ЭЛЕМЕНТЫ КРИПТОЛОГИИ

В. А. АРТАМОНОВ
Московский государственный университет им. М.В. Ломоносова

BASIC CRYPTOLOGY

V. A. ARTAMONOV

A survey of some basic algebraic aspects of cryptology is presented.

Изложены основные алгебраические аспекты криптологии.

ВВЕДЕНИЕ

Криптологией называется раздел математики, занимающийся изучением возможных способов шифрования информации (сокрытия от незаконного пользователя) и способов вскрытия шифров. В статье излагаются некоторые известные способы шифрования и дается их математическое объяснение. Подробнее с затрагиваемыми вопросами можно познакомиться в приведенной в конце статьи библиографии.

ШИФРЫ ПОДСТАНОВКИ

Потребность в сокрытии информации возникла в глубокой древности и связана с развитием государственности. Один из наиболее старых способов скрытия и передачи информации известен из истории Древнего Востока. На бритой голове раба писали сообщение. Выждав время, когда волосы на голове вырастут и сделают сообщение невидимым, раба посылали гонцом для передачи информации адресату. Ясно, что этот способ передачи информации крайне ненадежен и требует много времени для его реализации. Более прогрессивный способ сокрытия и передачи информации применялся в Спарте в IV веке до н.э. (*Ксенофонт.* Греческая история. СПб.: Алетейя, 1996. С. 97). Вот как объясняет это изобретение Плутарх (Сравнительные жизнеописания. М.: Наука, 1994. Т. 1: Лисандр, 19. С. 496): “Отправляя к месту службы начальника флота или сухопутного войска, эфоры берут две круглые палки совершенно одинаковой длины и толщины. Одну оставляют себе, другую передают отъезжающему. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую вроде ремня полосу папируса, наматывают ее на свою скиталу, не оставляя на ней ни одного промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, пишут на нем то, что нужно, а написав, снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, но разбросаны в беспорядке, прочитать написанное он может только взяв свою скиталу и намотав на нее вырезанную полосу, располагая ее извивы в

прежнем порядке, чтобы, водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение. Полоса папируса называется, как и деревянная палка, скиталой, подобно тому как измеряемый предмет называется по мере".

С математической точки зрения шифр скитал (или сцитал) представляет собой следующий способ шифрования. Предположим для простоты, что полоса является объединением трех непересекающихся частей, каждая из которых содержит по восемь букв и обвивает скиталу по диаметру. Тогда выражение ⟨МАТЕМАТИКА И КРИПТОЛОГИЯ⟩ записывается вдоль скиталы последовательно в восемь столбцов высоты 3. При разматывании полосы на ней возникает надпись: ⟨МЕТА ИОГАМИ КПЛИТАКИРТОЯ⟩.

Следующий интересный шифр принадлежит Г.Ю. Цезарю. Он предложил записывать сообщение, написанное на латинском языке, в котором 26 букв, используя сдвиг букв в латинском алфавите на 3 (по модулю 26). В этом случае слово ⟨MATHEMATICS⟩ преобразуется в слово ⟨PDWKHPDWLFV⟩.

Оба способа шифрования укладываются в следующую математическую конструкцию. Пусть X – алфавит открытого и шифрованного текстов. Предположим, что задано биективное отображение F множества X в себя. При этом сообщение $xy\ldots z$ переходит в $F(x)F(y)\ldots F(z)$. Далее можно считать, что текст разбивается на k блоков одинаковой длины m. Поэтому для большей скрытности полученные блоки переставляются в соответствии с заданной перестановкой степени k. Разумеется, можно и далее усложнять приведенные способы шифрования. Отметим, что при всех этих способах используется один алфавит, причем в процессе шифрования разные буквы переходят в разные.

Для описания этого способа шифрования нам необходимо привлечь соответствующий математический аппарат. Пусть m – фиксированное натуральное число. Для любого целого числа d через $[d]$ обозначим остаток от деления числа d на m. Обозначим через Z_m множество $[0], [1], \ldots, [m-1]$ всех остатков от деления целых чисел на m. Тогда на Z_m можно ввести операцию сложения и умножения. Положив $[a][b] = [ab]$, $[a] + [b] = [a + b]$, где ab и $a + b$ – произведение и сумма a, b как целых чисел. Несложная проверка показывает, что эти операции определены корректно, причем они обладают следующими свойствами:

$$([a][b])[c] = [a]([b][c]),$$
$$[a][b] = [b][a],\ [a][1] = [a],$$
$$([a] + [b]) + [c] = [a] + ([b] + [c]),$$
$$[a] + [b] = [b] + [a],\ [a] + [0] = [a],$$
$$([a] + [b])[c] = [a][c] + [b][c].$$

Таким образом, можно производить с элементами Z_m обычные алгебраические вычисления, учитывая лишь, что $[ml] = [0]$ для всех целых чисел l. Множество Z_m с введенными операциями сложения и умножения называется кольцом вычетов по модулю m.

Теорема 1. *Пусть a, n – целые числа, причем $n > 0$. Следующие условия эквивалентны:*

1) *числа a, n взаимно просты;*

2) *существует такое целое число d, что $ad - 1$ делится на n;*

3) *отображение, переводящее каждый элемент $[x]$ из Z_n в $[a][x]$, является взаимно однозначным.*

Вернемся теперь к шифру Цезаря. Пусть, например, мы работаем в латинском алфавите, состоящем из 26 букв. Записав этот алфавит и отождествив букву алфавита с номером i с элементом $[i]$, можно отождествить буквы алфавита с элементами кольца вычетов Z_{26}. Тогда процесс шифрования можно понимать как отображение, переводящее произвольный элемент $[x]$ в $[a][x] + [b]$, где $[a]$, $[b]$ – элементы Z_{26}, причем число a взаимно просто с 26 в силу теоремы 1. Так при $a = 1$, $b = 3$ получается шифр Цезаря.

Нетрудно указать способ взламывания этих шифров. Предположим, что вы зафиксировали достаточно большое количество шифрованных сообщений. Кроме того, предположим, что вы знаете, что в сообщениях используется русский алфавит. В этом случае необходимо воспользоваться таблицами частот букв (в процентах) в русском алфавите (табл. 1).

Таким образом, мы видим, что практически все буквы имеют разные частоты. Следовательно, анализируя текст, вы можете по частоте использования каждого символа в зашифрованном сообщении определить, какая буква зашифрована этим символом. Аналогичная таблица частот букв в английском алфавите приведена в [2, с. 263]. Отметим, что работа по анализу и прочтению текстов, зашифрованных с помощью перестановок

Таблица 1

Буква	Частота	Буква	Частота	Буква	Частота
А	6,2	Л	3,5	Х	0,9
Б	1,4	М	2,6	Ц	0,4
В	3,8	Н	5,3	Ч	1,2
Г	1,3	О	9,0	Ш	0,6
Д	2,5	П	2,3	Щ	0,3
Е	7,2	Р	4,0	Ы	1,6
Ж	0,7	С	4,5	Ъ, Ь	1,4
З	1,6	Т	5,3	Э	0,3
И	6,2	У	2,1	Ю	0,6
К	2,8	Ф	0,2	Я	17,5

букв (и с использованием другого алфавита), широко отражена в художественной литературе (см., например, Э. По “Золотой жук”, А. Конан Дойль “Пляшущие человечки”).

ИСПОЛЬЗОВАНИЕ КЛЮЧЕВОГО СЛОВА

Следующий важный этап развития теории шифрования связан с именами Блеза де Виженера (Франция, XVI век) и Джероламо Кардано (Италия, XVI век). Виженер предложил использовать для шифрования *ключевое слово*. Поясним его идею на примере. Пусть слово КНИГУ является ключевым, и нам предстоит зашифровать слово МАТЕМАТИКА. Ключевое слово состоит из пяти букв. Поэтому шесть раз запишем русский алфавит. Первый раз в естественном порядке, затем циклически его переставляя и начиная последовательно с каждой из букв ключевого слова. Получаем табл. 2.

Таблица 2

*	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т
0	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ь
1	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ь	э	ю	я
2	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
3	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х
4	у	ф	х	ц	ч	ш	щ	ъ	ь	э	ю	я	а	б	в	г	д	е

Начинаем процесс шифрования. Берем i-ю букву слова МАТЕМАТИКА и находим ее в строке $*$. Вычисляем остаток $[j] = [i]$ при делении числа i на пять, $j = 0, 1, 2, 3, 4$. Находим в столбце под i-й буквой строки $*$ букву, стоящую в j-й строке. Именно на эту букву заменяем шифруемую i-ю букву. Таким образом, получаем слово ⟨ХНЪИЯКЯСНУ⟩.

Из приведенного примера видно, что разным буквам исходного слова могут соответствовать одинаковые буквы (это зависит от положения буквы в слове) в зашифрованном слове и, наоборот, одной букве могут соответствовать в зависимости от положения буквы разные буквы в зашифрованном слове. Таким образом, приведенный шифр можно понимать как обобщенный шифр Цезаря с переменным сдвигом. Отметим, что, зная ключевое слово, нетрудно расшифровать ваше сообщение.

Изложенный процесс шифрования можно перевести на алгебраический язык. Ключевое слово состоит из пяти букв. Поэтому шифруемое сообщение записываем в одно слово без пробелов и затем разбиваем его на слова, состоящие из пяти букв. Заменим каждую букву на число $i = 0, 1, ..., 32$, обозначающее номер его места в русском алфавите. Тем самым возникает набор векторов $(x_1, x_2, ..., x_5)$ длины 5 с координатами $x_1, x_2, ..., x_5$ из кольца вычетов Z_{33}. Таким образом, шифруемое сообщение представляет собой некоторое множество векторов $X = \{(x_1, x_2, ..., x_5)\}$. Процесс шифрования состоит в применении ко всем элементам заданного множества векторов преобразования, переводящего каждую строку $(x_1, x_2, ..., x_5)$ в строку

$$(x_1, x_2, ..., x_5)A + (b_1, b_2, ..., b_5), \qquad (1)$$

где $A = (a_{ij})$ – фиксированная квадратная матрица размера 5 с элементами a_{ij} из Z_{33}, а $(b_1, b_2, ..., b_5)$ – фиксированный вектор с коэффициентами из Z_{33}. Напомним, что $(x_1, x_2, ..., x_5)A$ является вектором длины 5, i-я координата которого равна $x_1a_{1i} + x_2a_{2i} + x_3a_{3i} + x_4a_{4i} + x_5a_{5i}$. Ключом в этом случае являются матрица A и вектор $b = (b_1, b_2, ..., b_5)$. Для того чтобы каждое сообщение однозначно расшифровалось, необходимо и достаточно, чтобы матрица A была обратима над кольцом Z_{33}. Это означает, что ее определитель $\det A$ должен быть обратимым в кольце Z_{33}. Мы всегда можем понимать A как квадратную матрицу с целыми коэффициентами. Поэтому условие обратимости A в силу теоремы 1 означает, что $\det A$ как целое число должно быть взаимно просто с числом 33, то есть не делиться на 3 и 11. Для расшифровки сообщения необходимо совершить обратное преобразование, которое переводит строку Y в строку

$$YA^{-1} - bA^{-1}. \qquad (2)$$

В известной мере сложность расшифровки диктуется сложностью вычисления обратной матрицы и решения квадратных систем линейных уравнений.

Долгое время шифры Виженера и их модификации считались невзламываемыми. Политические деятели Франции XVI – XVII веков постоянно применяли эти шифры в своей переписке. Примечателен в этом отношении следующий абзац из мемуаров активного политического деятеля Фронды, парижского архиепископа кардинала де Реца, середина XVII века (*Кардинал де Рец.* Мемуары. М.: Наука, 1997. С. 581–582. (Литературные памятники)): “Мы с принцессой Пфальцской пользовались шифром, который прозвали непроницаемым, уверенные, что его нельзя прочесть, не зная слова, служащего к нему ключом. Мы полагались на него настолько безоглядно, что с его помощью не обинуясь сообщали друг другу самые важные и сокровенные тайны, доверяя их простым гонцам. ...Принц де Конде, у которого на службе состоял один из самых искусных в мире отгадчиков тайнописи – его, помнится, звали Мартен, – шесть недель продержал у себя в Брюсселе этот шифр и вернул мне его, признав, что Мартен подтвердил: прочитать его нельзя. Вот, казалось бы, неоспоримое доказательство достоинств шифра, но недолго спустя он был разгадан. Жоли, который, хотя и не

знал шифровального ремесла, поразмыслил, нашел в нему ключ и представил его мне в Утрехте, где я находился. Простите мне это маленькое отступление, быть может небесполезное".

Лишь в 1863 году прусским офицером Ф.В. Касиским был найден простой способ поиска ключа для шифра Виженера. Более подробно об этом см. [2, параграф 4.2.1].

Для повышения стойкости шифров можно периодически менять ключевое слово. Опишем современный способ открытого распределения ключей. Он основан на следующем принципе. Пусть n – произвольное натуральное число и

$$n = p_1^{m(1)} \dots p_k^{m(k)} \qquad (3)$$

– его разложение в произведение степеней различных простых чисел $p_1, p_2, \dots, p_k$ с показателями $m(1), m(2), \dots, m(k)$. Функцией Эйлера называется число $\varphi(n)$ всех натуральных чисел, меньших n и взаимно простых с n. Другими словами, $\varphi(n)$ – это число элементов a из кольца вычетов Z_n, удовлетворяющих всем условиям теоремы 1.

Теорема 2. *Пусть n – натуральное число из* (3). *Тогда* $\varphi(n) = p_1^{m(1)-1} p_2^{m(2)-1} \dots p_k^{m(k)-1}(p_1 - 1)\dots(p_k - 1)$.

Теорема 3. *Пусть n – натуральное число из* (3). *Тогда для любого целого числа d разность $d^{\varphi(n)} - 1$ делится на n.*

Теорема 4. *Пусть p – простое число. Тогда существует такое число $a = 1, 2, \dots, p - 1$, что для любого целого числа b, не делящегося на p, найдется такое натуральное число m, что $a^m - b$ делится на p.*

Другими словами, учитывая теорему 3, получаем, что Z_p состоит из элементов $\{[0], [1], [a], [a^2], \dots, [a^{p-1}]\}$. Элемент a из теоремы 4 называется примитивным (порождающим). Отметим, что примитивный элемент a по p определен неоднозначно. Можно показать, что если элемент a является примитивным в Z_p, то этим же свойством обладает и элемент a^{p-2}. Укажем примеры примитивных элементов для малых простых чисел p. Например, если $p = 2$, то $a = 1$. Если $p = 3$, то $a = 2$. Если $p = 5$, то в качестве a можно брать либо 2, либо 3. Действительно, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, и 8 сравнимо с 3 по модулю 5. Наконец, $2^4 = 1 \pmod 5$. В случае $p = 7$ в качестве a можно брать либо 3, либо 5. В общем случае задача о нахождении элемента a является одной из трудных в теории чисел.

В связи с теоремой 4 возникает следующая интересная задача *дискретного логарифмирования*, то есть по заданным a, b из теоремы 4 найти такое целое неотрицательное число $n < q$, что $a^n - b$ делится на p, то есть $[a]^n = b$ в Z_p. Для этой задачи, разумеется, можно осуществить полный перебор всех элементов из Z_p и проверки этого условия. Но это требует больших вычислительных ресурсов и неприемлемо с практической точки зрения при больших p. Поэтому возникла идея использовать данный факт в криптографии для открытого распределения ключей. Пусть p – достаточно большое простое число и Z_p – вычеты по модулю p. Выберем некоторым образом порождающий элемент a в Z_p. Пусть два абонента A, B обмениваются по открытому каналу связи числами a, p. Далее абоненты A, B выбирают числа $x, y = 1, 2, \dots, p - 1$ соответственно, которые они держат в секрете. Затем по открытому каналу связи они обмениваются числами a^x, a^y. Абонент A, получив число a^y, возводит его в степень x и получает число a^{yx}. Ту же операцию проводит B и получает число a^{xy}, которое и берется в качестве ключа. Посторонний наблюдатель знает числа a, p, a^x, a^y, но не знает чисел x, y. Для нахождения этих чисел и вычисления ключа a^{xy} необходимо решить задачу дискретного логарифмирования.

СИСТЕМА RSA

Все рассмотренные выше криптосистемы носили линейный характер, поскольку системы шифрования (1) и дешифрования (2) сводятся к линейному преобразованию и решению систем линейных уравнений над кольцом вычетов. Принципиально новая система была предложена в конце 70-х годов XX века У. Диффи, М.Э. Хеллмэном, а также Р. Ривестом, А. Шамиром, Л. Адлеманом. По имени последних трех авторов эта система названа RSA-системой. Предположим, что достаточно большое натуральное число n разлагается в произведение двух простых чисел: $n = pq$. Предположим, что e, d – два натуральных числа, причем $de - 1$ делится на $\varphi(n)$, где $\varphi(n) = (p - 1)(q - 1)$ – значение функции Эйлера. Будем рассматривать шифруемое сообщение x как элемент кольца вычетов Z_n, то есть $x = [1], [2], \dots, [n - 1]$, причем x не делится ни на p, ни на q. Это означает в силу теоремы 3, что $x^{\varphi(n)} = [1]$ в Z_n. Процесс шифрования состоит в применении отображения возведения в степень, то есть x заменяется на x^e в кольце вычетов Z_n. В этом случае процесс дешифровки также состоит в применении отображения возведения в степень, то есть x заменяется на x^d в кольце вычетов Z_n. Так как $de = 1 + m\varphi(n)$ для некоторого целого числа m, то по теореме 3 в кольце вычетов Z_n получаем

$$x^{de} = x^{1 + m\varphi(n)} = x \cdot x^{m\varphi(n)} = x[1] = x. \qquad (4)$$

Процесс возведения произвольного числа x в степень d не является сложным. Достаточно многократно возводить числа в квадрат и затем перемножать результаты. Этот алгоритм требует не более $3[\log_2 n]$ умножений [4, с. 13]. Кроме того, поскольку вычисления осуществляются в кольце вычетов Z_n, то требуется брать остаток при делении на n. К тому же требуется находить

разложения из теоремы 2, которое требует $O(\log_2 n)$ времени [4, с. 11].

Напомним, что в математике принята следующая терминология. Пусть $f(n)$, $g(n)$ – две последовательности. Говорят, что последовательность $f(n)$ растет как $O(g(n))$, если существует такая ненулевая константа C, что отношение $f(n)/g(n)$ стремится к C вместе с ростом n. Таким образом, процесс шифрования и дешифрования представляется несложной процедурой, не требующей больших вычислительных ресурсов, поскольку рост $O(\log_2 n)$ представляется довольно медленным. Для начала работы с этим шифром всем абонентам по открытому каналу передается справочник с набором пар чисел n_i, e_i, соответствующих i-му абоненту сети для любого i. При этом каждое число n_i является произведением двух различных простых чисел $n_i = p_i q_i$. Числа d_i являются секретными. Для передачи сообщений x от i-го абонента j-му необходимо x преобразовать в x^f, $f = e_j$, в Z_n и переслать его по открытому каналу связи. j-й абонент, получив x^f, возводит его в степень d_j и получает x в силу (4). При этом i-й абонент может подписать свое сообщение. Для этого он посылает текст m^g, где $g = d_i e_j$, причем все вычисления m^g происходят в Z_k, $k = n_j$. j-й абонент дешифрует это сообщение, возводя его в степень $d_j e_i$, и получает m. При этом если он возводит его в другую степень $d_j e_s$, где s отлично от i, то получает бессмысленное сообщение. Другими словами, j-й абонент точно уверен, что он получил сообщение от i-го абонента.

Посторонний наблюдатель знает числа x^f, e_j, n_j. Для нахождения x ему необходимо знать d_j. Для этого в силу равенства $d_j = 1 + m\varphi(n_j)$ нужно уметь вычислять число $\varphi(n_j) = (p_j - 1)(q_j - 1) = n_j - (p_j + q_j) + 1$. Поскольку число n_j известно из справочника, то для решения задачи дешифровки нужно уметь вычислять $p_j + q_j$. Число $n_j = p_j q_j$, как известно, включено в справочник. Но тогда в силу теоремы Виета наша задача сводится к нахождению самих чисел p_j, q_j, то есть к задаче о разложении числа n_j в произведение двух простых чисел p_j, q_j.

RSA-система требует для большого числа абонентов построения достаточно больших простых чисел и разработки быстрых критериев проверки простоты заданного большего числа n. Обзор литературы по этому вопросу можно найти в [1; 4, гл. 2, § 3].

Значительно сложнее оказался вопрос о разложении заданного большого числа на простые множители, даже если известно, что их всего два. В 1977 году Р. Ривестом, А. Шамиром, Л. Адлеманом была составлена таблица с указанием машинного времени, необходимого для существовавших тогда компьютеров, чтобы разложить наугад взятое натуральное число с данным количеством десятичных знаков на множители (табл. 3).

Таблица 3

Число знаков	Число операций	Время
50	$1{,}4 \cdot 10^{10}$	3,9 часа
75	$9{,}0 \cdot 10^{12}$	104 дня
100	$2{,}3 \cdot 10^{15}$	74 года
200	$1{,}2 \cdot 10^{23}$	$3{,}8 \cdot 10^{9}$ лет
300	$1{,}5 \cdot 10^{29}$	$4{,}9 \cdot 10^{15}$ лет
500	$1{,}3 \cdot 10^{39}$	$4{,}2 \cdot 10^{25}$ лет

Хотя за прошедшие годы вычислительные возможности возросли, характер табл. 3 принципиально не изменился. Обзор попыток решить поставленную задачу теоретико-числовыми методами изложен в [5]. Скорее всего, решение этой задачи будет найдено при построении квантового компьютера, теоретические обоснования для которого были изложены на математическом конгрессе в Берлине в августе 1998 году. По замыслу создателей этот компьютер будет решать задачу разложения числа с n десятичными знаками за время $O(n^k)$ для некоторого натурального k, не зависящего от n. Построение физической и математической модели такого компьютера – это задача будущего столетия. Подробнее с этими применениями и деталями обоснования RAS-системы можно познакомиться в статье В.А. Успенского [3], в книгах [1, 2]. Таким образом, исследования в указанном направлении находят и будут находить широкое применение. Можно выразить надежду, что новые поколения математиков смогут внести достойный вклад в развитие этих областей.

ЛИТЕРАТУРА

1. Введение в криптографию / Под ред. В.В. Ященко. М.: МЦНМО-Черо, 1998. 272 с.

2. *Акритас А.* Основы компьютерной алгебры с приложениями. М.: Мир, 1994. 544 с.

3. *Успенский В.А.* Как теория чисел помогает в шифровальном деле // Соросовский Образовательный Журнал. 1996. № 6. С. 122–127.

4. *Манин Ю.И.*, *Панчишкин А.А.* Введение в теорию чисел // Современные проблемы математики: Фундаментальные направления. М.: ВИНИТИ, 1990. Т. 49: Теория чисел 1. 348 с.

5. *Boeneh Dan.* Twenty Years of Attacks on the RSA Cryptosystem // Not. Amer. Math. Soc. 1999. Vol. 46, № 2. P. 203–213.

Рецензент статьи Ю.П. Соловьев

* * *

Вячеслав Александрович Артамонов, доктор физико-математических наук, профессор кафедры высшей алгебры механико-математического факультета МГУ. Область научных интересов – кольца, универсальная алгебра и их приложения. Автор 90 научных работ и двух книг.