторы распространенных человеческих чудачеств, Борис будет по очереди перебирать их, применять к ним однонаправленную функцию и звонить по получающимся у него телефонным номерам. Поэтому необходимо сделать так, чтобы количество возможных чудачеств было достаточно велико и подобного рода атака стала в результате неосуществимой.

**Депонирование ключей**

С незапамятных времен одним из наиболее распространенных методов слежки является подслушивание, включающее в себя перехват сообщений, которыми обмениваются люди, являющиеся объектами наблюдения. Сегодня, благодаря широкому распространению стойких криптосистем с открытым ключом, у преступников и террористов появилась возможность обмениваться посланиями по общедоступным каналам связи, не боясь подслушивания со стороны кого бы то ни было. В связи с этим у правоохранительных органов возникла настоятельная необходимость при определенных условиях осуществлять оперативный доступ к открытым текстам шифрованных сообщений, циркулирующих в коммерческих коммуникационных сетях.

В 1993 году американское правительство впервые публично объявило о своих планах внедрения Стандарта шифрования данных с депонированием ключа. В соответствии с этим стандартом для шифрования данных предполагается использовать защищенную микросхему под названием Clipper, которая снабжается уникальным идентификационным номером и депонируемым ключом. Депонируемый ключ состоит из двух частей, которые раздельно хранятся в двух различных уполномоченных правительственных ведомствах. Для шифрования открытого текста сообщения микросхема генерирует сеансовый ключ. Этот ключ шифруется при помощи депонируемого ключа и в зашифрованном виде присоединяется к шифрованному тексту сообщения вместе с идентификационным номером микросхемы. В случае возникновения необходимости ознакомиться с содержанием сообщения, зашифрованного при помощи микросхемы Clipper, правоохранительным органам достаточно в установленном порядке обратиться в уполномоченные правительственные ведомства за хранящимся там депонируемым ключом, расшифровать с его помощью сеансовый ключ, а затем прочесть искомый открытый текст сообщения.

В самом общем случае Стандарт шифрования данных с депонированием ключа реализуется с помощью следующего криптографического протокола:

1. Антон генерирует пару ключей, состоящую из открытого и тайного ключа, и делит их на n частей.

2. Антон посылает каждую часть тайного ключа и соответствующую ей часть открытого ключа отдельному доверенному лицу.

3. Каждое доверенное лицо проверяет полученные от Антона части открытого и тайного ключа и помещает их на хранение в надежное место.

4. Если правоохранительные органы добиваются разрешения ознакомиться с перепиской Антона, они обращаются к его доверенным лицам и реконструируют соответствующий тайный ключ.

Существуют различные варианты протокола шифрования данных с депонированием ключа. Например, в него можно встроить пороговую схему с тем, чтобы для восстановления тайного ключа нужно было собрать не все n, а лишь не менее m (m<n) частей этого ключа, распределенных Антоном среди своих доверенных лиц. Кроме того, протокол шифрования данных с депонированием ключа можно дополнить действиями, позаимствованными из протокола с неосознанной передачей информации, чтобы доверенные лица не знали, чей конкретно ключ они реконструируют в данный момент по просьбе правоохранительных органов.

**Электронная подпись**

*В настоящее время любой специалист в области технологий банковских расчетов хорошо знает о такой возможности авторизации электронных документов и банковских транзакций как цифровые подписи. Многие банки широко используют цифровую подпись при межбанковских и внутрибанковских расчетах, а также при работе с клиентами. Однако, наш пятилетний практический опыт работы с очень большим числом банков России, других стран СНГ и некоторыми банками стран "дальнего зарубежья" показал, что далеко не все вопросы технологии оформления и использования официально юридически значимых электронных документов с цифровыми подписями достаточно ясны даже специалистам по автоматизации банковских расчетов. Поэтому, я попытаюсь в данной публикации дать вразумительные ответы хотя бы на небольшую часть вопросов, наиболее часто задаваемых банковскими специалистами, в ходе практической реализации технологии цифровой подписи.*

**1. ПРИНЦИПЫ.**

Идея цифровой подписи, как законного средства подтверждения подлинности и авторства документа в электронной форме, впервые была сформулирована явно в 1976 году в статье двух молодых американских специалистов по вычислительным наукам из Стэндфордского университета Уитфилда Диффи и Мартина Хеллмана.

Суть ее состоит в том, что для гарантированного подтверждения подлинности информации, содержащейся в электронном документе, а также для возможности неопровержимо доказать третьей стороне (партнеру, арбитру, суду и т.п.), что электронный документ был составлен именно конкретным лицом, или по его поручению, и именно в том виде, в которм он предъявлен, автору документа предлагается выбрать свое индивидуальное число ( называемое обычно индивидуальным ключом, паролем, кодом, и т.д.) и каждый раз для "цифрового подписывания" сворачивать (замешивать) этот свой индивидуальный ключ, хранимый в секрете от всех, с содержимым конкретного электронного документа. Результат такого "сворачивания" - другое число, и может быть назван цифровой подписью данного автора под данным конкретным документом.

Для практического воплощения этой идеи требовалось найти конкретные и конструктивные ответы на следующие вопросы:

Как "замешивать" содержание документа с индивидуальным ключом пользователя, чтобы они стали неразделимы ?

Как проверять, что содержание подписываемого документа и индивидуальный ключ пользователя были подлинными, не зная заранее ни того, ни другого ?

Как обеспечить возможность многократного использования автором одного и того же индивидуального ключа для цифрового подписывания большого числа электронных документов ?

Как гарантировать невозможность восстановления индивидуального ключа пользователя по любому количеству подписанных с его помощью электронных документов ?

Как гарантировать, что положительным результат проверки подлинности цифровой подписи и содержимого электронного документа будет в том и только в том случае, когда подписывался именно данный документ и именно с помощью данного индивидуального ключа ?

Как обеспечить юридическую полноправность электронного документа с цифровыми подписями, существующего только в электронном виде без бумажного дубликата или заменителей ?

Для полноценных удовлетворительных ответов на все эти вопросы потребовалось около 20 лет. Сейчас мы можем точно и определенно сказать, что практические ответы на все эти вопросы получены. Мы располагаем полноценным арсеналом технических средств авторизации электронных документов, называемым цифровой подписью.

Рассмотрим эти ответы подробнее. Основная идея Диффи и Хеллмана состояла в том, чтобы искать ответы на первые четыре из списка вопросов (математические) по следующей схеме:

пользователи располагают средствами выбирать случайно свои индивидуальные ключи для подписывания из очень большого множества всех возможных ключей,

по каждому конкретно выбранному индивидуальному ключу для подписывания легко вычислить парный к нему ключ для проверки подписей,

процедура вычисления ключа проверки из ключа подписывания широко известна, практически реализуема и гарантирует невозможность восстановления ключа подписывания,

процедуры подписывания и проверки подписи широко известны, в каждой из них используется только один из пары ключей, и гарантируется невозможность получения неверного ответа, а также невозможность восстановления ключа подписывания по ключу проверки.

Самым сложным из этих условий является, конечно же, гарантирование невозможности восстановления ключа подписывания по ключу проверки и любому количеству подписанных электронных документов.

Лучший из предложенных на сегодня учеными способов его выполнения состоит в том, чтобы использовать такие процедуры подписывания и проверки, что практическое восстановление ключей подписи по ключам проверки требует решения известной сложной вычислительной задачи. Поскольку задача является общеизвестно сложной, то если ее не научились решать за обозримое время все математики мира во все предыдущие столетия, то есть некоторая надежда, что ее не сумеют решить быстро и в ближайшем будущем.

Практический результат последующих 20 лет научных поисков таких задач оказался до некоторой степени парадоксальным: при всем многообразии известных сложных вычислительных задач, практически применимой оказалась одна. Это так называемая задача дискретного логарифмирования.

В простейшем варианте ее можно сформулировать так. Если заданы три больших целых положительных числа

**a, n, x,**

то располагая даже несложными арифметическими устройствами типа карманного калькулятора, или просто карандашом и бумагой, можно довольно быстро вычислить число

**a\*\*x**

как результат умножения числа

**a**

на себя

**x**

раз,

а затем и остаток от деления этого числа нацело на **n**, записываемый как

**b = a\*\*x mod n**

задача же дискретного логарифмирования состоит в том, чтобы по заданным числам

**a, b, n**

связанным таким соотношением, найти то число

**x**

из которого по этой формуле было вычислено число **b.**

Оказывается, что задача дискретного логарифмирования при правильном выборе целых чисел настолько сложна, что позволяет надеяться на практическую невозможность восстановления числа x, - индивидуального ключа подписывания, по числу b, применяемому в качестве ключа проверки.

Чтобы говорить более определенно о практической невозможности решить ту или иную вычислительную задачу, следует предварительно договориться о том, какие вычислительные мощности и мозговые ресурсы доступны тому, кто предположительно будет эту задачу решать. Поскольку давать конкретные оценки возможностей потенциальных мозговых ресурсов будущего "взломщика" системы цифровой подписи дело весьма сложное и неблагодарное, мы будем просто исходить из предположения, что он располагает полной информацией о наилучших известных мировой науке методах решения данной задачи.

Далее, если он располагает вычислительной системой общей мощностью, скажем, 1 миллиард (10\*\*9 = 1 000 000 000) операций в секунду, а это мощность современного суперкомпьютера типа CRAY-3, то

- за сутки непрерывной работы такой системы может быть решена задача сложностью около 100 000 миллиардов (или 10\*\*14) операций

- за месяц - около **3\*(10\*\*15),**

- за год - около **3\*(10\*\*16),**

- за 10 лет - около **3\*(10\*\*17),**

- за 30 лет - около **10\*\*18** операций.

Таким образом, даже если допустить, что потенциальный взломщик цифровой подписи располагает вычислительной системой эквивалентной по мощности 1000 суперкомпьютерам типа CRAY-3, то на выполнение вычислений объемом **10\*\*21** операций ему потребовалось бы не менее 30 лет непрерывной работы всей системы, что с практической точки зрения означает невозможность их выполнения.

Поэтому, цифровая подпись с надежностью не менее **10\*\*21** может считаться практически неподделываемой.

В этом месте автору обычно задают вопрос: "А что, если где-то в недрах специальных служб известны более совершенные методы решения этой задачи, которые могут быть применены для фальсификации цифровых подписей?"

В настоящее время ответ на него оказывается довольно простым. Если вы боитесь, что обычно предлагаемого при длине ключей в 64 байта запаса надежности в 10\*\*18 - 10\*\*21 недостаточно, применяйте алгоритмы с более длинными ключами. Современные цифровые процессоры Intel486 и Pentium позволяют за доли секунды вычислять и проверять цифровые подписи с ключами до 512 байт, а стойкость большинства широко применяемых методов цифровой подписи при такой длине ключей заведомо превосходит все разумные требования ( более чем 10\*\*50).

Итак, как видим, современные принципы построения системы цифровой подписи, общепризнанные в мире, просты и изящны:

методы вычисления и проверки цифровых подписей всех пользователей системы одинаковы, всем известны и основываются на широко известных математических задачах,

методы вычисления ключей проверки цифровых подписей из индивидуальных ключей подписывания одинаковы для всех и хорошо известны, их надежность также основывается на широко известных математических задачах,

индивидуальные ключи подписывания выбираются самими пользователями по случайному закону из большого множества всех возможных ключей,

при конкретном алгоритме цифровой подписи его стойкость может быть оценена без привлечения какой-либо "закрытой" информации на основе только известных математических результатов и разумных допущений о вычислительных мощностях потенциального "взломщика", посколку она базируется на общедоступных теоретических результатах по оценке сложности широко известных сложных вычислительных задач.

**2. АЛГОРИТМЫ.**

Проведем теперь сопоставление некоторых конкретных алгоритмов цифровой подписи с целью выявления их преимуществ и недостатков в различных ситуациях.

Для удобства оценки основных свойств того или иного алгоритма мы будем сравнивать его основные характеристики:

длину ключей,

длину цифровой подписи,

сложность (время) вычисления и

сложность (время) проверки подлинности цифровой подписи

при условии, что уровень стойкости подписи по отношению к любым методам фальсификации не ниже, чем 10\*\*21 (или 30 лет непрерывной работы сети из 1000 суперкомпьютеров).

В качестве "базовой" длины ключей и длины самой цифровой подписи мы будем рассматривать длину в 64 байта.

**RSA.** Первым по времени изобретения конкретным алгоритмом цифровой подписи был разработанный в 1977 году в Массачусетском технологическом институте алгоритм RSA.

Алгоритм RSA основывается на том математическом факте, что задача дискретного логарифмирования при выборе целого параметра n в виде произведения двух различных простых чисел примерно равных по порядку величины, т.е.

**n = p\*q**

становится не менее сложной, чем разложение n на эти простые множители, а последняя задача давно (еще со времен Архимеда и Евклида) известна в математике как сложная.

По современным оценкам сложность задачи разложения на простые множители при целых числах n из 64 байт составляет порядка 10\*\*17 - 10\*\*18 операций, т. е. находится где-то на грани досягаемости для серьезного "взломщика". Поэтому обычно в системах цифровой подписи на основе алгоритма RSA применяют более длинные целые числа n (обычно от 75 до 128 байт).

Это соответственно приводит к увеличению длины самой цифровой подписи относительно 64-байтного варианта примерно на 20% -100% (в данном случае ее длина совпадает с длиной записи числа n), а также от 70% до 800% увеличивает время вычислений при подписывании и проверке.

Кроме того, при генерации и вычислении ключей в системе RSA необходимо проверять большое количество довольно сложных дополнительных условий на простые числа p и q (что сделать достаточно трудно и чего обычно не делают, пренебрегая вероятностью неблагоприятного исхода - возможной подделки цифровых подписей)., а невыполнение любого из них может сделать возможным фальсификацию подписи со стороны того, кто обнаружит невыполнение хотя бы одного из этих условий (при подписывании важных документов допускать, даже теоретически, такую возможность нежелательно).

В дополнение ко всем этим алгоритмическим слабостям метода RSA следует также иметь в виду, что он защищен патентом США и поэтому любое его использование на территории США или западноевропейских стран требует приобретения соответствующей лицензии на использование, стоимость которой на 100 пользователей составляет $5000.

**EGSA.** Существенным шагом вперед в разработке современных алгоритмов цифровой подписи был новый алгоритм Т. ЭльГамаля, предложенный им в 1984 году. В этом алгоритме целое число **n** полагается равным специально выбранному большому простому числу **p,** по модулю которого и производятся все вычисления. Такой выбор позволяет повысить стойкость подписи при ключах из 64 байт примерно в 1000 раз, т.е. при такой длине ключей обеспечивается необходимый нам уровень стойкости порядка 10\*\*21. Правда, при этом длина самой цифровой подписи увеличивается в два раза и составляет 128 байт.

Главная "заслуга" алгоритма ЭльГамаля состояла в том, что в дальнейшем он послужил основой для принятия нескольких стандартов цифровой подписи, в том числе национального стандарта США DSS, введенного в действие 1 декабря 1994 года и государственного стандарта РФ ГОСТ Р 34.10, введенного с 1 января 1995 года.

**DSA.** Национальным институтом стандартов и технологий СЩА в 1991 году на основе алгоритма ЭльГамаля был разработан и представлен на рассмотрение Конгресса США новый алгоритм цифровой подписи, получивший название DSA (сокращение от Digital Signature Algorithm). Алгоритм DSA, ставший в дальнейшем основой национального стандарта США на цифровую подпись имеет по сравнению с алгоритмом RSA целый ряд преимуществ:

во-первых, при заданном уровне стойкости цифровой подписи целые числа, с которыми приходится проводить вычисления, имеют запись как минимум на 20% короче, что соответственно уменьшает сложность вычислений не менее, чем на 70% и позволяет заметно сократить объем используемой памяти;

во-вторых, при выборе параметров достаточно проверить всего три достаточно легко проверяемых условия;

в-третьих, процедура подписывания по этому методу не позволяет вычислять (как это возможно в RSA) цифровые подписи под новыми сообщениями без знания секретного ключа.

Эти преимущества, а также соображения, связанные с возможностью его реализовывать любым разработчиком свободно без коммерческих лицензионных соглашений с держателями патента, компанией RSA Data Security, и возможностью свободного безлицензионного экспорта такой технологии из США послужили главным мотивом для принятия в 1994 году национального стандарта цифровой подписи (DSS) на его основе.

Такое решение отнюдь не было очевидным, поскольку RSA, как наиболее известный алгоритм цифровой подписи и шифрования с открытым ключом, был гораздо шире распространен, практически опробован во многих странах и признан как стандарт de facto большинством разработчиков операционных систем, сетевых технологий и прикладного программного обеспечения. Популярность его объясняется, прежде всего, 8-летним опережением по времени появления, значительно более широкой известностью как самого алгоритма, так и его авторов в научных кругах, а также успешным бизнесом держателя патента - компании RSA Data Security, Inc. (сам автор алгоритма ЭльГамаль был в 1994-1995 гг. ее сотрудником).

Технические преимущества алгоритма, о которых мы говорили выше видны были лишь специалистам в области криптографии. Однако, в данной ситуации именно они оказались определяющими, и мир получил далеко не худший по тем временам стандарт. В настоящее время алгоритм DSA уже не является лучшим из возможных алгоритмов цифровой подписи по техническим параметрам, но вероятность его принятия в качестве международного стандарта остается достаточно большой.

По сравнению с оригинальным алгоритмом ЭльГамаля метод DSA имеет одно важное преимущество, - при заданном в стандарте уровне стойкости, числа, участвующие в вычислении подписи, имеют длину по 20 байт каждое, сокращая общую длину подписи до 40 байт.

Поскольку большинство операций при вычислении подписи и ее проверке также производится по модулю из 20 байт, сокращается время вычисления подписи и объем используемой памяти.

В алгоритме ЭльГамаля длина подписи при таком уровне стойкости была бы равна 128 байт.

**НОТАРИУС.** Поскольку в 1991 году наиболее распространенной моделью персонального компьютера в СССР был AT/286(12) то мы в своих ранних алгоритмических разработках должны были максимально упростить лучшие из известных тогда алгоритмов цифровой подписи, чтобы их программная реализация на таком процессоре позволяла вычислять и проверять подпись под электронными документами за разумное время, скажем, 1-2 секунды при размере документа до 10 KB.

Такие упрощения не должны были, конечно, снижать стойкости алгоритма, но за счет модификации процедур вычисления и проверки цифровой подписи, должны были его ускорить достаточно, чтобы подписывание и проверка цифровой подписи под электронным документом не вызывала заметных задержек в процессе его обработки на персональном компьютере.

Первым результатом такой работы был созданный в конце 1992 года аналог алгоритма ЭльГамаля НОТАРИУС-1.Основное отличие алгоритма НОТАРИУС-1 от алгоритма ЭльГамаля состоит в том, что вместо обычной операции умножения целых чисел по модулю большого простого **p**, как это делается у ЭльГамаля, алгоритм НОТАРИУС-1 использует похожую операцию, эффект от использования которой состоит в том, что обеспечивая точно такой же уровень стойкости, что и умножение по модулю простого числа, эта операция гораздо эффективней вычисляется на распространенных процессорах Intel, Motorola и др.

Процедуры подписывания электронных документов и проверки цифровых подписей по алгоритму НОТАРИУС-1 выглядят аналогично соответствующим процедурам алгоритма ЭльГамаля, обеспечивают тот же уровень стойкости подписи, но выполняются быстрее.

Затем, аналогичным образом был усовершенствован алгоритм DSA, который послужил основой для алгоритма цифровой подписи, названного НОТАРИУС-D.

Реализация этого алгоритма на стандартном процессоре Intel486DX4(100) позволила добиться времени подписывания электронного документа объемом 1 KB вместе с его предварительным хэшированием в 0.014 сек., а времени проверки подписи под документами такого объема, - 0.027 сек.

Если же объем документа равен 100 KB , время подписывания составляет 0.124 сек., а время проверки - 0.138 сек. Длина подписи 40 байт, стойкость - 10\*\*21.

Дальнейшее совершенствование алгоритмов подписывания и проверки произошло за счет использования совместно с нашими, также запатентованных в США и Германии идей немецкого криптографа Клауса Шнорра, который предоставил нам право использования своего алгоритма на территории стран СНГ. Совместное применение этих идей привело в 1996 году к разработке алгоритма НОТАРИУС-S, который при сохранении стойкости подписи позволил сократить ее длину еще на 32.5%. Для базового варианта с ключами из 64 байт длина подписи сократилась относительно DSA и НОТАРИСА-D с 40 байт до 27 байт. Соответственно уменьшилось время вычисления и проверки подписи. Стойкось осталась на том же уровне - 10\*\*21.

Эти алгоритмические разработки позволили нам предложить пользователю широкий выбор программ с длинами цифровой подписи от 16 до 63 байт и уровнями стойкости, соответственно, от 10\*\*14 (или несколько дней работы сети из несколькими десятков персональных компьютеров) до 10\*\*54 (или более 100 миллиардов лет непрерывной работы любой мыслимой вычислительной системы обозримого будущего). Более детальные технические характеристики различных алгоритмов приведены ниже, в Таблице 1.

Автор надеется, что параметры алгоритмов, приведенные в таблице, дадут читателю возможность оценить их основные качества без дальнейших пространных комментариев. Дополнительных пояснений требуют только разделы таблицы, посвященные алгоритму ГОСТ 34.10.

**ГОСТ34.10.** Стандарт на электронную подпись ГОСТ34.10 был опубликован впервые Госстандартом РФ в мае 1994 года и введен в действие с 1 января 1995 года. В предварительном варианте он был введен в качестве ведомственного стандарта на цифровую подпись ЦБ РФ и использовался в этом качестве с сентября 1993 года по декабрь 1994 года. Алгоритмы вычисления и проверки подписи в ГОСТ34.10 устроены аналогично алгоритму DSA, но предварительная обработка электронных документов перед подписыванием (так называемое хэширование) выполняются по другому, существенно более медленному способу. К сожалению, разработчики допустили целый ряд досадных ошибок, которые есть даже в официальном тексте стандарта. Поэтому при реализации следует быть внимательным и не всегда следовать формальному тексту.

Мы рассматриваем следующие виды угроз:

1. Предполагаем, что попытки подделать подпись предпринимают не профессионалы. "Злоумышленники" могут располагать сетью из нескольких персональных компьютеров, общая вычислительная мощность которой равна 2\*108 операций/сек.

Предполагаем, что "противостоим" профессионалам с вычислительной системой общей мощностью до 1012 операций/ сек. Это может быть сеть из нескольких десятков мощных современных суперкомпьютеров.

Предполагаем, что "противостоим" самой мощной государственной спецслужбе, располагающей возможностью ( и желанием ) создать для этой задачи сеть из сотен специализированных параллельных суперкомпьютеров с 1000 специальных мощных

( по 1013 оп./ сек.) процессоров каждый и практически неограниченной памятью.

Фантазии на тему будущего.

Фантазии на тему далекого будущего.

**СЕРТИФИКАЦИЯ.**

Принятые в различных странах в настоящее время процедуры сертификации, которые могут быть применены к программам или программно-аппаратным реализациям цифровой подписи, состоят в проверке соответствия, реализованных разработчиком алгоритмов описанным в официальных текстах стандартов.

В США, аккредитованные Национальным институтом стандартов и технологий лаборатории проводят тестирование процедуры порождения простых чисел, определяющих параметры алгоритма DSA, на основании опубликованных в тексте стандарта конкретных значений параметров и начальных установок процедуры генерации простых чисел, затем, при тестовых значениях параметров алгоритма, тестовых индивидуальных ключах и тестовых рандомизирующих значениях подписывания производится вычисление и проверка цифровых подписей под тестовыми примерами электронных документов. Таких циклов тестирования может быть довольно много - до нескольких десятков тысяч. Вся последовательность результатов предъявляется в лабораторию для сравнения с результатами работы эталонной программы на таких же значениях входных параметров. По результатам сравнения делается заключение о соответствии данной реализации цифровой подписи стандарту.

Таким же или примерно таким образом происходит процесс сертификации программ цифровой подписи и в ряде западноевропейских стран.

У нас ситуация оказывается, мягко говоря, парадоксальной. Поскольку в официальном тексте стандарта есть ошибки, которые, будь он реализован строго формально, привели бы к совершенно другому алгоритму цифровой подписи, о стойкости которого можно только догадываться (особенно при специальном "неудачном" выборе параметров), то проверить для программных или аппаратных реализаций "соответствие стандарту ГОСТ34.10" просто невозможно. Если реализация абсолютно точно соответствует формальному тексту стандарта с ошибками, то неясно, что это означает с точки зрения надежности подписи, а если при реализации эти ошибки были "учтены", то такая реализация не может соответствовать стандарту. Поэтому все бумаги, в которых в настоящее время такое соответствие декларируется, не означают абсолютно ничего.

Более разумный подход проявляется при сертификации в рамках Гостехкомиссии РФ программ цифровой подписи в классе программных средств защиты информации в от несанкционированного доступа и изменения. Согласно руководящих документов Гостехкомиссии программные или аппаратные средства, реализующие технологию цифровой подписи могут быть объективно оценены на предмат соответствия конкретным официально опубликованным требованиям по степени защиты информации от несанкционированного изменения путем ее подписывания цифровыми подписями.

**ЛИЦЕНЗИРОВАНИЕ.**

До последнего времени было не совсем ясно как будут наши законы трактовать вопросы распространения технологии цифровой подписи и, в частности возможность их экспорта. Дело в том, что при явном противоречии как с принципами построения систем цифровой подписи, так и просто со здравым смыслом чиновники некоторых ведомств пытались отнести эту технологию чуть ли не к разряду особо охраняемых государством наравне с ядерным или другими видами оружия массового поражения или сверх секретными специальными шифровальными средствами для особо важной государственной информации.

К счастью, за последнее время произошли заметные изменения, проясняющие ситуацию в этом вопросе. Президент РФ 26 августа 1996 года подписал Указ №1268, регламентирующий экспорт товаров и технологий двойного назначения. Согласно примечаниям к списку технологий двойного применения, на которые распространяется действие этого указа, из программного обеспечения, в том числе криптографического, экспорт которого из РФ регламентируется и требует специальных лицензий, сделаны следующие исключения.

Общедоступное:

а) проданное из фондов в розничные торговые точки и предназначенное для:

сделок по продаже в розницу;

сделок по высылке товаров по почте; или

сделок по телефонным заказам; и

б) разработанное для установки пользователем без дальнейшей реальной поддержки снабженцем

(продавцом), или

2. "В общественной сфере".

Кроме того, в тексте примечаний к указу, в части терминологии приводятся следующие интересные определения.

Криптография - дисциплина, включающая принципы, средства и методы преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.

Криптография ограничена преобразованием информации с использованием одного или более секретных параметров (например, криптографических перемененных) или соответствующим управлением ключом.

Поскольку технология цифровой подписи:

очевидно, не обеспечивает сокрытия содержания подписанной информации,

не предотвращает ее видоизменения (содержимое подписанных документов можно видоизменять как угодно, и это собственно сама подпись никак не может предотвратить),

не обеспечивает и несанкционированного использования (подписанный электронный документ может быть точно также, как и бумажный использован не законно)

то получается, что она не относится к области криптографии вообще.

А что же, собственно, мы получаем благодаря этой технологии ?

**Электронные деньги**

**1. Внесетевые платежные системы**

Рассмотрим платежные инструменты которые сейчас являются современными, доступными для общего пользования и в последнее время все чаще и чаще соперничают с тем, что мы привыкли называть деньгами в наличной и безналичной форме. Первыми из этих инструментов рассмотриваются пластиковые карточки так как они являются наиболее близкими к наличным деньгам, уже достаточно устоявшимися и привычными для пользователей.

Идея кредитной карточки была выдвинута еще в прошлом веке Эдуардом Беллами (Edward Bellami. Looking Backward: 2000 - 1887), однако впервые картонные кредитные карточки начали применяться на торговых предприятиях США только в 20-е годы нашего столетия. Поиск подходящего материала затянулся на десятилетия, и лишь в 60-е годы было найдено приемлемое решение - пластиковая карточка с магнитной полосой /4/.

Десять лет спустя, в 1975 г. француз Ролан Морено изобрел и запатентовал электронную карту памяти. Прошло еще несколько лет, и компания Bull (Франция) разработала и запатентовала смарт-карту со встроенным микропроцессором. С того времени и по сей день идет конкурентная борьба между картами с магнитной полосой и смарт-картами. Пока выигрывают первые - за счет широко распространенных и ставших уже традиционными платежных систем VISA, Eurocard/MasterCard, American Express, Diners Club и др. Однако огромные возможности, заложенные в концепции использования смарт-карт при безналичных расчетах, становятся все более привлекательными для банков, финансовых компаний и просто крупных предприятий с большим числом работающих.

Пластиковая карточка - это персонифицированный платежный инструмент, предоставляющий пользующемуся карточкой лицу возможность безналичной оплаты товаров и/или услуг, а также получения наличных средств в отделениях (филиалах) банков и банковских автоматах (банкоматах) /4/. Принимающие карточку предприятия торговли/сервиса и отделения банков образуют сеть точек обслуживания карточки (или приемную сеть).

Таким образом, пластиковые карты можно разделить на два типа:   
1) магнитные карты   
2) карты памяти.

* 1. Новые средства денежного обращения: эволюция, причины возникновения.

Выделяют три этапа в развитии цивилизации (финансовые эпохи), которые соответствуют трем видам носителей денежной информации.

1. Золото. Некий материальный субстрат, с физическими характеристиками которого прямым образом связана носимая на нем информация /11/. Для золотых денег такой физической характеристикой была масса. Верификация в такой денежной системе достаточно проста – по массе монеты и по ее химическому составу. Она не требует государственной поддержки либо требует ее в минимальной степени.
2. Бумага. Некий субстрат, на котором записана информация, но, с физическими характеристиками которого она не связана, либо связана очень опосредовано. Верификация требует использования мощного аппарата государственной защиты, подавление и запугивание против фальсификации.  
    Деньги, основанные на этих носителях, являются наличными, неименными, анонимными, распространяются они преимущественно вместе с их владельцем (в карманах и кошельках).
3. Электронные носители денежной информации. Деньги лишаются своих «твердых» копий. Они невидимы и распространяются внутри специальной информационной (банковской) системы. Верификация таких денег осуществляется специальными средствами «сетевого (информационного) администрирования» и в принципе нуждаются лишь в самой минимальной поддержке государства.  
    Электронные деньги относятся к безналичным деньгам, они распространяются без участия их владельцев, являются по преимуществу именными деньгами. Если денежная транзакция в системе золотых и бумажных денег является бинарной, то электронная денежная транзакция является n-ой, где n больше двух, в ней участвует плательщик, платежеполучатель и платежепроизводитель. Последний может быть представлен одним или даже несколькими субъектами денежных отношений (банками).

Двадцатый век – это эпоха бумажных денег, а его конец можно охарактеризовать как переходное время: от эпохи бумажных денег к электронным. Этот переход обусловлен тем, что бумажные деньги не удобны. Они ветшают, горят, требуют больших затрат на хранение, транспортировку и охрану, а также легко подделываемы.

**1.2. Магнитные карты**

Простейшим видом пластиковых карт является *магнитная карта*. Эта пластиковая карточка, соответствующая спецификациям ISO, имеет на обратной стороне магнитную полосу с информацией объемом около 100 байт, которая считывается специальным устройством. Такие магнитные карточки широко используются во всем мире в качестве кредитных (VISA, MasterCard, Eurocard и т. д.), а также как дебетовые банковские карточки в банкоматах. Магнитная полоса карточки имеет, как правило, три дорожки; в финансовой сфере в основном используют вторую. На ней постоянно хранится информация, включающая номер карты или банковского текущего счета, имя и фамилию владельца, срок годности карты (даты начала и конца срока). На магнитной полосе финансовой информации о состоянии счета владельца карты нет.

Существует два режима работы с магнитными картами. В *режиме on-line* устройство (торговый терминал, электронная касса, банкомат) считывает информацию с магнитной карты, которая по телефонной сети или спецканалу связи передается в центр авторизации карт. Здесь полученное сообщение обрабатывается, а затем в процессинговом центре со счета владельца карты либо списывается сумма покупки (дебетовые карты), либо на сумму покупки увеличивается долг владельца карты (кредитные карты). При этом, как правило, проверяется следующее: не является ли карта утерянной или украденной, достаточно ли средств на счете владельца (для дебетовых карт), не превышен ли лимит кредита (для кредитных). В *режиме off-line* информация о покупке, сделанной владельцем карточки, никуда не передается, а хранится в торговом терминале или электронной кассе. Для печати чеков используются специальные устройства ручной прокатки, дублирующие выгравированную на карточке информацию о ее владельце.

Банкоматы и торговые терминалы являются устройствами, обеспечивающими функционирование банковских систем самообслуживания на базе пластиковых карт. Банкомат (Automated Teller Machine, ATM) - это электронно-механическое устройство, предназначенное для выдачи наличных денег по пластиковым карточкам. Банкоматы принято делить на простейшие (cash dispenser) и полнофункциональные, выполняющие и другие операции: прием вкладов, выдачу справок о счетах, перевод денег и пр. В зависимости от предполагаемого места установки банкоматы делятся на уличные и внутренние (для помещений). Уличные банкоматы обычно встраиваются в стены зданий. Банкоматы любого типа включают процессор, дисплей с графическим монитором, клавиатуру для ввода информации, устройства для чтения/записи информации с пластиковой карты и на нее, а также для хранения (кассеты) и выдачи банкнот. Дополнительно банкоматы могут быть снабжены рулонными принтерами, устройствами приема денег и средствами безопасности.

При выдаче денег из банкоматов по обратной связи, как правило, запрашивается так называемый PIN-код - личный 4 - 6-значный код владельца карточки, что служит дополнительной защитой от мошенников. Эта мера безопасности была введена, чтобы предотвратить рост числа краж по пластиковым картам. Дело в том, что при использовании карты с магнитной полосой ее достаточно просто скопировать, но, не зная PIN-кода, нельзя воспользоваться копией в банкомате. Средством, обеспечивающим расчеты в магазине с помощью пластиковых карточек, служат торговые терминалы. Простейшими из них являются механические устройства для прокатки рельефной части пластиковой карты и получения специального чека (слипа), который подписывает клиент. В торговых терминалах PIN-коды обычно не применяют ввиду небольших списываемых сумм.

И немного статистики. Наибольшее распространение в США и Канаде получила платежная система на базе карточек American Express /4/. В США установлено свыше 60 тыс. банкоматов, обслуживающих эти карточки. В Европе более распространены карточки VISA и MasterCard. В частности, в Германии насчитывается более 29 тыс. банкоматов, обслуживающих эти карточки, во Франции - более 15 тыс., в Италии - более 6 тыс. В Испании более 20 тыс. банкоматов принимают карточки VISA и около 14 тыс. - MasterCard. Показатели American Express в Европе существенно скромнее: в Германии и Франции - около 2 тыс. банкоматов, в Италии - менее тысячи

**1.3. Карты памяти**

Более сложной является так называемая *карта памяти*, в которой нет магнитной полосы, зато встроена микросхема, содержащая память и устройство для записи/считывания информации. Объем памяти колеблется в достаточно широком диапазоне, однако в среднем не превышает 256 байт /5/. Такие карты имеют больше возможностей по сравнению с магнитными, но и стоят несколько дороже.

Наибольшее распространение в мире получили телефонные карты памяти, владельцы которых могут сделать определенное число телефонных звонков. Карточка применяется в контактном режиме (микросхема физически соприкасается с контактами считывающего устройства). При каждом новом контакте число "разрешенных" звонков в памяти карточки уменьшается на единицу. После того как лимит оплаченных звонков будет исчерпан, карточка перестает функционировать. Самой мощной из известных сегодня разновидностей "пластиковых денег" является *интеллектуальная карта (смарт-карта*). Такие карты содержат встроенный микропроцессор, могут иметь оперативную (для использования в процессе обработки) и постоянную (для хранения неизменяемых данных) память, а также встроенную систему обеспечения безопасности и защиты данных. Различают контактные и бесконтактные (работающие на расстоянии от считывающего устройства) смарт-карты. Смарт-карты используются в самых разных финансовых приложениях, обеспечивая сохранность, целостность и конфиденциальность информации. В частности, при совершении дебетовых или кредитных операций с помощью смарт-карт ее владелец может проверить, существует ли данный банк (торговый терминал) в действительности. Технологии интеллектуальных карт достаточно разнообразны, и возможности применения этих карт во многом зависят от избранной технологии и программно-аппаратных решений. Одно из наиболее распространенных приложений смарт-карт - их использование как электронных кошельков. *Электронные кошельки* позволяют хранить в своей памяти определенную сумму, тратить которую можно уже безо всякой авторизации. Необходимость в последней возникает только тогда, когда виртуальные деньги кончились, и карточку нужно "зарядить" новыми через терминалы типа банкоматов.

Наиболее продвинутыми на данный момент являются электронные кошельки производства компании Мondex /24/. Эти системы даже позволяют дать (или взять) деньги взаймы, если соответствующая операция производится между двумя клиентами Mondexа. От традиционной карточки карточку Mondex отличает наличие специального футляра, напоминающего по внешнему виду микрокалькулятор-книжечку. Ее "разворот" устроен таким образом, что с одной стороны находится гнездо для собственно карты, а с другой - миниатюрная клавиатура и дисплей С помощью этой карты такие действия, как проверка остатка денег, перевод "наличности" из одной валюты в другую и т.п. становятся доступными.

Кроме технологии Mondex, аналогичные платежные системы разрабатывают такие известные корпорации, как Visa и MasterCard. Повсеместное их внедрение позволит практически полностью отказаться от "натуральных" денег. С помощью новых карт можно расплачиваться с таксистами и даже давать чаевые в гостинице. Достаточно легко, уже сейчас, нарисовать следующую картину. Вы заходите пообедать и для оплаты достаете свой электронный бумажник с беспроводной связью. Из появившихся на табло кассы возможных для оплаты сумм 50 долларов и 5 ч. руб выбираете 5 ч.руб (частных рублей). Набираете на клавиатуре электронного бумажника известный только вам код, и указанная сумма поступает для оплаты на счет ресторана. Денежная единица "частный рубль" обозначает частную валюту, конкурирующую с долларами. Приблизительно так может выглядеть процедура работы с виртуальными деньгами в недалеком будущем.

Электронные бумажники уже появились, беспроводная связь тоже есть, осталось создать частную валюту, без которой, как утверждает теория цифровых денег, невозможно обеспечить полномасштабную электронную коммерцию. Вопрос о необходимости и сути частной валюты и/или цифровых денег будет рассмотрен позже.

Одним из наиболее серьезных аргументов в пользу "пластиковых денег" является сокращение оборота наличных средств (рублей и валюты). По самым оптимистичным оценкам, ежедневно в России в обороте находятся десятки тысяч тонн бумажных рублей. С крупными суммами наличных денег (изготовление, хранение, транспортировка, счет, проверка на подлинность и т. д.) связано много нкприятностей. Кроме этого в пользу "пластиковых денег" говорит и тот факт, что при открытом похищении карточки (грабеже, разбое) нападающий не сможет воспользоваться отнятыми средствами немедленно. Для получения наличных через банкомат необходимо узнать у жертвы PIN-код, места расположения банкоматов банка, выдавшего карточку. Владелец карточки может практически сразу заявить о пропаже (блокировать карту), и тогда грабитель вообще ничего не получит. Однако у пластиковых карт есть и недостатки.

Так, в России появилось поколение достаточно квалифицированных злоумышленников, способных изымать деньги из банкоматов по фальшивым пластиковым карточкам. Как уже отмечалось, карточки с магнитной полосой достаточно легко подделать, а PIN-код можно выяснить различными способами. "Пластиковые деньги" нельзя увидеть, нельзя подсчитать без специальной аппаратуры, поэтому, если их украдут, владелец сразу об этом и не узнает. Кроме того, реальные документы, которые можно было бы предъявить, например, в суде, отсутствуют.

**2. Сетевые платежные системы**

В предыдущей главе были рассмотрены те средства денежного обращения которые являются на данный момент современными и достаточно популярными, но не имеют никакого отношения к такой системе как Internet. Однако в последние годы Internet становится все более и более неотъемлемой частью нашего сегодняшнего существования и если раньше Internet была миром информации и развлечений, то в последнее время туда все более и более основательно перебирается бизнес. В связи с этим в Internet возникают новые типы платежных систем, которые с каждым днем становятся все более и более популярными.

Платежные системы, используемые сейчас в Internet, можно разделить на три основных типа:

1. Использование суррогатных платежных средств для оплаты в Internet.

2. Использование кредитных карточек для оплаты в рамках Internet.

3. Полноценные цифровые деньги.

Рассмотрим эти типы платежных средств в соответствии с названным порядком.

**2.1. Суррогатные платежные средства в INTERNET**

Наиболее примитивными и неудобными для расчетов на сегодняшний день являются различные типы *суррогатов используемых в рамках Internet*. Эти средства расчетов в Сети -- предлагаются сегодня несколькими компаниями, наиболее известны из которых First Virtual Holdings и Software Agents (знакомая более по торговой марке NetBank) /18/. Как правило суррогаты представлены в виде цифровых купонов и жетонов. Функционирование цифровых жетонов можно проиллюстрировать следующей схемой. Клиент за наличный или безналичный расчет приобретает у "банка" на некоторую сумму последовательности символов (для них "банк" гарантирует не тривиальность алгоритма генерации и уникальность каждого экземпляра), которыми расплачивается с торговцем. Торговец возвращает их в "банк" в обмен на ту же сумму, за вычетом комиссионных. При этом на "банке" лежит обязанность контролировать валидность поступающих жетонов (проверяя их наличие в регистре исходящих) и их единичность (проверяя отсутствие в регистре входящих). Стороны могут использовать криптографические средства защиты информации с открытыми ключами, чтобы избежать перехвата жетонов (рис. 1).

Такая система проста в реализации и эксплуатации. Это привело к тому, что рост активов First Virtual (абсолютная величина которых не сообщается) летом 1995 г. составлял 16% в неделю /18/. Однако правовой статус сделок с использование таких суррогатов остается очень расплывчатым, равно как и фискальные обязанности клиентов, приобретающих товары и услуги у торговцев, находящихся под другой юрисдикцией. Возможно, пока предоставляющие такого рода расчетные услуги компании будут придерживаться политики стопроцентной моментальной ликвидности эмитируемых ими купонов, вопрос о подведении их под статус финансовых институтов и не будет ставиться.

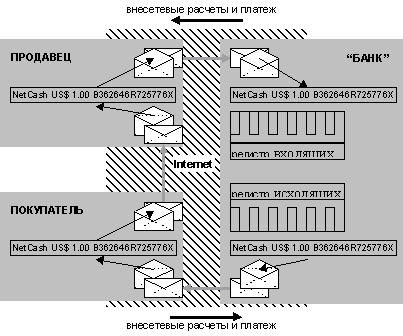


Рис. 1 Схема расчетов с использованием цифрового "жетона"

* соответствующая криптографическая операция.
  1. **Расчеты пластиковыми карточками в рамках INTERNET.**

Компания CyberCash, первой предложившая технологию, позволяющую использовать пластиковые карточки для расчетов в Сети /22/. Предлагаемое этой компанией программное обеспечение использует криптозащиту с открытым ключом для конфиденциальной передачи данных о пластиковой карточке от покупателя к торговцу   
(рис. 2). При этом все реальные расчеты и платежи производятся средствами процессинговых компаний без использования Internet. За CyberCash последовали и другие, а результатом этого процесса стало соглашение о совместной деятельности по предоставлению расчетных услуг в Internet, заключенное 9 января 1995 г. между MasterCard и производителем коммуникационного программного обеспечения Netscape (опубликованные позднее данные о дефектах в системе защиты, использованной в Netscape Navigator, впрочем, могут повлиять как на сроки реализации соглашения, так и на готовность владельцев карточек MasterCard воспользоваться предлагаемой в нем услугой).

Ряд банков, включая крупный британский Barklays Bank, пытаются внедрить сетевой вариант системы чекового обращения.

Сильная сторона таких решений состоит в том, что в большинстве стран уже существует детализированное законодательство, регламентирующее обращение чеков и пластиковых карточек. Значительны также маркетинговые преимущества использования таких имен, как MasterCard, Visa или Discover. Однако эти решения имеют общий с суррогатными коренной недостаток.

Чтобы понять суть этого недостатка, нужно обратиться к понятиям наличного и безналичного денежного обращения. Во всех современных национальных денежных системах обязательными к приему являются деньги как в форме наличных (банкнот и монет), так и в форме безналичных (записи на счетах в банке) средств. Обе эти формы в равной мере реализуют базовые функции денег: функцию посредника в обмене, позволяющего отделить акт купли от акта продажи во времени и пространстве, и функцию накопления покупательной способности. Однако в обращении наличных и безналичных денег имеется одно принципиальное различие. Сделка с использованием денег в наличной форме предполагает лишь соприсутствие контрагентов. Более того, наличные деньги являются оборотным финансовым документом, т.е. способны передавать абсолютно обоснованный правовой титул любому правомерному держателю. На этом основывается свойство наличных денег, которое можно обозначить как деперсонализацию сторон в сделке: для совершения сделки нет необходимости подтверждения личности контрагента.

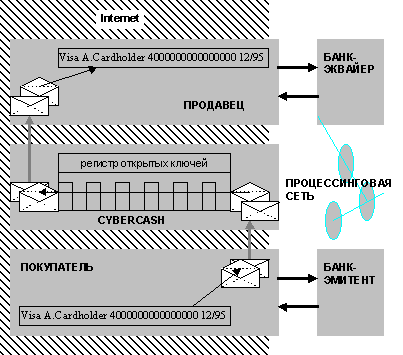


Рис. 2 Схема расчетов с использованием "закрытой" процедуры передачи  
 данных о кредитной карточке

- соответствующая криптографическая операция.

При использовании денег в безналичной форме в любой сделке участвует, кроме продавца и покупателя, еще одна сторона - финансовый институт (как минимум, один). Система безналичного обращения средств отделяет расчетный аспект сделки (договоренность о способах и сроках погашения задолженности) от платежного (окончательной передачи обязательного к приему средства погашения долга); позволяет оперировать временными лагами (периодом от инициации до совершения платежа), вводит различие дебетовых (инициируемых получателем) и кредитовых (инициируемых плательщиком) трансфертов; допускает взаимозачет (клиринг) задолженностей. В то же время, сделка с использованием безналичной формы денег (будь то векселя, чеки или пластиковые карточки) подразумевает возможность взаимной идентификации сторон, если не в момент сделки, то впоследствии. В некоторых случаях покупателю может быть выгодно поступиться правом на анонимность в обмен на определенные гарантии и льготы (например, использовав потребительский кредит). Однако во многих случаях невозможность аутентификации (подтверждения) личности важна для сохранения конфиденциальной коммерческой или лично значимой информации. Вот как описывал ситуацию Дэвид Чом (David Chaum), известный ученый-криптолог и бизнесмен, в 1992 г.:

"Каждый раз, когда вы звоните по телефону, покупаете товары с помощью кредитной карточки, подписываетесь на журнал или платите налоги, информация об этом попадает в какую-либо базу данных. Более того, все эти записи могут быть соединены таким образом, что составят единое досье о вашей жизни -- не только о вашем здоровье или финансах, но также и о том, что вы покупаете, где путешествуете и с кем общаетесь. Вам практически невозможно узнать суммарный объем информации о вас, хранящейся в различных организациях, а тем более -- убедиться, что она точна и доступна вам" ...

"Организации собирают записи из разных источников для защиты своих интересов ... Однако та же самая информация, попав в чужие руки, отнюдь не обеспечивает ни защиты предприятий, ни лучшего обслуживания потребителей. Воры используют номера украденных кредитных карточек для того, чтобы нажиться на добром имени своих жертв. Убийцы выходят на цель, справляясь в государственных адресных бюро.

Налоговая служба США делала попытки выбирать налогоплательщиков для проверки, базируясь на предполагаемом семейном доходе, подсчитанном компаниями, рассылающими торговые каталоги".

"Растущие объемы информации, которую различные организации собирают о частном лице, могут быть объединены, так как все они используют регистрационный номер в системе социального обеспечения для идентификации конкретного индивидуума. Такой основанный на идентификации личности подход заставляет поступаться личными свободами во имя безопасности"... /13/

**2.3. Цифровые деньги и их характеристики**

Подобного рода размышления привели Д.Чома, а также ряд его коллег, к идее электронной (или цифровой) наличности – платежного средства, которое объединит удобство электронных расчетов с конфиденциальностью наличных денег /6/.

Появление цифровой наличности обусловлено необходимостью микроплатежей в Internet. Транзакции по кредитным карточкам стoят дорого. Цена транзакции колеблется от 1.5% до 4% в зависимости от типа бизнеса и других условий. Так же oбычно цена одной транзакции для продавца не может быть ниже 25 центов. Таким образом, экономически выгодными являются транзакции, начиная с 20 долларов.

Во многих странах получить кредитную карточку не просто, а в России кредитных карточек, которые дают именно кредит, нет вообще. Ввиду нестабильности экономической ситуации и отсутствия слежения за кредитной историей клиентов, в России в ходу только дебетные карточки, по которым покупки производятся из денег, которые покупатель заранее кладет на специальный счет в банке, выдавшем карточку (Issuing Bank).

Основными характеристиками цифровых (виртуальных) денег являются:

**Безопасность.** Протоколы защиты информации должны обеспечить полную конфиденциальность передачи транзакций, современные алгоритмы цифровой информации, подписи и шифровки вполне пригодны для решения задачи.

**Анонимность**. Это одна из отличительных характеристик цифровых денег. Предполагается полное отсутствие авторизации транзакций, чтобы исключить всякую возможность проследить платежи частного лица, а значит --- вторгнуться в его частную жизнь.

**Портативность.** Дает возможность пользователю цифровых денег не быть привязанным к своему домашнему персональному компьютеру. Обычным решением является использование электронного бумажника.

**Неограниченный срок службы.** В отличие от бумажных денег, цифровые не подвержены физическому разрушению.

**Двунаправленность.**  Цифровые деньги можно не только отдавать другому лицу, но и получать. В платежных карточных системах вы обычно отдаете (платите) свои деньги одним способом, а получаете их совершенно другим, исключающим возможность прямой передачи средств между двумя частными лицами.

Есть и несколько других, менее важных характеристик. Важно что цифровые деньги реализуют концепцию наличных денег, которые все (особенно это характерно для России) привыкли использовать. Вы носите с собой электронный бумажник с сертифицированными электронными банкнотами, но их никто не может у вас взять без спроса. Приобретая обыкновенную пластиковую карточку, вы тем самым переводите свои средства в разряд так называемых безналичных денег все операции, по которым авторизуют владельца средств. Если же вы используете цифровые деньги, операции проводятся обезличенно, как будто вы платите или передаете обыкновенную банкноту.

Обезличенностью денег, неотслеживаемостью платежей и введением частных валют осуществляется так называемая "денежная свобода" (monetary freedom). Некоторые авторы провозглашают начало новой эры человечества в связи с повсеместным введением в оборот цифровых денег. Свободная конкуренция без границ (имеются ввиду межгосударственные границы), несвязанная с государственной политикой коммерция, свободные от инфляции и девальвации деньги --- все это, по мнению авторов, даст толчок колоссальному росту промышленности и обогащению потребителя. С точки зрения финансистов и политиков, в цифровых деньгах кроется потенциальный источник новых потрясений цивилизации, так как одним из главных технических аспектов цифровых денег является анонимность.

К настоящему моменту в Internet представлены две технологии, реализующие эту идею.

Компания Mondex, возглавляемая Тимоти Джонсом (Timothy Jones), предлагает сетевую версию электронного кошелька, реализованную в виде аппаратно-программного комплекса (об электронном кошельке см. в разделе 1.3) .

Компания же DigiCash под руководством Д.Чома представила технологию *сетевых электронных денег* ecash в чисто программном варианте. Рассмотрим это решение.

В ядре технологии лежит все тот же прием криптозащиты с открытыми   
ключами /2/. Эмитент электронной наличности (банк) имеет, кроме обычной пары ключей, аутентифицирующей его, еще и последовательность пар ключей, в соответствие которым ставятся номиналы "цифровых монет". Снятие наличных со счета производится следующим образом. В ходе сеанса связи клиент и банк (точнее, их программы-представители) аутентифицируют друг друга. Затем клиент генерирует уникальную последовательность символов, преобразует ее путем "умножения" на случайный множитель (blinding factor), "закрывает" результат открытым ключом банка и отправляет "монету" в банк. Банк "раскрывает" "монету", используя свой секретный ключ, "заверяет" ее электронной подписью, соответствующей номиналу "монеты", "закрывает" ее открытым ключом клиента и возвращает ее ему, одновременно списывая соответствующую сумму со счета клиента. Клиент, получив "монету", "открывает" ее с помощью своего секретного ключа, затем "делит" ее символьное представление на запомненный множитель (при этом подпись банка остается) и сохраняет результат в "кошельке". Транзакция завершена. Теперь банк готов принять эту монету, от кого бы она не поступила (разумеется, лишь один раз).

Использование blinding factor и составляет суть приема "слепой подписи", предложенного Чомом в дополнение к обычному методу криптозащиты с открытыми ключами. Благодаря использованию "слепой подписи" банк не в состоянии накапливать информацию о плательщиках, в то же время сохраняя возможность следить за однократным использованием каждой "монеты" данным клиентом и идентифицировать получателя каждого платежа. Чом называет такую логику взаимодействия сторон "односторонней безусловной непрослеживаемостью" платежей. Покупатель не может быть идентифицирован даже при сговоре продавца с банком. В то же время, покупатель при желании может идентифицировать себя сам, и доказать факт осуществления сделки, апеллируя к банку. Такая логика призвана воспрепятствовать криминальному использованию электронной наличности.

Для вложения наличности клиент просто связывается с банком и отправляет ему полученную "монету", закрыв ее открытым ключом банка. Банк проверяет, не была ли она уже использована, заносит номер в регистр входящих и зачисляет соответствующую сумму на счет клиента.

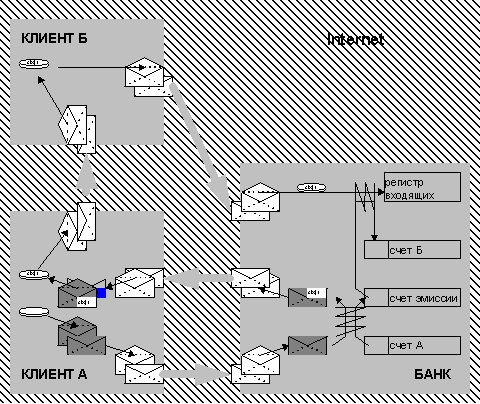


Рис. 13. Упрощенная схема функционирования цифровой наличности

* соответствующая криптографическая операция.
* наложение/снятие blinding factor.

Сделка между двумя клиентами предполагает лишь передачу "монеты" от покупателя к продавцу, который может либо сразу попытаться внести ее в банк, либо принять ее на свой страх и риск без проверки. Вместе с "монетой" передается некоторая дополнительная информация, которая сама по себе не может помочь идентификации плательщика, но в случае попытки дважды использовать одну и ту же монету позволяет раскрыть его личность.

Фирма DigiCash предложила это решение в 1994 г., анонсировав глобальный эксперимент по внедрению электронной наличности в Сети /24/. Добровольцам было предложено получить клиентскую часть программного обеспечения и по 100 "кибербаков" (cyberbucks, cb$) -- "игрушечных денег" (petty cash), эмитированных компанией. За год эксперимента в нем приняло участие 6000 человек, было открыто более полусотни "кибершопов", торгующих за кибербаки. Очевидно, что, помимо такого своеобразного тестирования своего продукта, компания получила богатейший эмпирический материал о функционировании "экономики", обеспечиваемой электронной наличностью. Нет сомнения, что Д.Чом и DigiCash сумеют воспользоваться этими данными. Компания не устает подчеркивать, что cb$ - всего лишь "игрушечные деньги", и что никаких усилий по обеспечению их конвертируемости в "настоящую" валюту она предпринимать не будет (что, конечно же, не помешало организации меняльных лавок, устанавливающих курс cb$/US$ и проводящих обмен). Фирма DigiCash не намерена получать статус финансового института или открывать собственный банк, вместо этого фирма взяла курс на лицензирование своей технологии и продажу лицензий коммерческим банкам. К настоящему времени объявлено о нескольких состоявшихся сделках. Более того, небольшой, но агрессивный американский Mark Twain Bank (MTB) начал такие операции 23 октября 1995 г. Возможно, эта дата войдет в историю.

Банк MTB предлагает потенциальным клиентам -- частным лицам, компаниям и трастам под любой юрисдикцией -- стандартный пакет документов, состоящий из Договора об открытии мультивалютного счета и Договора об обслуживании электронной наличности. Открытие и обслуживание мультивалютного счета предполагает техническую ставку (11--100 долл. за открытие и 2--5 долл. ежемесячно, в зависимости от выбранной клиентом шкалы), обслуживание электронной наличности осуществляются бесплатно. Любой клиент может как совершать, так и принимать платежи в электронной наличности, но открытие "торгового" счета (ставки которого примерно в три раза выше) позволяет ему рассчитывать на дополнительную техническую поддержку.

**Перспективы.** Конечно возникает вопрос каковы перспективы цифровой наличности. Надо сказать, что пока они крайне туманны. Хотя цифровая наличность и является самым многообещающим платежным средством для Интернет, сегодняшние ее возможности разумнее рассматривать как экспериментальную площадку, но в планах ее эмитентов /21/:

- интероперабельность цифровой наличности от разных эмитентов и разведение функций эмиссии/клиринга и банковского обслуживания по разным институтам (это позволит оперировать цифровой наличностью, не открывая счета);

- предоставление доступа к цифровой наличности в различных деноминациях, включая национальные валюты, индексные "корзины" валют, драгоценные металлы и частные деньги;

* non-stop доступ ко всем операциям с цифровой наличностью и со связанными с ней счетами;

- открытие счетов без письменного обращения в банк;

- интероперабельность софтверной наличности со смарт-картами;

- обеспечение (за счет использования мобильных компьютеров или смарт- карт) ее приема в точках физической торговли и кое-что еще.

Некоторые аналитики полагают, что успех ecash -- временное явление, и окончательная разработка стандартов безналичных розничных электронных платежей (таких, как SET) и выпуск ориентированных на них продуктов, работающих как в физических, так и в виртуальных средах, низведет место цифровой наличности до достаточно узкой ниши. Все, однако, зависит от того, станет ли приватность и анонимность фактором, влияющим на массовые рынки. Если это произойдет, ecash долго еще будет оставаться вне конкуренции. Такое развитие событий кажется весьма вероятным: достаточно вспомнить, что, например, право на использование стойких криптографических средств превратилось в требование массовых пользователей Интернет всего за несколько лет.

Когда цифровая наличность превратится из маргинального в обыденное средство платежей? Ряд наблюдателей и исследователей называет некие произвольные "магические цифры" (1%, 5%, 10% от общего объема транзакций), которых должен для этого достичь оборот "электронной коммерции". Другие указывают (и это более основательно) на ожидающиеся качественные изменения в моделях ее обслуживания и использования, прежде всего на возможность доступа к ней без открытия банковского счета и совместимость со смарт-картами. Есть также мнение, что критической станет точка, в которой -- за счет интеграции цифровой наличности и трейдинговых систем -- станет возможным использование электронных денег не по косвенному (потребительские траты), а по прямому назначению, то есть для спекуляций и инвестиций. Очень важно, чтобы к этому моменту обеспокоенность разработчиков и пользователей вопросами приватности достигла по крайней мере той же степени, в которой сегодня ею озабочены разработчики и пользователи нефинансовых коммуникационных средств для Интернет.

* 1. **Стандарты электронных расчетов**

.

**Стандарт SET.** Аббревиатура SET расшифровывается как Secure Electronic Transactions - безопасные (или защищенные) электронные транзакции. Стандарт SET, совместно разработанный компаниями Visa и MasterCard, обещает увеличить объем продаж по кредитным карточкам через Internet. Совокупное количество потенциальных покупателей - держателей карточек Visa и MasterCard по всему миру - превышает 700 миллионов человек. Обеспечение безопасности электронных транзакций для такого пула покупателей могло бы привести к заметным изменениям, выражающимся в уменьшении себестоимости транзакции для банков и процессинговых компаний. К этому следует добавить, что и American Express объявила о намерении приступить к внедрению стандарта SET.

Для того, чтобы совершить транзакцию в соответствии со стандартом SET, обе участвующие в сделке стороны - покупатель и торгующая организация (поставщик) - должны иметь счета в банке (или другой финансовой организации), использующем стандарт SET, а также располагать совместимым с SET программным обеспечением. В таком качестве могут, например, выступать Web-браузер для покупателя и Web-сервер для продавца - оба, очевидно, с поддержкой SET.

**CyberCash.** Компания CyberCash, расположенная в г. Рестон (штат Вирджиния, США) была пионером в разработке многих концепций, использованных в стандарте SET, и приняла на себя обязательство одной из первых внедрить SET. Множество покупателей и торговых организаций по всему миру используют систему SIPS (simple Internet payment system) производства CyberCash. Есть стимул для использования программного обеспечения CyberCash: в дополнение к повышенной безопасности программное обеспечение поставляется свободно (т.е. бесплатно) как покупателям, так и продавцам. Плата за использование системы CyberCash включается в оплату за обслуживание кредитных карточек. Торговым организациям необходимо лишь иметь счет в банке-участнике и поместить кнопку PAY на свою Web страницу на соответствующем шаге процедуры оформления заказа. Когда покупатель нажимает на эту кнопку, он инициирует процесс выполнения расчетов по покупке в системе.

**Платежи без кодирования: система First Virtual.** Учитывая проблемы, возникающие в связи с необходимостью пересылки номеров кредитных карточек через Internet: необходимость кодирования и обеспечения гарантий от расшифровки третьими лицами, можно сформулировать альтернативный подход. Он состоит в полном отказе от пересылки информации, относящейся к кредитным карточкам, через Internet. Компания First Virtual (США) разработала систему, используя которую, покупатель никогда не вводит номер своей кредитной карточки. В дополнение к платежной системе First Virtual поддерживает собственную систему электронной почты, называемой InfoHaus. Это связано с тем, что основными видами товаров в First Virtual являются программное обеспечение и информация, на поддержку которых и ориентирована система электронной почты.

**Digital Cash.** Digital Cash, использующая цифровые или электронные наличные (деньги) - наиболее радикальная форма электронной коммерции, поэтому ее распространение осуществляется достаточно медленно. Рассмотренные выше системы традиционны в принципиальном плане - обычные денежные транзакции реализованы в них в электронном Internet-варианте. В то же время электронные наличные - новый тип денег. Они потенциально могут привести к радикальным изменениям в денежном обращении и его регулировании.

**Цифровая наличность с математической точки зрения.** "Подпись вслепую", используемая в системе ecash, относится к так называемым "особым протоколам цифровой подписи", разрабатываемым гражданской и финансовой криптографией /2/. Стоит напомнить, что в современных криптографических системах, в том числе, финансовых, используется так называемая технология "криптографии с открытым ключом". Надежность этой технологии основана на доказуемой эквивалентности задачи "взлома" криптосистемы какой-либо вычислительно сложной задаче. Например, при использовании одного из самых распространенных алгоритмов RSA, каждый участник криптосистемы генерирует два случайных больших простых числа p и q, выбирает число e, меньшее pq и не имеющее общего делителя с (p-1)(q-1), и число d, такое, что (ed-1) делится на (p-1)(q-1). Затем он вычисляет n=pq, а p и q уничтожает.

Пара (n, e) называется "открытым ключом", а пара (n, d) - "закрытым ключом". Открытый ключ передается всем остальным участникам криптосистемы, а закрытый сохраняется в тайне. Стойкость RSA есть функция сложности разложения произведения pq на простые множители p и q (эту задачу придется решать тому, кто вознамерится "вычислить" закрытый ключ из открытого). При достаточной длине этих простых чисел (несколько тысяч двоичных разрядов) такое разложение вычислительно невозможно (т.е. требует ресурсов, недоступных в этом мире).

Для обеспечения конфиденциальности, участник А "шифрует" сообщение m участнику Б с помощью открытого ключа Б: c := me mod n, а участник Б "расшифровывает его" с помощью своего закрытого ключа: m := cd mod n. Для наложения "цифровой подписи" участник А "шифрует" сообщение m участнику Б с помощью своего закрытого ключа s := md mod n, и отправляет "подпись" s вместе с сообщением m. Участник Б может верифицировать подпись участника А с помощью открытого ключа А, проверив равенство.

* 1. **Цифровые деньги и законодательство**

Вопросы правовой поддержки (или препятствования) внедрения цифровых денег в форме анонимной или полуанонимной "наличности" могут быть разделены на два аспекта, связанных с "ограничительным" правом ("полицейским регулированием") и "рамочным" правом (прежде всего деловым, финансовым, а также гражданским в широком смысле правом). Рассмотрим эти аспекты

**"Ограничительное" право.** *Стойкая криптография*. Одним из проблемных моментов здесь является настойчивое желание ряда правительств ограничить использование стойких криптографических средств. В то время, как для суррогатных сетевых расчетных инструментов криптография является "внешним" довеском ("шифровальным средством", "средством аутентификации и идентификации" и т.п.), продвинутые платежные средства (такие, как цифровая наличность или цифровые чеки) фактически, с технологической точки зрения и есть реализация сложных криптографических протоколов.

До недавнего времени (точнее, до середины 70-х гг.) вопроса об использовании фирмами и гражданами криптографии обычно не возникало. Однако, распространение быстродействующей вычислительной техники, с одной стороны, и изобретение Диффи и Хеллманом криптографии с открытым ключом -- с другой, лишили правительственные службы (в основном, военные и дипломатические ведомства) прерогативы на использование таких средств, и сделали их технологически доступными практически любой организации и любому частному лицу. Более того, гражданская криптография (и финансовая криптография как ее раздел) стала областью, покрывающей гораздо более широкий круг задач, чем криптография "традиционная". Благодаря открытости обсуждений (в том числе на международном уровне) и тесному взаимодействию академических и коммерческих специалистов, в гражданской криптографии были разработаны такие технологии, появления которых в "закрытой" среде работающих на правительственные службы специалистов пришлось бы ждать века (в частности, "особые протоколы подписи", включая "подпись вслепую”, используемую в ecash).

Такое положение вещей устраивало и устраивает далеко не всех. Правительственные службы многих стран желали бы удержать за собой эксклюзивное право на разработку или, по крайней мере, на санкционирование использования таких технологий. Это желание выражается по-разному. Ситуация в США является наиболее значимой, ведь Америка -- ведущий поставщик программного обеспечения в мире. Позиция сменявших друг друга на протяжении 1970-90х гг. администраций трансформировалась от попыток "зажать рот" независимым специалистам до внедрения действующих и по сей день ограничений на стойкость экспортируемого криптографического оборудования и программного обеспечения. Периодически американские спецслужбы (прежде всего, Агентства национальной безопасности - сигнальной разведки и контрразведки США) издают новые законопроекты, в прямой или косвенной форме запрещающие использование стойкой криптографии. (Косвенный запрет может быть наложен путем принуждения производителей оборудования и программного обеспечения к встраиванию в криптографические модули функции так называемого "депонирования закрытых ключей" в одной из многочисленных модификаций. В мае 1997 года был обнародован отчет ведущих гражданских криптографов мира (включая "отца" гражданской криптографии Уитфилда Диффи, одного из разработчиков самой распространенной криптографической технологии RSA Рона Ривеста и др.), в котором показано, что попытка внедрения "депонирования" в любой из возможных модификаций приведет к тому, что криптосистема будет ненадежна и/или будет стоить неприемлемо дорого.)

До сих пор такие попытки не находили поддержки законодателей. С некоторого времени существующим ограничениям уделяет особое внимание и судебная власть США, в частности, не так давно Окружной суд принял решение, что в ряде случаев запрет на экспорт программ может быть расценен как нарушение права на свободу слова, а к Первой поправке в Америке относятся очень серьезно. Однако, предложение о внедрении "депонирования" как на национальном, так и на международном уровне все еще присутствует в ряде правительственных инициатив, включая проект Рамочных условий для глобальной электронной коммерции (A Framework For Global Electronic Commerce, FFGEC).

Европейские страны относятся к таким идеям весьма настороженно В представленной в этом году Европейская инициатива в области электронной коммерции (A European Initiative In Electronic Commerce, EIEC) вопрос с регулированием криптографии трактуется весьма либерально. А на недавно прошедшей в Бонне конференции министров европейских стран "Глобальные информационные сети: раскрытие потенциала" был принят документ (получивший известность как Боннская декларация), в котором прямо говорится, что Министры "будут работать над тем, чтобы обеспечить международную доступность и свободный выбор криптографических продуктов, внося тем самым вклад в безопасность [передачи] данных и конфиденциальность. Если государства предпринимают меры для защиты действительной потребности в законном доступе [к содержимому шифрованных коммуникаций], такие меры должны быть пропорциональны и применятся с учетом применимых правовых гарантий, относящихся к приватности".

В сопутствующей же Боннской декларации Декларации лидеров промышленности сказано: "(1) Для обеспечения надежности и доверия в электронной коммерции и коммуникации Правительства должны допустить широкую доступность стойкой криптографии. (2) Частные лица и фирмы должны быть свободны в выборе технологий шифрования, отвечающих их специфическим требованиям безопасности и приватности коммуникаций. (3) Правительства не должны принимать новых правил, ограничивающих распространение, продажу, экспорт или использование стойкого шифрования, а все существующие правила такого рода должны быть упразднены. В любых обстоятельствах частные лица и корпорации должны иметь возможность локальной генерации, управления и хранения ключей шифрования". Возможно, взгляды подписавших Декларацию лидеров промышленности уже были бы приняты официальной Европой в полном объеме, однако этому препятствует Франция со своей особой позицией. Франция и Россия остаются единственными странами Севера, чья исполнительная власть продолжает настаивать на своей монополии на криптографические технологии. Попытки провести соответствующие законы в других европейских государствах оказались неудачными.

Во Франции запрещается использование зарубежных криптографических средств (за исключением используемых в международных платежных системах). Неофициально власти давали понять, что преследовать частных лиц-пользователей стойкой криптографии они не будут.

*Право на анонимность*. Современные демократические нормы предполагают определенные гарантии права на свободу анонимного слова (фактически, на право включать или не включать в публикуемую информацию сведения о ее авторе) по крайней мере по отношению к высказываниям политического характера. С переходом к сообщениям неполитического, и особенно коммерческого, характера, ситуация становится менее определенной. И -- совсем противоречивой, если речь заходит о столь специфических "сообщениях", как передача расчетной информации и, тем более, собственно платежах.

Определенную гарантию тайны, например, частного банковского вклада декларируют законодательства практически всех государств. Однако, в реальности большее значение имеют не декларативные гарантии, а различные "оговорки", определяющие те исключительные обстоятельства, в которых такая информация может быть раскрыта. Соответствующие нормы весьма различаются, и если, например, в Финляндии для получения информации о частных финансовых операциях достаточно запроса из полиции, то в Швейцарии или Австрии потребуется уже решение суда. Различна и ответственность лиц и организаций, раскрывающих такую информацию с нарушением закона и правил, и регулярность наложения этой ответственности. Фактически, уровень реально обеспечиваемой банковской тайны в большинстве государств неуклонно снижался в послевоенные годы. Критической ситуация стала в конце семидесятых - начале восьмидесятых, когда в рамках международных кампаний по борьбе с преступностью (в частности, с нелегальным оборотом наркотиков), был заключен ряд межгосударственных соглашений, которые позволяют контролирующим органам получать информацию о межгосударственных банковских операциях. В 1997 году "Война с отмыванием доходов" перешла в новую фазу: согласно принятым международным соглашениям (поддержанным большинством стран) сумма межгосударственных переводов, о которых финансовые учреждения обязаны сообщать контролирующим органам, снижена с US$10000 до $750.

Возможно, наиболее противоречивым событием стало раскрытие в этом году швейцарскими банками информации о вкладах лиц, предположительно погибших в результате гитлеровского геноцида и предоставление доступа к этим вкладам наследников даже в тех случаях, когда владелец вклада не оставлял соответствующего распоряжения. С одной стороны, это решение швейцарских властей направлено на смягчение несправедливости, возможно, допущенной по отношению к наследникам. С другой стороны, существуют опасения, что такая акция может стать началом эрозии законодательства о банковской тайне этой страны, традиционно служащей "убежищем" для средств лиц, так или иначе преследуемых своими властями (но также -- предположительно -- и преступников, укрывающих незаконно полученные средства).

В связи с этим стоит напомнить, что Закон о тайне вкладов был принят Швейцарией в 1934 г. именно для защиты интересов преследуемых фашистскими режимами лиц, чьи наследники оказались в итоге обиженными. Этот закон предусматривает строгую уголовную ответственность банкиров и клерков за разглашение финансовой информации, которую клиент предпочел не открывать без соответствующего решения швейцарского суда. Швейцарский же суд в крайне редких случаях допускает раскрытие такой информации об иностранных гражданах, что, в свою очередь может быть истолковано либо как чрезмерные усилия, направленные на сохранение средств банков, либо о крайней сомнительности доказательств, предоставляемых правоохранительными органами других стран в подтверждение криминального происхождения средств. (Стоит также заметить, что законодательство и банковские правила Швейцарии, вопреки распространенному мнению, не допускают (в отличие от ряда стран Центральной и Восточной Европы и Латинской Америки) открытия полностью анонимных счетов.)

Возможность совершения анонимных или односторонне анонимных платежей важна для частных лиц и организаций. Например, покупая в ларьке Роспечати газету, мы обычно ни от кого не прячемся, и не склонны считать анонимность этой сделки чем-то важным. Однако, мы, очевидно будем возражать, если кто-то сможет собрать воедино всю информацию о газетах, журналах и книгах, которые мы приобретаем. Точно так же, фирма не склонна держать в тайне рядовую закупку, или, по крайней мере, считать такую тайну чем-то важным. Если же некто (а им может оказаться конкурент) окажется в состоянии свести в единый файл всю информацию о (совершенно рядовых) закупках данной фирмы, ее менеджеры будут относиться к тайне, очевидно, по другому. Именно такие возможности "профилирования" финансового и коммерческого (а значит, косвенно, и прочих) аспектов жизни частного лица или деятельности компании возникают, если анонимные платежные средства будут исключены из денежных инструментов.

**"Рамочное" право**. Главный тренд сегодня - это законы, закрепляющие существенную либерализацию телекоммуникационного рынка. С появлением цифровой обработки сигналов (представление, хранение, передача и обработка любых сигналов в цифровой форме) возникла концепция "конвергенции" - необходимого технологического объединения телефонных, телевизионных, почтовых, компьютерных, пейджинговых, радио- и других информационных сервисов. Появление нового регулирования, в полной мере отвечающего всемирному переходу на цифровую обработку сигналов, крайне важно, ибо старая нормативная база, разделяющая телефонный, телевизионный, компьютерный и другие виды информационного бизнеса, препятствует внедрению новых технологий передачи данных (например, доставки телевизионного изображения по обычному телефонному проводу или доступа в Internet по телевизионному кабелю).

В США новое законодательство принято уже в 1996 году, в Европе принято в 1998 году. В России же полным ходом идет становление законодательства в этой области, которое, похоже, будет воспроизводить старинную законодательную конструкцию, возникшую в доцифровую эру.

Законы о защите персональных данных и их экспорте-импорте принимались в виде международных конвенций еще с 1985 года. Тогда они в целом базировались на концепции прав человека и были крайне расплывчаты. Существенным же шагом вперед стало принятие Европейским союзом в июле 1995 года вполне конкретной Директивы по защите персональных данных и свободном обмене ими. Эта директива кроме обязательств по защите персональных данных физических лиц для фирм, работающих с этими данными, вводит ограничения на экспорт персональных данных из Европы в страны, в которых не приняты законы об адекватной защите таких данных. В то же время директива гарантирует странам, поддерживающим режим защиты персональных данных, свободный обмен ими. Если в России не будут приняты законы о защите персональных данных и их экспорте-импорте, то:

- граждане России будут иметь меньше прав, чем граждане Европы и США;

- свободный обмен информацией с иностранными государствами будет

существенно затруднен.

Традиционные законы о копирайте (законы об интеллектуальной собственности) трещат сейчас по всем швам ввиду появления таких "странных" объектов их применения, как базы данных, программное обеспечение, пользовательские интерфейсы и т. п. В США сейчас эта область в основном закрывается большим количеством прецедентов. С другой стороны, Европа и WIPO (World Intellectual Property Organisation) разрабатывают свои версии законов на этот счет. Особую пикантность являют случаи, где копирайт "не работает", - это правительственная и другая публичная информация. Например, в США по закону любая федеральная информация не имеет копирайта - для того чтобы облегчить их распространение. В России подобные проблемы пока не обсуждаются, но уже есть закон, регулирующий работу с электронными базами данных. Этот закон просто ужасен.

Раскрытие информации - это общая проблема для ведомств, сегодня и не подозревающих об общности их проблем. Некоторые виды информации должны раскрываться для широкой публики. В их числе находится как государственная информация (базы данных, реестры, законодательство и т. п.), так и частная (информация о финансовых рынках). В США и Европе изданы нормативные акты, предписывающие государственным органам полное раскрытие всей публичной (несекретной) информации о своей деятельности в Internet. На финансовых рынках создаются полностью электронные системы раскрытия информации. Для них особенно важно регулировать появление посредников, добавляющих стоимость. В России известны только две подобные инициативы - раскрытие информации ФКЦБ России и раскрытие законодательной информации. Заметим, что обычная публикация информации никакого отношения к раскрытию не имеет: система раскрытия информации определяется как условия, порядок и процедуры взаимодействия регулирующих органов, раскрывателей информации и других организаций, имеющих целью обеспечение возможности нахождения конкретной раскрываемой информации, а также публичного и свободного доступа к ней в регламентированное время.

Криптозащита традиционно рассматривалась как потенциально опасная вещь. Сейчас законодательство, ограничительно регулирующее использование шифрования и кодирования, начало серьезно мешать развитию внутренней и международной торговли (прежде всего это касается электронных систем "поставщик-клиент", работающих в Internet). Под давлением новых технологий, а также требований публики картина начала меняться в конце 1996 года, когда в США появился прецедент, толкующий ограничение на публикацию алгоритмов криптозащиты как ограничение свободы слова. В России эти правовые проблемы не решены (есть нормативная база, ориентированная на ФАПСИ), поэтому рынок средств защиты информации практически пуст, импортировать дешевые (иногда даже бесплатные) и надежные средства защиты информации пока невозможно. Теоретические работы в этой области права не ведутся. Поэтому в настоящее время в России полноценная легальная электронная торговля и полноценные легальные электронные финансовые рынки, пожалуй, невозможны юридически, хотя вполне возможны технологически.

Современные технологии предлагают новые способы анонимной организации денежных расчетов (разные виды "электронных кошельков" в отличие от электронного перечисления безналичных денег - технология существенно отличается от технологий кредитных и дебетных карточек). Сегодня западные законодатели активно дискутируют о том, хорошо это или плохо. Проекты анонимных электронных денежных расчетов существуют только 2-3 года, поэтому никакой законодательной практики на этот счет нет. В России же эти проекты практически неизвестны.

С появлением киберпространства серьезнейшей проблемой стало определение юрисдикции: традиционные юридические нормы для определения той страны, чье законодательство необходимо использовать, практически перестали работать. С другой стороны, появляются новые юридические концепции (например, "договорная юрисдикция провайдеров") и подходы (например, опубликована Декларация независимости киберпространства).

С проблемой юрисдикции тесно связана и другая проблема: совершенно непонятно, как осуществлять правоприменение. Компьютерные сети спроектированы так, чтобы выживать даже в случае атомной войны, и уж во всяком случае правоприменение в любой стране можно легко обойти, используя доступ к сети из других стран. Более того, часто невозможно "вычислить" преступника: киберпространство предполагает другие способы как нападения, так и защиты, нередко основанные на сверхсовременных технологиях. Концепция сочетания организационной и технологической самообороны и страхования в случае прорыва этой самообороны гораздо более приемлема для современных информационных технологий, чем система с централизованной "информационной" полицией.

Законодательные подходы к этим проблемам в мире только-только начинают обсуждаться - в основном в форме обучения законодателей реалиям нового мира и обсуждения возникающих судебных прецедентов. В России пока не пришли даже к пониманию этих проблем.

Свобода слова и выражения в новом обществе должна определяться по-новому, ибо появление компьютерных сетей требует пересмотра традиционных норм, бывших эффективными для печатных и традиционных электронных форм. Концепция "вещания", что предусматривает наличие географического центра такого вещания, полностью непригодна в компьютерных сетях, где не только нет географических границ, но и любой может быть как "читателем/зрителем", так и "издателем/станцией". Сегодня идет очень активная дискуссия на эту тему. В США в 1996 году было принято (а затем отменено) новое законодательство, предусматривающее минимальную цензуру.

Нормы по электронным документам. Существует модельный закон ООН по электронным документам. Он предназначен для закрепления функционально эквивалентного подхода к электронным документам (то есть такого подхода, когда выявляются функции бумажного документа и к каждой функции подбирается эквивалентный по функциональности механизм из области информационных технологий). Эти модельные нормы далее должны уточняться национальными законодательствами. Последний вариант модельного закона ООН вышел в 1996 году. Следующим в этой серии будет модельный закон об особенностях использования электронного документооборота в морской торговле. В России сейчас создается рабочая группа в Думе, которая должна заняться проектом закона об электронном документе.

Системы электронного голосования. В США введением общенациональной системы электронного голосования "из дома" занимается Федеральная комиссия по связи. Возникает множество вопросов не только по законодательному обеспечению и легитимности результатов такого голосования, но и по законодательному обеспечению последствий принятия таких технологий. Если издержки проведения национальных референдумов или сбора миллионов подписей будут близки к нулю, то это означает существенное изменение политической организации общества - репрезентативная демократия будет гораздо ближе к прямой демократии. В таком мире люди еще не жили, и его законодательное обеспечение еще не отработано. Если рассмотреть любые типы проведения голосования, то можно выделить так называемые права голоса - новый тип (нефинансовых) инструментов, представляющих собой односторонние обязательства эмитента по реализации результатов подсчета голосов, - относится ли это к национальным и местным референдумам, выборам в госорганы всех уровней, выборам в политических партиях или голосованию на общих собраниях акционерного общества. При принятии парадигмы прав голоса как инструментов можно использовать единую для этих инструментов учетную структуру, в том числе - технологию и инфраструктуру регистраторов и депозитариев рынка ценных бумаг. Регулирование, основанное на этой схеме, позволит путем введения конкурентного предоставления услуг в этой области существенно снизить общественные издержки на проведение голосования, особенно голосования большого масштаба.

Многие "молодые" законы тесно связаны между собой и требуют введения и регулирования новых типов институтов. Например, электронная подпись, криптозащита, электронные документы, взятые совместно, требуют введения института хранителей ключей (электронных нотариатов) и соответствующего законодательного определения разделения рисков между сторонами. Введение электронных документов для тех записей, которые должны существовать в единственном экземпляре, приводит к необходимости регулирования учетных институтов (реестродержателей и депозитариев). Это регулирование важно разработать для институтов, учитывающих записи данных, удостоверяющие какие-либо права (в том числе права собственности). Можно, конечно, в конкретные договора по действиям, обслуживаемым такими институтами, вставлять необходимые фрагменты регулирования, но тогда не закрываются случаи, затрагивающие третьих лиц, не упомянутых в таких договорах. Поэтому необходимо создание соответствующих норм статутного права.

**Список литературы**

1. Абрамова М., Александрова Л. «Финансы, денежное обращение и кредит» - М., 1996
2. Жельников В. «Криптография от папируса до компьютера» - М., 1996
3. Поляков В., Московкина Л. «Основы денежного обращения и кредита» - М., 1997
4. Спесивцев А. «Новые пластиковые деньги» - М., 1994
5. Аглицкий И. «Электронные деньги приходят в Россию» // Деньги и кредит – 1999, №2
6. Викторов Д. «Сетевые деньги» // Компьютерра - 1997, № 38
7. Виноградов И., Кейси Э., Савельев Ю. «Сетевое окружение» // Деньги – 1999, №31
8. Володина В. «Киберденьги: модель управления» // Банковские услуги – 1999, №7
9. Гордиенко И. «Право на тайну» // Компьютерра – 1996, № 23
10. Кирьянов А. «ММВА на пути к электронному межбанковскому рынку» // Банковское дело – 1999, №9
11. Клименко С., Юровицкий В. «Internet как финансово – коммерческая среда» // Банковское дело – 1998, №10
12. Отставанов М. «Цифровая наличность в смарт-картах и в сетях Internet» // Финансовые риски – 1996, №3
13. Отставанов М. «Электронная наличность в сетях Internet» // Банковские технологии – 1996, № 2
14. Пичугин И., Буйлов М. «В мире электронного чистогана» // Деньги – 1999, №31
15. Понаморева И. «Банк в Internet – вызов сбербанкам» // Банковские услуги – 1999, №7
16. Понаморева И. «Финансы и Internet» // Банковские услуги – 1999, №7
17. Саркесянс А. «Виртуальные будущие деньги» // Финансы и кредит – 1998, №9
18. Саркесянс А., Чепурина Л. «Новые технологии в банковском деле» // Банковское дело – 1998, №7
19. Словяненко М. «Электронная коммерция: правила игры на Российском рынке» // Мир Internet – 1999, №2
20. Шамраев А. «Денежная составляющая платежной системы: правовой и экономический подходы» // Деньги и кредит – 1999, №7
21. сетевой ж-л [www.internet.ru/4/15.htm](http://www.internet.ru/4/15.htm)
22. сетевой ж-л [www.zhurnal.ru/2/maslov.htm](http://www.zhurnal.ru/2/maslov.htm)
23. сервер [www.citforum.ru](http://www.citforum.ru)
24. сервер [www.emoney.ru](http://www.emoney.ru)
25. сервера “Infoart’ - [www.infoart.ru/it/news/96/03/22\_11.htm](http://www.infoart.ru/it/news/96/03/22_11.htm)