Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, с.29-33.

Поступила: 01.09.2017
Окончательный вариант: 05.10.2017

УДК 004.056:004.94

Компьютерная деловая игра «Цифровая наличность»

***Жаркова Г.А.*[1,*]*, Медведев И.И.*[1]**

[*]zharkovaga@inbox.ru
[1]УлГУ, Ульяновск, Россия

В статье описывается криптографический протокол, реализующий «электронные наличные», то есть платежную систему, в которой роль «наличных» играет пара чисел, подписанных анонимно на секретном ключе банка-эмитента. Протокол реализован в криптосистеме RSA с использованием относительно небольших чисел, которых, впрочем, достаточно для иллюстрации основных идей протокола. Для повышения интереса к данной теме протокол представлен в виде деловой игры «Цифровая наличность», которая представляет собой модель финансово-экономической электронной платежной системы (ЭПС). Деловая игра предназначена для использования в учебном процессе и представляет собой многоуровневое задание по генерации и проверке на подлинность «электронных наличных». От студента требуется свободное владение возможностями современного программирования и знания информационных потоков в ЭПС.

***Ключевые слова**: деловая игра, электронная наличность, криптосистема RSA, криптографические протоколы.*

В современном информационном мире появление электронных платежных систем (ЭПС) выглядит закономерно, подаётся как большое удобство и для потребителя, и для финансовых агентов, и для государства, как гаранта всей этой финансовой конструкции. Уже сейчас практически каждый взрослый гражданин имеет кредитную карточку, а то и не одну. В некоторых государствах ставится вопрос о полном отказе от наличных платежей. Однако у подобных систем есть принципиальный недостаток: к ним нельзя обратиться анонимно, то есть доказать свое право на владение некоторым денежным ресурсом, не раскрывая свою личность.

Кредитная карточка при каждом ее использовании полностью идентифицирует своего владельца, следовательно, всю историю прошлых покупок можно легко отследить и использовать при анализе предпочтений без санкции прокурора. Если владелец карточки использует её при покупке билетов на транспорте, то все его поездки можно отследить.

Отсюда один шаг для организации тотальной слежки за вполне законопослушными гражданами.

Если ставится задача предотвратить подобную угрозу, то необходима система контроля за доступом к денежным ресурсам, которая должна удовлетворять двум, казалось бы, взаимоисключающим требованиям: всякий желающий имеет возможность обратиться к платёжной системе анонимно и, не раскрывая свою личность, доказать своё право на доступ.

Понятно, что обычные бумажные деньги обеспечивают оба свойства, кредитные карточки – ни одного. Возможна ли финансово-экономическая электронная платежная система, в которой проходят платежи (транзакции) с использованием специально выпущенной «электронной наличностью», без участия банковских пластиковых карт?

Идеальная система «электронных наличных» должна удовлетворять следующим требованиям [1]:

— платеж не зависит от местонахождения покупателя;
— безопасность, т.е. банкноту нельзя скопировать, подделать или использовать дважды;
— анонимность платежа;
— неотслеживаемость истории платежей;
— автономность платежа, то есть продавцу не надо немедленно связываться с банком-эмитентом банкноты;
— перемещаемость, то есть можно передавать банкноту другому лицу;
— делимость банкноты, то есть можно использовать часть номинала банкноты.

Для работы с «электронной наличностью» разрабатываются специальные криптографические протоколы. В этих протоколах принимают участие три участника: Клиент (он же Покупатель), Продавец и Банк-эмитент, размещающий электронные банкноты (ЭБ). Протокол состоит из трех основных транзакций: «Снятие со счета», то есть покупка Клиентом у Банка ЭБ, «Платеж», то есть передача Покупателем ЭБ Продавцу в качестве оплаты за некоторый товар и, соответственно, проверка Продавцом подлинности ЭБ, и «Депозит», то есть проверка Банком подлинности ЭБ и перечисление Банком номинала ЭБ Продавцу.

Описываемая ниже деловая игра «Цифровая наличность» представляет собой модель финансово-экономической ЭПС, в которой имитируются платежи с использованием специально выпущенной «электронной наличностью», без участия банковских пластиковых карт. В протоколе используется криптосистема RSA [2].

В этой криптосистеме под «электронной наличностью» понимается пара «очень больших» натуральных чисел, одно из которых подготовлено Покупателем и «вслепую» подписано Банком-эмитентом, а второе используется при проверке подлинности «электронной банкноты» Продавцом в Точке продаж (см. рис. 1).

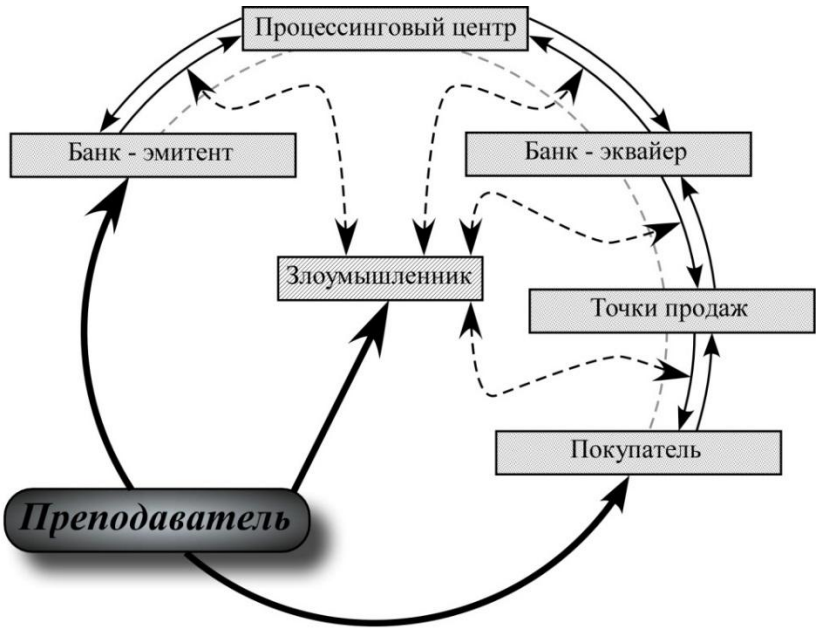

Рис. 1. Деловая игра «Цифровая наличность»

Участники игры моделируют действия различных составных частей ЭПС, осуществляя взаимодействия по точно описанному протоколу. Протокол представляет собой совокупность общих правил взаимодействия и обслуживания и подразумевает наличие криптографической защиты всех транзакций.

Игра является дидактической (обучающей), то есть все участники ставят перед собой педагогические цели. Среди этих целей основная: развитие информационной культуры студентов - участников игры. Это достигается общим погружением игры в профессиональную среду финансовой деятельности, осуществляемой в электронной форме с использованием информационных технологий банковской деятельности и средств криптографической защиты информации.

Основной метод игры: создание ситуационной модели действий в условиях возможных атак извне и нарушений протокола внутри ЭПС. Для этого в игру вводится «нетипичный» участник - злоумышленник, задача которого - нарушать все протоколы (что является также своеобразным и точно прописанным протоколом), подменять собой в злоумышленных целях любого участника, осуществлять действия, направленные против интересов других участников.

Основной замысел деловой игры: развитие прогностических способностей и информационной культуры личности, которые должны позволять осуществление не только текущих (типичных) действий, по защите информации, но и предсказывать возможные действия злоумышленника и нарушение протокола другими участниками, уметь строить защиту еще до возникновения угроз.

Банк генерирует некоторые простые числа p и q (они секретны), вычисляет $N = pq$, а также пару ключей $(e; d)$, из которых e – произволен, а d (секретен) вычисляется как ре-

шение уравнения $ed = 1(\mathrm{mod}\ \varphi(N))$. Числа N и e - открытые и известны всем, например, N=999997, e=921157.

Банк также вводит некоторую одностороннюю функцию $n \to f(n)$, которая также известна всем. Это может быть некоторая стандартная хэш-функция [3], но в данной деловой игре используется функция

$$n \to f(n) = a^n (\mathrm{mod}\ P),$$

где P - некоторое простое число ($P < N$), a – первообразный корень для модуля P. Величины P и a открыты для всех, например, P=999983, a=23.

Безопасность всех участников этой системы электронных платежей основывается на вере в стойкость криптосистемы RSA, что достигается использованием «очень больших» чисел, порядка 10 в 100-й и даже в 200-й степени. Так как вычислительные возможности учебных компьютеров ограничены, то в протоколах деловой игры вынужденно используются «не очень большие» числа [4].

Рассмотрим последовательно все три транзакции электронного платежа.

(I) «Снятие со счета». Клиент самостоятельно (или с помощью Банка) готовит предварительно некоторую информацию:

1). Выбирает n ($n < N$) - случайное число, которое будет играть роль номера электронной банкноты (ЭБ), и вычисляет f(n).

2). Выбирает r ($r < N$) - случайное число (затеняющий множитель), и одновременно вычисляет r^{-1} как решение уравнения $r * r^{-1} = 1(\mathrm{mod}\ N)$ (алгоритм Эвклида). Если решения не существует (что маловероятно), то необходимо выбрать иное r. В итоге Клиент вычисляет $\tilde{r} = f(n)r^e (\mathrm{mod}\ N)$. Это число передается Банку для подписания ЭБ.

3). Банк вычисляет $\tilde{\tilde{r}} = \tilde{r}^d (\mathrm{mod}\ N)$ и передает его Клиенту.

4). Клиент вычисляет $s = \tilde{\tilde{r}} * r^{-1} (\mathrm{mod}\ N)$, то есть снимает затемняющий модуль. При этом число $s = f(n)^d (\mathrm{mod}\ N)$ является подписанной Банком электронной банкнотой.

С этого момента пара чисел (n; s) является ЭБ.

(II) «Платеж». Покупатель (Клиент) передает Продавцу ЭБ, то есть пару чисел (n; s). Продавец самостоятельно (или с помощью Банка) производит проверку этой ЭБ:

1). Вычисляет f(n).

2). Вычисляет $\tilde{s} = s^e (\mathrm{mod}\ N)$.

3). Проверяет равенство: $f(n) = \tilde{s}$. Если равенство истинно, то ЭБ признается подлинной, в противном случае – нет.

(III) «Депозит». Продавец передает ЭБ (то есть пару чисел (n; s)) Банку. Банк производит окончательную проверку ЭБ (так же, как и Продавец), заносит эту пару чисел в базу данных оплаченных ЭБ и производит платеж Продавцу.

На этом период жизнедеятельности ЭБ закончился.

Приведем пример выполнения:

p=757, q=1321, (N)=997920, d=13.

Секретная информация:

n=251720 – номер ЭБ

$f(n) = a^n \pmod P$=793946

r=563002 – затеняющий множитель

r^{-1}=380319 – обратная величина

$r^e \pmod N$=941130

$\tilde{r} = f(n)r^e \pmod N$=640604

$\tilde{\tilde{r}} = \tilde{r}^d \pmod N$=523752

$s = \tilde{\tilde{r}}r^{-1} \pmod N$=434467.

Таким образом, покупатель получает {251720; 434467} – подписанную Банком ЭБ.

При проверке Продавец (или Банк) вычисляет:

$f(n) = a^n \pmod P$=793946 и $s^e \pmod N$= 793946.

Так как эти числа равны, то ЭБ - подлинная.

Задание деловой игры может представлять собой, например, проверку подлинности приведённых в табл.1 «электронных банкнот».

Таблица 1. Задание деловой игры

n	s	?
299887	219127	
875051	824109	
426635	61815	
509059	718243	
443297	438254	

n	s	?
828844	823953	
193904	835705	
279007	101019	
867983	565967	
53177	309686	

n	s	?
588455	175236	
580701	35440	
521068	440657	
920503	87430	
390924	62024	

Список литературы

1. *Введение в криптографию* / Под общ. ред. В.В. Ященко. 2-е изд., испр. М.: МЦМНМО: «ЧеРо», 1999. – 272 с.
2. Домашев А.В. *Программирование алгоритмов защиты информации. Учебное пособие.* / А.В. Домашев, В.О. Попов, Д.И. Правиков, И.В. Прокофьев, А.Ю. Щербаков. – М.: «Нолидж», 2000.
3. Сингх С. *Книга шифров: тайная история шифров и их расшифровки.* Пер. с англ. А. Галызина. М.: АСТ: Асатрель, 2007.
4. Жарков А.В. *Криптографические протоколы: учебно-методические рекомендации*. Ульяновск: УлГУ, 2011.