ЛАБОРАТОРНАЯ РАБОТА № 7

ЦИФРОВЫЕ ДЕНЬГИ

Цель работы: практическое изучение протокола электронных платежей с помощью цифровых денег.

1. Теоретические сведения

Центральным понятием протоколов электронных платежей с помощью цифровых денег протоколов являются понятия “цифрового конверта” и подписи “вслепую”. Схемы подписи “вслепую” позволяют получать документы, подписанные претендентом, который не знает содержания самих этих документов. Если  претендентом на выставление подписи является банк, а подписываемые им документы – это чеки на предъявителя, то для нужд финансовой криптографии такие подписи обеспечивают два важных аспекта:

-      подпись банка на чеке является правильной и служит свидетельством того, что именно он заверил чек; такая подпись убедит банк в том, что именно он заверил этот чек, когда тот впоследствии будет ему предъявлен; разумеется, подпись “вслепую” обладает всеми остальными свойствами электронной цифровой подписи;

-      банк не сможет связать заверенный им чек с моментом его подписания; даже если предположить, что банк фиксирует все подписи “вслепую”, по предъявленному чеку он не сможет определить, кто и когда обратился к нему с просьбой подписать данный конкретный чек.

 Ниже приведен базовый вариант платежной системы с цифровыми деньгами (рис.1).

Покупатель подготавливает чек с указанной на нем суммой, которую он хочет снять со своего счета в банке. Обозначим в протоколе этот чек буквой *m*. Покупателю надо получить подпись на чеке, но так, чтобы банк не увидел самого чека и не смог пометить его.

Для этого покупатель подготавливает большое число чеков на нужную сумму и запечатывает их в конверты, а затем отправляет все их в банк. Банк вскрывает все конверты, кроме одного, и убеждается в корректности чеков. Тогда он подписывает последний конверт, не распечатывая его, и списывает со счета покупателя требуемую сумму. Если покупатель заранее положит во все конверты копировальную бумагу, то подпись банка автоматически окажется на чеке. Таким образом, банк подписал чек, не видя его и не имея возможности пометить. Криптографическое преобразование с использованием схемы RSA, обеспечивающее процедуру формирования конверта и подписи выглядит следующим образом. Пусть http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image002.gif – модуль шифрования, а http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image004.gif – открытый ключ банка. Покупатель генерирует столько случайных чисел http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image006.gif, сколько конвертов он будет отсылать в банк (чем больше конвертов, тем лучше). Далее каждое http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image006.gif шифруется с помощью открытого ключа банка и умножается на значение чека: http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image009.gif. Для того чтобы вскрыть каждый из конвертов, банк должен обратиться к покупателю с просьбой сообщить ему значение множителя http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image006.gif, так как вскрытие конверта означает получение значения http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image012.gif. Поэтому покупатель может быть уверен, что банк не сможет вскрыть ни одного конверта без его ведома. Один из конвертов банк не вскрывает, а подписывает http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image014.gif и отсылает назад покупателю.

Покупатель проверяет подпись банка на конверте равенством http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image016.gif, и если оно соблюдается, то вскрывает конверт и извлекает из него подписанный чек http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image018.gif.

Подписанный чек покупатель передает продавцу. Продавец проверяет подпись банка http://www.e-biblio.ru/book/bib/09_ekonomika/el_raschet_v_kom_deajt/posob/docs/piece025.files/image020.gif и затем пересылает чек в банк.

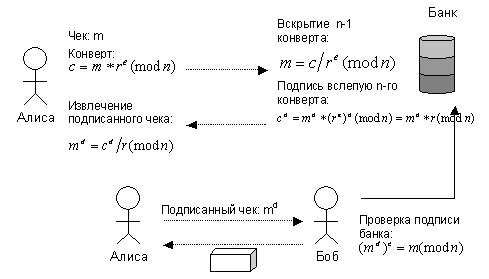


Рис 1.1

Банк проверяет точно таким же образом свою собственную подпись на полученном чеке, и если она правильная, то перечисляет сумму, указанную в чеке, на счет продавца.

Из приведенного выше протокола хорошо видно, на каких именно механизмах строятся действующие платежные системы. Однако данный протокол  практически  никак  не  решает  вопросов,  связанных  с  возможностью мошенничества со стороны покупателя или продавца, например путем повторного использования полученного подписанного чека и невозможности идентифицировать мошенника и т.д. Все эти проблемы решаются некоторыми модификациями базового варианта протокола

1. Задание на выполнение

Протокол электронных платежей с помощью цифровых денег (Участники информационного обмена - оператор банка, покупатель, продавец):

1. Оператор банка генерирует ключи (по методу RSA):

*p* и *q* - два различных простых числа, *n* = *p*⋅*q*

*e* некоторое целое, взаимно простое с (*p*-1)⋅(*q*-1).

*d*, такое что *e⋅d* = 1 mod *ф*(n), где *ф*(*n*) = (*p*-1)⋅ (*q*-1) – функция Эйлера. По теореме Эйлера *m*(ed) = *m* mod(*n*) для любого целого числа *m*

Открытый ключ числа *e* и *n*, а секретный ключ - числа *d*, *p* и *q.*

Например, пусть *p* = 19 и *q* = 23, тогда *n* = 437 и *ф*(*n*) = 396. Пусть также *e* = 13, и поэтому *d* = 61, так как 13⋅61 = 793 = 2*ф*(*n*)+1.

1. Покупатель подготавливает цифровые конверты

Покупатель желает получить от банка чек, например, на 120 у.е. Следовательно, *m* = 120. Покупатель случайным образом выбирает пять чисел из интервала 1 < *r* < *n*(=15) : *r1, r2, r3, r4, r5*.

Покупатель вычисляет цифровые конверты: *Ci* = (*m*⋅*ri* e) mod *n*

Покупатель отправляет все пять конвертов оператору банка.

3. Банк подписывает чек «вслепую» Оператор банка выбирает любые четыре цифровых конверта, например, *C1*, C*2*, C*4*, C*5* и запрашивает для них маскирующие числа *ri*.

Покупатель присылает маски *r1*, *r2*, *r4*, *r5*.

Оператор банка вскрывает конверты *mi* = *ci* /*ri* mod *n* = (*ci* ⋅(*ri*−1)e)

Т.е. вычисляет *m1*, *m2*, *m4*, *m5*

Предварительно необходимо вычислить мультипликативно обратные элементы для *ri* по модулю *n*: *ri*⋅(*ri*−1) mod *n* = 1

Оператор банка убеждается, что все – одинаковые (в данном случае 120), подписывает «вслепую» последний запечатанный конверт C3:

*F* = C3*d* mod *n* и отправляет подписанный конверт *F* покупателю.

4. Покупатель извлекает подписанный чек из конверта

Покупатель снимает маску с подписанного чека:

*md* = (*F*/*r*3) mod *n* =(F⋅( r3)−1) mod *n*,

Покупатель проверяет, что подпись – подлинная (*md*)e = *m*

5. Продавец принимает чек

Продавец, получив чек, проверяет, что чек – подлинный: (*md*)e = *m* (покупатель передает чек на сумму 120 у.е.). Так как подпись на чеке – верная, то продавец соглашается принять чек в качестве оплаты за товар.

6. Обналичивание чека

Оператор банка, получив чек от продавца, проверяет, что он – не фальшивый (*md*)e = *m*.

Продавец передает чек на сумму 120 у.е. Банк переводит эту сумму на счет продавца.