УДК 004.056:378 (147)

Технология использования криптосистемы Эль-Гамаля с помощью пакета компьютерной алгебры «Mathematica»

Коляда М.Г.
Донецкий национальный технический университет
E-mail: kolyada_mihail@mail.ru

Abstract

Kolyada M. Technology of use cryptosystem the El Gamal by means of a package of computer algebra «Mathematica»*. In article the technology of use cryptosystem the El Gamal by means of a package of computer algebra «Mathematica» is resulted. As a problem, the organization ciphering correspondences between two computer users in view of their digital signature is chosen.*

Введение

Современная криптография является очень важной, бурно развивающейся областью информационных технологий. Прерогативой этой науки является задача надежной аутентификации пользователей, под которой понимают подтверждение соответствия удаленного субъекта с тем, за кого он себя выдает. Используя терминологию информатики, о задаче аутентификации говорят как о системе клиент-сервер – сторона, инициирующая запрос и, соответственно, нуждающаяся в аутентификации, именуется клиентом, сторона, принимающая запрос и производящаяся аутентификацию, обычно называется сервером. Очевидно, что принятие сервером решения об аутентичности клиента может быть принято только на основе какой-либо уже имеющейся на сервере информации о клиенте, т. е. установление предварительного защищенного канала считается выполненным и выходит за рамки собственно процесса аутентификации [1, с. 361].

Большое число исследователей (А.П. Алферов, С.Г. Барычев, Ж. Брассар, Ю.В. Гатчин, А.В. Домашен, В. Жельников, А.Ю. Зубов, Н. Коблиц, А.Г. Коробейников, С. Коутинхо, А.С. Кузмин, А.И. Мартынов, В.А. Мухачев, В.И. Нечаев, А.А. Петров, Б.Я. Рябко, А. Саломаа, Д.В. Скляров, Н. Смарт, Р.Е. Серов, А.А. Терехов, Л.Ю. Щербаков, Б. Шнайер, Н. Фергюсон, А.Н. Фионов, В.М. Фомичев, В.А. Хорошко, А.В. Черемушкин, В.В. Ященко) посвятило свои научные работы изучению темы аутентификации, но, к сожалению, большинство из них имеет общетеоретический характер.

Как известно применение популярной открытой криптографической системы RSA (название – по имени авторов Ривеста, Шамира, Айдлемана) для шифрования и подтверждения электронной подписи не обладает полиномиальной стойкостью даже в отношении пассивного нападения на нее, а система Эль-Гамаля имеет такую стойкость, однако не защищена в отношении активного адаптивного противника. Поэтому часто приходится вручную перепроверять работу того, или иного блока работы этой системы шифрования или цифровой подписи. В многочисленной литературе по криптографии и криптоанализу обычно приводят теоретические выкладки использования этой системы, там нет практических механизмов их реализации. Иногда приводятся примеры программного использования системы Эль-Гамаля на языках программирования [2, с. 492], но возникает проблема проверки достоверности работы таких программ. Мы же, впервые предлагаем полную технологическую цепочку не только ручного просчета, но и его правильности, с использованием инструментальной среды псевдокода системы компьютерной алгебры пакета «Mathematica», достоверность работы которой не вызывает сомнения. Поэтому, актуальность материала очевидна, он будет полезен не только студентам, которые учатся на специальностях по направлению подготовки 1701 «Информационная безопасность», но и преподавателям, которые ведут практические занятия по прикладной криптологии, а также уже состоявшимся специалистам-практикам в области криптоанализа. Цель статьи и состоит в том, чтобы показать технологический механизм использования криптосистемы Эль-Гамаля с помощью программной математической среды компьютерной алгебры. В качестве задачи, выбрана организация шифрованной переписки между двумя компьютерными пользователями с учетом их электронной подписи.

1. Технология использования криптосистемы Эль-Гамаля

Криптосистема Ель-Гамаля предложенная ее автором (El Gamal T) в 1985 году, это фактически один из вариантов разработки открытых ключей Диффи-Хеллмана [3, с. 121]. Безопасность системы основывается на усложненности вычисления дискретных логарифмов в конечном поле.

Опишем организацию шифрованной переписки с помощью системы Эль-Гамаля между пользователями **A, B, C,...,** если **A** хочет получить шифрованные сообщения от пользователей **B, C,...**

1). Пользователь **A** генерирует открытый ключ k1, и закрытый ключ k_2. Для этого надо:

- выбрать простое большое число p и вычислить первоначальный корень g по модулю *2*. Это – первый и второй элементы открытого ключа k_1;

- наугад выбрать целое число a из интервала (*1; p-2*). Число a – закрытый ключ k_2;

- вычислить значения третьего элемента h открытого ключа k_1 из условия $h=g^a(mod\ p)$;

Открытый ключ k_1, то есть тройка чисел p, g, h, пользователь **A** посылает всем пользователям **B, C,...**

2). Каждый из пользователей B, C,...

- выбирает наугад случайное r – т.е. произвольное целое число из отрезка *[1; p-1]*;

- разбивает свои сообщения на блоки M. Каждый блок – элемент группы Z_p^*;

- шифрует блоки открытых сообщений по формулам:

$C_1=g^r(mod\ p)$, $C_2=M\ h^r(mod\ p)$;

- посылает криптограммы $Y=(C_1;\ C_2)$ пользователю **A**.

3). Для дешифровки криптограммы пользователь **A**, зная закрытый ключ a, вычисляет $D_k(C_1;\ C_2)= C_2)C_1^a)^{-1}(mod\ p)=M$.

Итак, именно подсказка C_1, дает возможность восстановить открытый текст на основе замаскированного вида C_2.

Замечание 1. Корректность шифрования доказать довольно легко, поскольку

$D_k(C) = M\ h^r((g^r)^a)^{-1}(mod\ p) = M\ h^r(g^{ra})^{-1}(mod\ p) = M$

(g - первоначальный корень по модулю p).

Замечание 2. Криптосистему Эль-Гамаля можно применять в любой оконченной группе G, в мультипликативной группе $GF(2^m)$ характеристики 2 или в группе точек эллиптической кривой над конечным полем.

Замечание 3. Шифровать разные открытые тексты M і M' следует с помощью разных генераторов случайных чисел, так как в противном случае соответствующие криптограммы $C=(C_1;\ C_2)$ и $C'=(C_1';\ C_2')$ объединенные соотношением $C_2\ (C')^{-1} = M_2\ (M')^{-1}$ и текст M' можно восстановить, если известный текст M.

Пример. *Сгенерировать ключи и зашифровать с использованием системы Эль-Гамаля открытое сообщение* ***M = 5***.

Решение. Выберем простое число **p = 11** и вычислим первоначальный корень **g = 2** по модулю **11**. Пусть **a = 6**. Далее определим последний элемент **h** открытого ключа по формуле $\mathbf{h=g^a(mod\ p) = 2^6(mod\ 11) = 9}$. Итак, открытый ключ $\mathbf{k_1 =11; 2; 9}$ и закрытый ключ $\mathbf{k_2 =a = 6}$ сформированы. Зашифруем сообщения **M = 5**, для чего выберем на собственное усмотрение случайное число **r = 9** из интервала **[1; p-1]** и вычислим:

$$\mathbf{C_1=g^r(mod\ p)=2^9(mod\ 11) = 6;}$$

$$\mathbf{C_2=M\ h^r(mod\ p)= 5\ 9^9(mod\ 11) = 3.}$$

Криптограмма имеет вид **(6;3)**. Рассмотрим процесс ее дешифровки:

$$\mathbf{D_k(C_1;\ C_2) = C_2(C_1^a)^{-1}(mod\ p);}$$

$$\mathbf{D_{k2}(6;\ 3) = 3(6^6)^{-1}(mod\ 11) = 3(46656)^{-1}(mod\ 11) = 3(5^{-1})(mod\ 11)}.$$

Поскольку $\mathbf{5^{-1}(mod\ 11) = 9}$, тогда

$$\mathbf{D_{k2}(6;\ 3) = 3\ 9\ (mod\ 11) = 27\ (mod\ 11) = 5.}$$

Тот же пример можно интерпретировать по-другому, но сначала:

Пусть ***p = 11*** *и* ***a = 6***. *Пользователь* ***A*** *случайным образом выбирает секретный показатель* $\boldsymbol{m_A = 28}$, *а пользователь* ***B*** *аналогично выбирает секретный показатель* $\boldsymbol{m_B = 55}$. *Они вычисляют свои публичные ключи с помощью функции* ***PowerMod***:

```
In[8]:= cA = PowerMod[6, 28, 11]
        cB = PowerMod[6, 55, 11]

Out[8]= 4

Out[9]= 10
```

Пользователь ***A*** *может вычислить общий с пользователем* ***B*** *ключ, возводя публичное* $\boldsymbol{c_B}$ *в степень* $\boldsymbol{m_A}$, *известное только ему, и получая:*

```
In[10]:= PowerMod[10, 28, 11]

Out[10]= 1
```

Пользователь ***B*** *получает тот же самый общий ключ, возводя* $\boldsymbol{c_A}$ *в степень* $\boldsymbol{m_B}$. *В самом деле:*

```
In[11]:= PowerMod[4, 55, 11]

Out[11]= 1
```

Продолжаем этот пример с публичными параметрами $p = 11$, $a = 6$ *и* $c_B = 10$. *Число* $m_B = 55$ *известно только пользователю* ***B***.

Предположим, что пользователь ***A*** *хочет подписать для пользователя* ***B*** *сообщение* $M = 5$. *Пусть* $r = 7$ *– случайное целое число, выбранное пользователем* ***A*** *(оно простое). Пользователь* ***A*** *вычисляет пару (R, S), вычисленную так:*

```
In[7]:= p = 11; a = 6; cB = 10; r = Rando
        M = 5; R = PowerMod[a, r, 11]
        S = Mod[PowerMod[cB, r, 11] * I

Out[7]= 7

Out[8]= 8

Out[9]= 6
```

При дешифровании пользователь **B** вычисляет $S/R_B^m \bmod p$, используя свое секретное число $m_B = 55$ и функции **Mod, PowerMod** пакета «Mathematica» Заметим, что *PowerMod [a, -1, p]* вычисляет мультипликативный обратный элемент к *a* по модулю *p*.

```
In[10]:= mB = 55;
         Mod[S * PowerMod[PowerMod[R,

Out[11]= 5
```

Перехватчик не может определить **r**, исходя из *R*, так как мы предполагаем, что проблема логарифмов не поддается решению. В силу этого перехватчик не способен выделить c_B^r из S (чтобы получить секретное **M**, которое у нас было равно 5).

2. Схема подписи Эль-Гамаля

Подписывание сообщения пользователем A.

Предположим, что пользователь ***A*** хочет послать *пользователю* ***B*** подписанное сообщение. Сообщение снова представлено числом **M** из {0,1,..., p - 2}.

Пользователь ***A*** выбирает случайное целое **r**, взаимно простое с $p - 1$, и вычисляет $R = a^r \bmod p$. Затем пользователь ***A***, использует свой секретный показатель $m_A = 28$ для вычисления числа S, удовлетворяющего сравнению:

$$M = m_A R + r S \ (mod\ p-1).$$

Чтобы эффективно найти *S*, можно использовать расширенную версию алгоритма Эвклида.

Пользователь ***A*** посылает пользователю ***B*** тройку (*M, R, S*), где пара (*R, S*) служит подписью к сообщению *M*.

Проверка подписи пользователем B.

Пользователь ***B*** получает подпись (*R, S*) вместе с сообщением *M* и проверяет эту подпись, убеждаясь, что

$$a^M = (c_A)^R R^S \ (mod\ p).$$

Это сравнение должно выполняться, так как в силу предыдущего соотношения:

$$a^M = a^{mA\,R}\, a^{r\,S} = (a^{mA})^R\, (a^r)^S = (c_A)^R\, R^S \ (mod\ p).$$

Продолжаем рассмотренный пример с публичными параметрами $p = 11$, $a = 6$ *и* $c_A = 4$. *Число* $m_A = 28$ *известно только пользователю* **A**. *Предположим, что пользователь* **A** *хочет подписать для пользователя* ***B*** *сообщение* $M=5$. *Пусть* $r = 97$ *– случайное число, выбранное пользователем* **A** *(оно простое). Пользователь* ***A*** *вычисляет:*

```
In[12]:= p = 11; a = 6; mA = 28; r = 97; M = 5; S =.;
         R = PowerMod[a, r, 11]
         S /. Solve[{r S == M - mA * R, Modulus == p - 1}, S][[1]]

Out[12]= 8

Out[13]= 3
```

чтобы найти подпись *(R, S) = (8, 3)*, которую он добавляет к своему сообщению *M*.

Пользователь ***B*** проверяет эту подпись, убеждаясь, что

$$a^M = (c_A)^R R^S \ (mod\ p):$$

```
In[16]:= cA = 4; R = 8; S = 3;
         PowerMod[a, M, p] ==
          Mod[ PowerMod[cA, R, p] * PowerMod[R, S, p], p]

Out[17]= True
```

Замечание. Введение в правило шифрования генератора случайных чисел **r** делает шифр Эль-Гамаля шифром многозначной замены. Случайность выбора параметра **r** дает возможность отнести этот шифр к схемам вероятностного шифрования, так как здесь открытый текст и ключ не определяют криптограмму однозначно.

Выводы

Особенностью системы цифровой подписи Эль-Гамаля является то, что она работает на основе генерации случайных чисел. Нахождение пары чисел (R, S) без знания секретного ключа вычислительно сложно – практически невозможно. Различных подписей, соответствующих данному документу, может быть чрезвычайно много, но выработать правильную подпись может только владелец секретного ключа. Для вычисления секретного ключа

по открытому ключу необходимо решить задачу дискретного логарифмирования, которая считается вычислительно очень сложной. Поэтому эту систему можно надежно использовать для контроля доступа к данным, подтверждения личности пользователя, аутентификации данных, подписывания «реальных документов», т.е. в межбанковских расчетах, при работе банка с физическими лицами: электронная коммерция, электронные переводы, электронные деньги и т.д.

Самым главным врагом криптографии на сегодняшний день является отнюдь не криптоанализ, а характер и привычки самого человека – конечного пользователя любой криптосистемы. Для того чтобы правильно пользоваться криптографией, нужно в первую очередь знать основы ее функционирования и базовые правила информационной безопасности. В том случае она будет четко, надежно и незаметно служить человеку, как и огромное множество других прикладных наук.

Литература

1. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 725 с.

2. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с.

3. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО «Полигрф-Кансалтинг», 2005. 215 с.

Поступила в редакцию 20.12.2009