ЧЕБЫШЕВСКИЙ СБОРНИК

Том 19. Выпуск 3.

УДК 511.313:511.331.1:511.526

DOI 10.22405/2226-8383-2018-19-3-61-73

Теория чисел и приложения в криптографии

Востоков Сергей Владимирович — доктор физико-математических наук, профессор, профессор кафедры алгебры и теории чисел Санкт-Петербургского государственного университета, президент фонда им. Л. Эйлера.

e-mail: sergei.vostokov@gmail.com

Востокова Регина Петровна — старший преподаватель, Балтийский государственный технический университет "Военмех".

e-mail: rvostokova@yandex.ru

Беззатеев Сергей Валентинович — доктор технических наук, доцент, заведующий кафедрой «Кафедра технологий защиты информации», Санкт-Петербургский государственный университет аэрокосмического приборостроения.

e-mail: bsv@aanet.ru

Аннотация

В статье рассмотрены некоторые элементы теории чисел и показано каким образом они используются в современных системах защиты информации. В качестве примеров выбраны наиболее известные протоколы и алгоритмы, такие как протокол Диффи-Хеллмана для создания парного ключа, алгоритмы шифрования с открытым ключом RSA и Эль Гамала. Рассмотрен обобщенный алгоритм Евклида, являющийся одним из наиболее часто встречающихся примитивов из теории чисел, используемом в криптографии. Приведены алгоритмы электронной подписи RSA и Эль Гамала. В заключение предложен алгоритм электронной подписи, основанный на билинейном преобразовании, использующем упрощенный вид спаривания в явном законе взаимности.

Ключевые слова: теория чисел, криптографические протоколы, несимметричные алгоритмы шифрования, электронное подписание, билинейное преобразование.

Библиография: 21 названий.

Для цитирования:

С. В. Востоков, Р. П. Востокова, С. В. Беззатеев. Теория чисел и приложения в криптографии // Чебышевский сборник, 2018, т. 19, вып. 3, с. 61–73.

CHEBYSHEVSKII SBORNIK

Vol. 19. No. 3.

UDC 511.313:511.331.1:511.526

DOI 10.22405/2226-8383-2018-19-3-61-73

Number theory and applications in cryptography

Vostokov Sergey Vladimirovich — doctor of physical and mathematical Sciences, Professor, Professor of algebra and number theory Department of St. Petersburg state University, President of the Foundation. L. Euler.

e-mail: sergei.vostokov@gmail.com

Vostokova Regina Petrovna — senior lecturer, Baltic State Technical University "Voenmech".
e-mail: rvostokova@yandex.ru

Bezzateev Sergei Valentinovich — Doctor of technical sciences, Saint-Petersburg State University of Aerospace Instrumentation.
e-mail: bsv@aanet.ru

Abstract

The paper describes some elements of the number theory and shows how they are used in modern information security systems. As examples, the most famous protocols and algorithms such as the Diffie-Hellman Protocol for pair key generation, RSA and El Gamal public key encryption algorithms. The generalized Euclid algorithm is considered, as a one of the most common element of the number theory used in cryptography. Algorithms are given RSA and El Gamal signature algorithms are given. In conclusion, the algorithm of the electronic signature based on bilinear transformation uses a simplified case of the pairing in the explicit law of reciprocity.

Keywords: number theory, cryptography protocols, public key cryptographic algorithms, signature, bilinear transformation.

Bibliography: 21 titles.

For citation:

S. V. Vostokov, R. P. Vostokova, S. V. Bezzateev, 2018, "Number theory and applications in cryptography", *Chebyshevskii sbornik*, vol. 19, no. 3, pp. 61–73.

1. Введение

Один мой друг, который закончил Ленинградский ВУЗ, спросил меня как-то: «Ну что ты делаешь в своей математике, ведь всю Высшую математику мы прошли в институте». В этой работе мы попробуем разъяснить это заблуждение очень многих людей не только в нашей стране. Попытаемся это сделать на примере теории чисел и криптографии.

Теория чисел очень древняя наука, которая сейчас переросла в направление «Арифметическая геометрия». Но даже самые давние фундаментальные результаты этой науки только в наше время находят применения в очень востребованной ныне прикладной науке — криптографии [5]. Мы покажем это на примере теоремы Эйлера из теории чисел, которая была доказана в середине XVIII века и нашла свое применение в созданном в 1978 году первом современном методе криптографии RSA[9].

Во второй части работы будет рассказано, как окончательное решение 9 проблемы Гильберта в 1978 году [2] дало в 2003 году новый способ электронной подписи.

2. Теория чисел

2.1. Функция Эйлера

Определим функцию Эйлера $\varphi(m)$ для целого числа $m > 1$ следующим образом.

Рассмотрим все остатки при делении на число m : $0, 1, 2, \dots, m-1$ и сосчитаем количество взаимно-простых с m остатков. Это число и будем называть функцией Эйлера.

Рассмотрим два частных случая:

1. Если p — простое число, то нетрудно заметить, что $\varphi(p) = p - 1$.
2. Если p и q — два различных простых числа, то $\varphi(pq) = (p - 1)(q - 1)$.

2.2. Теорема Эйлера

ТЕОРЕМА 1 (Эйлера). [1] Пусть a и m — взаимно простые числа, тогда выполнено сравнение

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad (1)$$

3. Расширенный Алгоритм Евклида

Для понимания выполняемых операций в криптографических преобразованиях одним из наиболее часто используемых инструментов является расширенный алгоритм Евклида для нахождения мультипликативно обратного по модулю некоторого целого числа. Надо отметить, что в общем случае применение этого алгоритма значительно шире и затрагивает не только криптографические преобразования но и, например, теорию алгебраического кодирования. Однако здесь мы остановимся только на возможностях этого замечательного алгоритма для наших целей, а именно, - вычисление числа x обратного по умножению числу y по модулю целого числа p .

$$x : x \cdot y \equiv 1 \pmod{p}.$$

Необходимым условием для нахождения такого x очевидно является взаимная простота y и p . В расширенном алгоритме Евклида используются вспомогательные элементы u_i связанные рекуррентной формулой $u_{i+1} = q_i \cdot u_i + u_{i-1}$ где $u_{-1} = 0, u_0 = 1$ и q_i - частное, полученное на i -ом шаге алгоритма.

Приведем теперь последовательность шагов алгоритма:

Шаг 1. $p = y \cdot q_1 + r_1, u_1 = q_1 \cdot u_0 + u_{-1}$, где q_1 и r_1 соответственно частное и остаток от деления p на y .

Шаг 2. $y = r_1 \cdot q_2 + r_2, u_2 = q_2 \cdot u_1 + u_0$,

Шаг 3. $r_1 = r_2 \cdot q_3 + r_3, u_3 = q_3 \cdot u_2 + u_1$,

...

Шаг i . $r_{i-2} = r_{i-1} \cdot q_i + r_i, u_i = q_i \cdot u_{i-1} + u_{i-2}$,

...

Шаг (ℓ) $r_{\ell-2} = r_{\ell-1} \cdot q_\ell + 1, u_\ell = q_\ell \cdot u_{\ell-1} + u_{\ell-2}$. Это последний шаг алгоритма, так как остаток, полученный на этом шаге равен 1 - наибольшему общему делителю чисел p и y .

Искомое значение x определяется следующим образом:

$$x \equiv (-1)^\ell \cdot u_\ell \pmod{p}.$$

4. Приложения в криптографии

4.1. Несимметричная криптография

История создания криптографических алгоритмов не менее загадочна и секретна чем сами алгоритмы [7]. Идея передачи секретной информации по незащищенному каналу была первоначально предложена James H. Ellis в 1970 году [12]. Затем Ellis, Cocks и Williamson в 1973 году [11] предложили идею алгоритма RSA, однако результат был засекречен Government Communications Headquarters (Великобритания) и лишь 18 декабря 1997, Clifford Cocks анонсировал его, сделав достоянием широкой общественности. К сожалению James Ellis умер 25

ноября 1997 за месяц до публичного анонсирования этого факта. В 2010 Malcolm Williamson, Clifford Cocks и James Ellis получили престижную награду Milestone Award Института IEEE (IEEE) за развитие криптографии с открытым ключом. Рассмотрим здесь, какой же алгоритм был предложен этими тремя британцами.

4.1.1. Алгоритм WCE

В качестве секретного ключа выбираются два большие простые числа p и q . Открытым ключом является их произведение $N = p \cdot q$. Сообщением m должно удовлетворять следующим ограничениям: это целое положительное число, $m < N$. Для того чтобы зашифровать сообщение, его необходимо возвести в степень открытого ключа N и результат взять по модулю N (то есть вычислить остаток от деления).

$$e = m^N \mod N \quad (2)$$

Таким образом, для зашифрования достаточно знание только открытого ключа. При этом отметим здесь, что открытый ключ в алгоритме WCE представляет собой одно число N являющееся произведением двух секретных простых чисел p и q таких что

$$(p, (q-1)) = 1, \quad (q, (p-1)) = 1.$$

Для того чтобы расшифровать сообщение e необходимо знание секретного ключа. Первоначально находится функция Эйлера $\varphi(N) = (p-1)(q-1)$ и вычисляется вспомогательное число c

$$c = N \mod \varphi(N).$$

Затем вычисляется секретный ключ d

$$d \cdot c = 1 \mod \varphi(N)$$

Для этого используется расширенный алгоритм Евклида. Здесь следует заметить, что автоматически выполняется очень важное свойство для корректной работы расширенного алгоритма Евклида. А именно - наибольший общий делитель чисел N и $\varphi(N)$ равен 1. И, наконец, зашифрованное сообщение e возводится в степень d .

$$m = e^d = m^{c \cdot d} = m^{1 \mod \varphi(N)} \equiv m \mod N$$

А теперь посмотрим официальную, наиболее часто встречающуюся, версию появления несимметричной криптографии.

4.1.2. Протокол Диффи-Хеллмана

В 1976 году американцы Уитфилд Диффи и Мартин Хеллман опубликовали в журнале IEEE Transaction on Information Theory статью "New directions in cryptography"[8] в которой описали схему шифрования без обмена секретным ключом по открытому каналу. Основной идеей, лежащей в основе предложенного протокола являлось использование проблемы дискретного логарифма. То есть отсутствие эффективного алгоритма вычисления числа x при известных простом числе p , и целых числах a и b .

$$a = b^x \mod p$$

Что же собой представляет этот протокол, опубликованный более 40 лет назад и до сих пор эффективно используемый в огромном числе практических приложений обеспечивающих

безопасный канал для любых двух устройств не имевших до этого никакой информации друг о друге и использующих для выработки секретного ключа канал связи свободно прослушиваемый всеми.

Первым шагом протокола является выбор сторонами в открытом обсуждении пары чисел : большого простого числа p и b -первообразного корня из 1 по модулю p . На втором шаге каждый из участников протокола выбирает свое секретное число . Соответственно x, y , $1 < x < p - 1, 1 < y < p - 1$. Для обмена по открытому, прослушиваемому каналу участники вычисляют числа , $a = b^x \bmod p$ и $c = b^y \bmod p$ соответственно. После получения этих значений участники протокола могут вычислить общий парный ключ K .

$$K = a^y = c^x \equiv b^{xy} \bmod p. \quad (3)$$

4.1.3. Алгоритм шифрования RSA

В 1978 году Рональд Райвест, Ади Шамир и Леонард Адлеман запатентовали и опубликовали свой алгоритм получивший в дальнейшем название RSA [9]. В этом же номере журнала, известный математик и учёный Мартин Гарднер по согласию авторов алгоритма, опубликовал математическую задачу, получившую название RSA-129. В условии задачи он указал два числа n и e - открытый ключ и зашифрованный текст. Длина числа n составляла 129 десятичных знаков, а число $e = 1007$. За расшифровку текста предполагалась премия в 100 долларов. Шифр удалось взломать через 17 лет — около 600 человек объединились в сеть и усилиями 1600 компьютеров за полгода смогли прочитать фразу в 1995 году:

«The Magic Words are Squeamish Ossifrage»¹

Основные этапы алгоритма RSA

Выбор секретного ключа и вычисление открытого ключа

Шаг 3. Выбираем большие простые числа p и q с близким количеством цифр, после чего вычисляем $N = pq$.

Шаг 4. Вычисляем $\varphi(N) = (p - 1)(q - 1)$.

Шаг 5. Случайным образом выбираем число c , взаимно простое с $\varphi(N)$.

Шаг 6. С помощью расширенного алгоритма Евклида вычисляем число d , такое что $c \cdot d \equiv 1 \bmod \varphi(N)$.

ОПРЕДЕЛЕНИЕ 1. Число d — секретный ключ, так же как и числа p и q .

ОПРЕДЕЛЕНИЕ 2. Пара (c, N) — открытый ключ, который распространяется открыто .

Шифрация сообщений с использованием открытого ключа

Сообщение может быть любое целое положительное число m не превосходящее N . При шифрации используется открытый ключ:

$$e \equiv m^c \bmod N.$$

Дешифрация с использованием секретного ключа

Возводим число e в степень d и ищем остаток числа e^d при делении на N . Это и будет искомое число m , так как

$$e^d = m^{cd} \equiv m^{1+k \cdot \varphi(N)} \equiv m + \ell \cdot N \equiv m \bmod N.$$

¹В переводе с английского: «Волшебные слова — это брезгливая скопа». Скопа — это птица, родственник стервятника.

ЗАМЕЧАНИЕ 1. Если число N имеет 100 цифр, то имеется не менее $4 \cdot 10^{42}$ простых числа, которые могут делить число N . Если компьютер выполняет 1 миллион операций в секунду, то ему понадобится примерно 10^{35} лет для вычисления $\varphi(N)$.

ЗАМЕЧАНИЕ 2. В алгоритме RSA, использованном Гарднером для своего конкурса, использовались 64 и 65-значные простые числа.

ЗАМЕЧАНИЕ 3. Сейчас для алгоритма RSA используют 150-значные простые числа.

4.2. Алгоритм Эль Гамала

Основные этапы алгоритма Эль Гамала

В 1985 году в журнале IEEE Transactions on Information Theory [10] Тахером Эль-Гамалем был предложен алгоритм шифрования использующий идеи протокола Диффи-Хеллмана. В отличие предыдущих авторов Эль-Гамаль не патентовал свою схему и во многом именно вследствие этого она была использована как основа для национальных стандартов в большинстве стран (Россия, США, Европа и т.д.).

Выбор секретного ключа и вычисление открытого ключа

Шаг 1. Выбираем большое простое число p и q - примитивный корень из единицы по модулю p .

Шаг 2. Случайным образом выбираем число c , $1 < c < p - 1$.

Шаг 2. Вычисляем $b = q^c \mod p$.

ОПРЕДЕЛЕНИЕ 3. Число c — секретный ключ.

ОПРЕДЕЛЕНИЕ 4. Тройка чисел (p, q, b) — открытый ключ, который распространяется открыто.

Шифрация сообщений с использованием открытого ключа

Сообщением может быть любое целое положительное число m не превосходящее N . При шифрации используется открытый ключ и случайное число r , $1 < r < p - 1$:

$$e \equiv m \cdot b^r \mod p.$$

ОПРЕДЕЛЕНИЕ 5. Зашифрованное сообщение представляется парой чисел:

$$(e, f \equiv q^r \mod p).$$

Дешифрация с использованием секретного ключа

Возводим число f в степень c и получаем $b^r \mod p$.

$$f^c = q^{rc} = q^{cr} = b^r \mod p$$

Используя расширенный алгоритм Евклида находим мультипликативно обратное d к b^r по модулю p .

$$d \cdot b^r \equiv 1 \mod p.$$

Теперь осталось умножить первое из пары чисел представленных в зашифрованном сообщении и мы получим исходное сообщение.

$$e \cdot d = m \cdot b^r \cdot d \equiv m \cdot 1 = m \mod p.$$

4.3. Электронная подпись

В предыдущем разделе мы посмотрели каким образом можно создать общий секретный ключ используя для этого открытый прослушиваемый канал связи. Однако шифрация решает лишь одну из трех основных задач информационной безопасности - обеспечение конфиденциальности хранимой, обрабатываемой и передаваемой информации. К сожалению, это не позволяет предотвратить незаметное изменение критически важной информации [5]. Очевидно, что злоумышленник, зная открытый ключ, которым было зашифровано исходное сообщение, может легко заменить его на другое [6]. Для того, чтобы этого нельзя было сделать требуется использовать некоторую секретную информацию - секретный ключ. Когда говорят про электронную подпись, то обязательно упоминается некоторая однонаправленная функция - хэш-функция, позволяющая сообщение любого размера преобразовать в "отпечаток" фиксированной длины (например 256 бит). Такое преобразование и выполняется с помощью хэш-функции. В английском языке одним из значений слова "hash" является "путаница". И действительно при выполнении хэш-преобразования исходная информация "запутывается" так, что распутать (восстановить) ее обратно практически не представляется возможным. Для реализации подписи исходная информация сначала хэшируется, а затем подписывается с помощью секретного ключа. Таким образом возникает первая уязвимость подписи - так называемая коллизия при вычислении хэш-функции. Очевидно, если два разных сообщения имеют один и тот же результат хэш-функции, то и подписи у этих сообщений будут одинаковые. Таким образом, можно просто подставить подпись одного сообщения под другим. Существуют два вида электронной подписи:

- отрицаемая подпись,
- неотрицаемая подпись.

Отрицаемая подпись подразумевает использование одного и того же секретного ключа и при вычислении и при проверке электронной подписи. В этом случае, очевидно, обе стороны могут подписать сообщение и невозможно будет доказать кто же из них на самом деле подписал документ.

Неотрицаемая подпись использует при вычислении секретный ключ пользователя, а при проверке - его открытый ключ. Такой вариант позволяет говорить о том, что подпись может быть сформирована только одним лицом - обладателем секретного ключа, в о время как поверить подпись может любой, кому известен его открытый ключ. Как мы с вами уже видели на примере алгоритмов несимметричного шифрования, знание открытого ключа не дает возможности вычислить соответствующий ему секретный ключ.

Рассмотрим теперь алгоритмы электронной подписи соответствующие приведенным ранее алгоритмам шифрования RSA и Эль Гамала.

4.4. Электронная подпись RSA

Используя введенные ранее обозначения опишем этапы вычисления электронной подписи и ее проверки, считая, что для сообщения m значение хэш-функции равно h и $h < N$. Тогда подпись s вычисляется следующим образом:

$$s = h^d \mod N.$$

После вычисления электронной подписи хранимой или передаваемой информацией является пара - сообщение и подпись - (m, s) . Не трудно заметить, что алгоритм подписи для RSA совпадает с алгоритмом расшифровки и естественным образом требует секретного ключа.

Для того чтобы проверить правильность электронной подписи s , то есть проверить не искажен ли исходный документ m и действительно ли он подписан конкретным лицом, имеющим открытый ключ (c, N) необходимо выполнить следующие действия:

- вычислить хэш функцию от проверяемого сообщения m' , $h' = Hash(m')$,
- проверить выполняется ли равенство $s^c \equiv h' \pmod{N}$.

Очевидно, что для выполнения этих операций необходим только открытый ключ (c, N) .

4.5. Электронная подпись Эль Гамала

Подпись Эль Гамала реализуется на много сложнее и главное требует использования случайного числа, что с одной стороны затрудняет ее вычисление, а с другой делает ее более защищенной, так как одно и то же сообщение подписанное тем же пользователем будет иметь каждый раз разную подпись.

При наличии секретного ключа c и открытого (p, q, b) нам понадобится еще случайное целое положительное число r , такое что $1 < r < p - 1$ и наибольший общий делитель r и $p - 1$ равен 1. Зачем требуется второе ограничение на это случайное число мы увидим немного позже. Электронная подпись s для сообщения m с хэш-функцией h вычисляется из соотношения

$$h \equiv r \cdot s + f \cdot c \pmod{p-1}.$$

где $f = q^r \pmod{p}$.

Не трудно заметить что здесь опять необходимо найти мультипликативно обратное к r по модулю $p - 1$ и это можно сделать только в том случае когда $(r, (p - 1)) = 1$. Подписью в системе Эль Гамала так же как и при шифровании являются два числа (s, f) .

Для проверки целостности сообщения и принадлежности подписи требуется сообщение m' , подпись (s, f) и открытый ключ пользователя. Если искажений не было, то есть $m' = m, h' = Hash(m') = Hash(m) = h$ и подпись была вычислена пользователем с открытым ключом (p, q, b) и соответствующим ему секретным ключом c то будет выполнено сравнение

$$q^{h'} \equiv f^s \cdot b^f \equiv q^{r \cdot s} \cdot q^{c \cdot f} \equiv q^{r \cdot s + c \cdot f} \equiv q^{h + \ell \cdot (p-1)} = q^h \pmod{p}.$$

4.6. Электронная подпись на билинейном преобразовании

Метод для создания электронной подписи, который сейчас будет предложен, использует упрощенный вид спаривания в явном законе взаимности, полученном С.В.Востоковым в работе [2].

Множество целых чисел, взаимно простых с p :

$$\mathbb{Z}^{(p)} = \{a \in \mathbb{Z} \mid \text{н.о.д. } ap = 1\}.$$

Из свойств взаимно-простых чисел ясно, что умножение оставляет числа из $\mathbb{Z}^{(p)}$ в этом же множестве.

Пусть $\mathbb{N}^+$ — множество натуральных чисел с операцией сложения. Зададим спаривание

$$\begin{aligned} \langle, \rangle_p: \quad \mathbb{Z}^{(p)} \times \mathbb{N}^+ &\rightarrow \mathbb{Z} \pmod{p} \\ \langle a, n \rangle &= l(a)n \pmod{p} \\ l(a) &= \frac{\log a^{p-1}}{p} \end{aligned}$$

Здесь $\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$

ОПРЕДЕЛЕНИЕ 6. Число a называем числом Вифериха, если $a^{p-1} \equiv 1 \pmod{p^2}$.
В противном случае будем называть антивифериховым.

УТВЕРЖДЕНИЕ 1. Спаривание $\langle \cdot, \cdot \rangle_p$ является билинейным, то есть

$$\begin{aligned} \langle ab, n \rangle_p &= \langle a, n \rangle_p + \langle b, n \rangle_p && \text{для любых } a \text{ и } b \text{ из } \mathbb{Z}^{(p)}; \\ \langle a, n+t \rangle_p &= \langle a, n \rangle_p + \langle a, t \rangle_p && \text{для любых } n \text{ и } t \text{ из } \mathbb{N}^+. \end{aligned}$$

Кроме того, это спаривание невырождено для антивиферихова числа a , то есть для такого a найдется n из $\mathbb{N}^+$ такое, что $\langle a, n \rangle_p = 1 \pmod{p}$.

ДОКАЗАТЕЛЬСТВО.

1. Билинейность по второму аргументу очевидна, а по первому следует из свойств логарифма.
2. Невырожденность. Пусть число a — антивиферихово. Тогда

$$\frac{a^{p-1} - 1}{p} \not\equiv 0 \pmod{p}.$$

Поэтому

$$\begin{aligned} L(a) &= \frac{\log(a^{p-1})}{p} = \frac{\log\left(1 + \frac{a^{p-1}-1}{p} \cdot p\right)}{p} = \\ &= \frac{\frac{a^{p-1}-1}{p} \cdot p}{p} - \frac{\left(\frac{a^{p-1}-1}{p} \cdot p\right)^2}{2p} + \dots = \frac{a^{p-1} - 1}{p} \end{aligned}$$

не делится на p . Тогда в качестве n можно взять такое число, чтобы спаривание $\langle a, n \rangle_p$ стало бы равно $1 \pmod{p}$.

Действительно, так как $\text{н.о.д.}(l(a)p) = 1$, то найдутся целые числа x и y такие, что $l(a)x + py = 1$. Заменяя, если нужно, x на $x' = x + pk$, а y на $y' = y - l(a)k$, получаем, при подходящем k , что x' — натуральное число. $\square$

4.6.1. Формирование подписи

Алиса — доверенное лицо (арбитр). Она выбирает большое простое число p , взаимно простое с ним антивиферихово число a из $\mathbb{Z}^{(p)}$ и натуральное число n из $\mathbb{N}^+$ такое, чтобы было выполнено сравнение

$$\langle a, n \rangle = \frac{a^{p-1} - 1}{p} \cdot n \equiv 1 \pmod{p}$$

Пусть x — случайное число такое, что $1 < x < p$, и s — решение сравнения $sx \equiv n \pmod{p}$.

ОПРЕДЕЛЕНИЕ 7. Набор (a, x, n) является секретным ключом.

Пусть $M = \{m_1, m_2, \dots, m_k\}$ — информация (сообщение). В криптографии определена функция, называемая хэш-функцией, которая однозначно задана информацией M .

Найдем остаток при делении a^{hx} на p^2 :

$$r = a^{hx} \pmod{p^2}, \quad 0 < r < p^2.$$

Подписанное сообщение имеет вид $\Pi = (M, r < s < h)$. Получатель Боб должен проверить подпись, то есть проверить справедливость сравнения

$$\frac{r^{p-1} - 1}{p} \cdot s \equiv h \pmod{p}, \quad (4)$$

то есть остаток $\frac{r^{p-1}-1}{p} \cdot s$ при делении на p должен быть равен ha .

УТВЕРЖДЕНИЕ 2. Если подпись верна, что сравнение (4) выполнено.

ДОКАЗАТЕЛЬСТВО. Вычислим спаривание $\langle r, s \rangle_p$. Имеем

$$\langle r, s \rangle_p \equiv l(r) \cdot s \equiv \frac{\log \left(1 + \frac{r^{p-1}-1}{p} \right)}{p} \cdot s = \frac{r^{p-1} - 1}{p} \cdot s \equiv h \pmod{p}.$$

Действительно, так как $r = a^{hx} \pmod{p^2}$, то

$$\begin{aligned} \langle r, s \rangle_p &= \langle a^{hx}, s \rangle_p \equiv x \langle a^h, s \rangle_p \equiv \\ &\equiv \langle a^h, sx \rangle_p \equiv h \langle a, n \rangle_p \equiv h \pmod{p}. \end{aligned}$$

□

УТВЕРЖДЕНИЕ 3. Подпись Π удовлетворяет требованиям к подписи, то есть

1. никто, кроме Алисы, не может подписать сообщение с ее подписью;
2. в случае конфликта Алиса с Бобом они обращаются к третьим лицам и судья проверяет подлинность подписи после предъявления ему чисел (a, x, n) .

Используя явную формулу закона взаимности [2, 3], а также полученные позднее соответствующие формулы в формальных модулях Любина-Тейта [13, 14, 16] и в формальных модулях Любина-Тейта [19, 20, 21] и явные формулы в многомерных локальных полях [15, 17, 18] можно применить их в алгоритме WCE, протоколе Диффи-Хеллмана и алгоритме Эль-Гамала, что будет сделано в последующих работах

5. Заключение

В данной работе рассмотрены криптографические примитивы шифрования и подписи, использующие основные понятия теории чисел. Предложен алгоритм электронной подписи, основанный на билинейном преобразовании использующем упрощенный вид спаривания в явном законе взаимности, описанный С. В. Востоковым в работе [2], где было дано окончательное решение 9-ой проблемы Гильберта.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. А. А. Бухштаб, Теория чисел, Москва, 1960
2. С. В. Востоков, Явная форма закона взаимности, Изв АН СССР, Сер мат, том 42, № 6, 1978
3. С. В. Востоков, Символы на формальных группах Изв. АН СССР, Сер. матем. том 45, № 5, 985-1014, 1981

4. Н. Коблиц, Курс теории чисел и криптографии, Москва, изд. ТВП, 2001, 254 с.
5. Б. Шнайер, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си, Москва, изд. Триумф, 2002, 816 с.
6. Б. Шнайер, Секреты и ложь. Безопасность данных в цифровом мире, изд. Питер, 2003, 366 с.
7. Д. Кан, Взломщики кодов, Центрполиграф, 2000, 480 с.
8. W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, vol. IT-22, pp. 472-492, 1976.
9. R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commun. ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.
10. T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. Inform. Theory, 31 (4), pp. 469-472, 1985
11. C. C. Cocks, A Note on non-secret encryption, UK Communications Electronics Security Group, November 20, 1973
12. J. H. Ellis, The possibility of secure non-secret digital encryption, CSEG Report 3006, January 1970.
13. С. В. Востоков, В. А. Лецко, Каноническое разложение в группе точек формальной группы Любина–Тэйта, Зап. научн. сем. ЛОМИ, 103 (1980), 52–57
14. С. В. Востоков, Символ Гильберта для формальных групп Любина–Тэйта I, Зап. научн. сем. ЛОМИ, 114 (1982), 77–95
15. С. В. Востоков, А. Н. Кириллов, Норменное спаривание в двумерном локальном поле, Зап. научн. сем. ЛОМИ, 132 (1983), 76–84
16. С. В. Востоков, И. Б. Фесенко, Символ Гильберта для формальных групп Любина–Тэйта II, Зап. научн. сем. ЛОМИ, 132 (1983), 85–96
17. С. В. Востоков, Явная конструкция теории полей классов многомерного локального поля, Изв. АН СССР. Сер. матем., 49:2 (1985), 283–308
18. D. G. Benous and S. V. Vostokov, Sur les representations p-adiques des corps locaux multidimensionnels attache's aux groups formels, J fuer die reine und angew. Math., 437(1993), 131-166
19. С. В. Востоков, О. В. Демченко, Явная формула спаривания Гильберта для формальных групп Хонды, Зап. научн. сем. ПОМИ, 272 (2000), 86–128
20. Falko Lorenz and Sergei Vostokov, Honda groups and explicit pairing on the module of Cartier curves, Algebraic Number Theory and Algebraic Geometry, Contemporary Mathematics 300, Parshin Festschrift, Ed. S. Vostokov and Y. Zarhin, AMS, Providence Rhode Island, 2002, pp. 143-170.
21. С. В. Востоков, Ф. Лоренц, Явная формула символа Гильберта для групп Хонды в многомерном локальном поле, Матем. сб., 194:2 (2003), 3–36

REFERENCES

1. A. A. Buhstap, 1960, *Teoriya chisel*, Moskva
2. S. V. Vostokov, 1978, "Yavnaya forma zakona vzaimnosti", *Izv AN SSSR, Ser mat*, tom 42, № 6
3. S. V. Vostokov, 1981, "Simvol'y na formal'nyh gruppah", *Izv. AN SSSR, Ser. matem.* tom 45, № 5, 985-1014
4. N. Koblic, 2001, *Kurs teorii chisel i kriptografii*, Moskva, izd TVP, 254 P.
5. B. SHnajer, 2002, *Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si*, Moskva, izd. Triumf, 816 P.
6. B. SHnajer, 2003, *Sekrety i lozh'. Bezopasnost' dannyh v cifrovom mire*, izd. Piter, 366 P.
7. D. Kan, 2000, *Vzломshchiki kodov*, Centrpoligraf, 480 P.
8. W. Diffie and M. Hellman, 1976, "New directions in cryptography", *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 472-492.
9. R. Rivest, A. Shamir, and L. Adleman, 1978, "A method for obtaining digital signatures and public key cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 120-126, Feb.
10. T. ElGamal, 1985, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Trans. Inform. Theory*, 31 (4), pp. 469-472
11. C. C. Cocks, 1973, "A Note on non-secret encryption", *UK Communications Electronics Security Group*
12. J. H. Ellis, 1970, "The possibility of secure non-secret digital encryption", *CSEG Report 3006*.
13. S. V. Vostokov, V. A. Lecko, 1980, "Kanonicheskoe razlozhenie v gruppe toчек formal'noj gruppy Lyubina-Tehjta", *Zap. nauchn. sem. LOMI*, 103, pp. 52-57
14. S. V. Vostokov, 1982, "Simvol Gil'berta dlya formal'nyh grupp Lyubina-Tehjta I", *Zap. nauchn. sem. LOMI*, 114, pp. 77-95
15. S. V. Vostokov, A. N. Kirillov, 1983, "Normennoe sparivanie v dvumernom lokal'nom pole", *Zap. nauchn. sem. LOMI*, 132, pp. 76-84
16. S. V. Vostokov, I. B. Fesenko, 1983, Simvol Gil'berta dlya formal'nyh grupp Lyubina-Tehjta II, *Zap. nauchn. sem. LOMI*, 132, pp. 85-96
17. S. V. Vostokov, 1985, "Yavnaya konstrukciya teorii polej klassov mnogomernogo lokal'nogo polya", *Izv. AN SSSR. Ser. matem.*, 49:2, pp. 283-308
18. D. G. Benous and S. V. Vostokov, 1993, "Sur les representations p-adiques des corps locaux multidimensionnels attache's aux groups formels", *J fuer die reine und angew. Math.*, 437, pp. 131-166
19. S. V. Vostokov, O. V. Demchenko, 2000, "Yavnaya formula sparivaniya Gil'berta dlya formal'nyh grupp Hondy", *Zap. nauchn. sem. POMI*, 272, pp. 86-128

-
20. Falko Lorenz and Sergei Vostokov, 2002, "Honda groups and explicit pairing on the module of Cartier curves", *Algebraic Number Theory and Algebraic Geometry, Contemporary Mathematics 300*, Parshin Festschrift, Ed. S. Vostokov and Y. Zarhin, AMS, Providence Rhode Island, pp. 143-170.
21. S. V. Vostokov, F. Lorenc, 2003, "Yavnaya formula simvola Gil'berta dlya grupp Hondy v mnogomernom lokal'nom pole", *Matem. sb.*, 194:2, pp. 3-36

Получено 01.09.2018

Принято к печати 10.10.2018