Компьютерные инструменты в образовании, 2017
№ 5: 5–11
УДК: 004.056.55 + 003.26
http://ipo.spb.ru/journal



# КОД ОБЩЕГО ДОСТУПА

Коточигов А. М.[1], Левицкий Д. В.[1], Носова О. А.[1]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, Россия

**Аннотация**

Группа лиц должна узнать секретный код, анализируя доступную всем таблицу. Каждый участник знает свою строчку в таблице и одно слово из кода. Участник может сообщить всем другим только одно из двух сообщений — знает он код или не знает. В статье описан алгоритм, позволяющий строить таблицы, по которой за несколько ходов обмена сообщениями все участники узнают код.

**Ключевые слова:** *криптографический алгоритм с открытым ключом, криптосистема RSA, аутенфикация, одновременная подпись контракта.*

**Цитирование:** Коточигов А. М., Левицкий Д. В., Носова О. А. Код общего доступа // Компьютерные инструменты в образовании. 2017. № 5. С. 5–11.

## 1. ВВЕДЕНИЕ

Возможности легко передавать гигантские объемы информации породили проблемы, связанные с необходимостью защищать информацию от тех, кому она не предназначена. Эти вопросы активно исследуются как в теоретическом, так и в прикладном плане [1–5]. Обсуждаемая здесь задача возникла из обнаруженной в интернете шуточной задачи. Двое молодых людей $D$ и $M$ хотят узнать дату рождения девушки. Девушка, желая проверить их интеллект, называет одному дату, а другому — месяц своего рождения, кроме того, она сообщает обоим несколько вариантов ответа (ответ — это пара чисел: дата и месяц). Отгадывающий может говорить только, знает ли он правильный ответ или нет. Содержание разговора известно: первый говорит «нет», второй говорит «да», после этого первый тоже говорит «да». Посмотрим, как происходит отгадывание на конкретном примере. Описание базы (пар чисел, названных девушкой) приведено в табл. 1.

**Таблица 1.** Исходный вид базы

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $D$ | 7 | 6 | 5 | 3 | 2 | 1 | 3 | 2 | 1 |
| $M$ | 3 | 2 | 1 | 4 | 4 | 4 | 3 | 2 | 1 |

Девушка родилась 1 января, $D$ знает дату «1», $M$ — номер месяца «1». У $M$ все числа в строчке повторяются — он не может узнать дату, и его высказывание не даст возможности сократить базу. Он молчит. $D$ видит, что числа 7, 6, 5 не повторяются в его строке и среди них нет известной ему даты. Его ответ «не знаю» повлияет на структуру базы —

столбцы, содержащие числа 7, 6, 5, можно удалить. База приобретает следующий вид (см. табл. 2).

**Таблица 2.** Вид базы после первого шага

| $D$ | 3 | 2 | 1 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| $M$ | 4 | 4 | 4 | 3 | 2 | 1 |

Очередь говорить $M$. Поскольку 1 встречается в его строке только один раз, то он понимает, что ответ «1,1». Он говорит «знаю». Тогда $D$ видит, что пары содержащие 4, не могут содержать правильного ответа и может еще раз сократить базу (см. табл. 3).

**Таблица 3.** Вид базы после второго шага

| $D$ | 3 | 2 | 1 |
|---|---|---|---|
| $M$ | 3 | 2 | 1 |

Теперь и он видит, что дата рождения «1,1».

## 2. ПОСТАНОВКА ЗАДАЧИ

Эффектная формулировка привлекла внимание, а анализ решения навел на мысль об описании алгоритма решения задачи совместного доступа, когда несколько участников должны узнать заданный код, по доступной им базе наборов, среди которых содержится код.

Базой будем называть таблицу с числом строк равным числу участников (длине кода). Каждый участник знает номер свой строки и число, стоящее на пересечении его строки и кодового столбца. Код записан в одном из столбцов таблицы.

Правила угадывания те же: каждый из участников по очереди говорит, знает он код или нет. Эти переговоры в дальнейшем будут называться протоколом. Отметим, что главную трудность здесь представляет составление правильной базы, гарантирующей возможность реализации алгоритма решения.

## 3. ПАРАМЕТРЫ ЗАДАЧИ, НУЖНЫЕ ДЛЯ ФОРМИРОВАНИЯ БАЗЫ

Проанализируем еще раз решение задачи, абстрагируясь от конкретных цифр. Для этого будет использована терминология, позволяющая выделять некоторые элементы базы. Поскольку перестановка столбцов базы не меняет задачи, то, выделяя те или иные объекты, будем переставлять столбцы базы в удобном порядке.

1) $m$ — моноинтервал, множество всех чисел, встречающихся в данной строке один раз.
2) $bm$ — блок моноинтервала, множество всех столбцов, пересекающих моноинтервал.
3) $em$ — пустой моноинтервал, моноинтервал, не содержащий чисел, входящих в код.
4) $km$ — кодовый моноинтервал, моноинтервал, содержащий одно из чисел кода.
5) $dem$ или $dkm$ — дублирующий интервал, интервал содержащий те же числа, что $em$ или $km$, которые становятся моноинтервалами после удаления дублирующих интервалов.
6) $bal$ — балластный интервал, все числа в этом интервале повторяются хотя бы два раза.

Подчеркнем, что введенные обозначения являются динамическими, то есть после каждого хода названия интервалов могут меняться. База будет построена так, что в каждый момент один (активный) участник видит в своей строке моноинтервал, строки остальных участников — балластные интервалы.

Информация, поступившая от активного участника, позволяет сокращать размер базы. Если участник говорит, что знает код, то все понимают, что его моноинтервал кодовый, и все столбцы, не пересекающие моноинтервал, можно удалить. Если участник говорит, что не знает кода, то его моноинтервал пустой, и всем ясно, что соответствующие столбцы можно удалить из базы. Таким образом, база сокращается на каждом ходе и процедура отгадывания должна завершиться. Главным фактором в этой конструкции является то обстоятельство, что после каждого сокращения базы у одного из участников должен появляться моноинтервал, то есть блок моноинтервала активного участника должен содержать дублирующий интервал участника, активного в следующем ходе. Естественно сокращать базу не только по столбцам, но и по строкам, точнее, переводить строки участников, узнавших код, в пассивную часть базы. Участник, узнавший код, больше не участвует в процессе переговоров. Из этих замечаний следует, в частности, что число «1» в протоколе равно числу участников. Еще одно наблюдение, существенное для построения базы, состоит в том, что, когда предпоследний участник узнает код, последний участник должен увидеть кодовый моноинтервал, иначе он его уже не узнает, то есть протокол должен заканчиваться двумя «1». Других ограничений на протокол нет. Далее будет показано, как по протоколу составить базу, позволяющую всем участникам узнать код, если вначале каждый знал номер своей строки в базе и соответствующий элемент кода.

Протокол — это список $pr$ длины $S$ ($S$ — число ходов), а $pr(st)$ — высказывание участника, активного на шаге $st$: $pr(st) = 0$ — участник не знает кода, $pr(st) = 1$ — участник узнал код. Единственное ограничение на протокол: $pr(S) = pr(S-1) = 1$. Число участников (длина кода) $N = \sum_{st=1}^{S} pr(st)$. Список единиц в протоколе:

$$(st_1, st_2, \ldots, st_N),\ pr(st_k) = 1,\ st_k < st_{k+1}.$$

Нумерация участников, порождаемая протоколом, возникает из списка участников, активных в данном шаге $np(st)$, $1 \le st \le S$, и определяется следующими правилами:

$np(st) \ne np(st+1)$ — участник не может быть активным два раза подряд;

$np(st_k) = k$ — эти равенства задают нумерацию участников (первый номер имеет участник, первым узнающий код, последний номер $N$ имеет участник, узнающий код последним);

если $st_k < st < st_{k+1}$, то $np(st)$ — любое число, большее $k$ (любой из участников, не узнавших код к этому шагу), единственное ограничение: $np(st) \ne np(st+1)$.

## 4. ФОРМИРОВАНИЕ БАЗЫ

Формирование базы происходит пошагово. Обозначим $n$-ю строку базы через $base(n)$ ($n = 1, 2, \ldots, N$). Изначально все строки пустые. Поскольку построение базы идет пошагово (развивается во времени), удобно ввести обозначение $line(st)$ — вид строки базы с номером $np(st)$ на шаге $st$ (то есть строки участника, активного на этом шаге).

Структура всех строк одинакова: сначала кодовый моноинтервал, затем балластный интервал, затем интервал, дублирующий кодовый, а далее чередование балластных интервалов, пустых моноинтервалов и дублирующих интервалов. Отметим, что на любом

шаге формирования строка $line(st)$ обязательно завершается дублирующим интервалом. Исключение составляет только последний этап формирования, который будет описан отдельно. Задача формирования базы сводится к правильному согласованию длин этих интервалов (чтобы после каждого шага открывался один моноинтервал). Код будем считать, состоящим из 1. Каждую строку заполняем независимо от остальных. Открывающий строку кодовый моноинтервал имеет вид $(1,2,\ldots,k)$, затем балластный интервал $(k+1,k+1,\ldots,k+m,k+m)$ и вслед за ним интервал, дублирующий кодовый $(1,2,\ldots,k)$. Параметры $k$ и $m$ свободны только на первом шаге построения, а дальше определяются условиями согласования длин интервалов. Число $k$ удобно выбрать четным (тогда, как будет видно из анализа алгоритма, все интервалы будут иметь четную длину, а это удобно при заполнении балластных интервалов).

Алгоритм устроен так, что строки заполняются противоходом, то есть от $line(S)$ до $line(1)$ при этом, если $np(st^{(1)}) = np(st^{(2)})$ (на шаге $st^{(1)}$ и на шаге $st^{(2)}$ активен один и тот же участник) и $st^{(1)} < st^{(2)}$, то список $line(st^{(1)})$ является расширением списка $line(st^{(2)})$.

База заполняется числами по жестким правилам исключительно ради того, чтобы иметь возможность контролировать правильность конструкции. После того как база построена, можно (отдельно в каждой строке) перевести (взаимно однозначно) все встречающиеся там числа в любые символы.

Чтобы проводить наращивание, создается список $inf$, в котором для каждой строки базы $base(n)$ хранятся два числа — ее текущее состояние:

$pos$ — номер последней заполненной позиции,

$max$ — наибольшее число, встречающееся в этой строке.

Первой формируется строка участника $N$ на последнем шаге $line(S)$. Правило ее формирования описано выше. Кодовый интервал $(1,2,\ldots,k)$, балластный интервал $(k+1,k+1,\ldots,k+m,k+m)$ и вслед за ним интервал, дублирующий кодовый, $(1,2,\ldots,k)$. Обозначим через $pos_1$ — начальную и $pos_2$ — конечную позицию дублирующего интервала. Готовая строка записывается в строчку базы $base(N)$. В список $inf$ запишем $inf(N) = (2k+2m, k+m)$. Для того чтобы участник $N$ мог узнать код, надо поставить в строке участника $N-1$, делающего согласно протоколу $S-1$-й шаг (то есть в список $line(S-1)$), балластный интервал на позиции с $pos_1$ по $pos_2$. В описание протокола включено обязательное требование $pr(S-1) = 1$, то есть участник $N-1$ должен иметь кодовый моноинтервал на позициях с 1-й по $pos_1 - 1$, далее, как отмечено выше, балластный интервал и интервал, дублирующий кодовый. Готовая строка записывается в строчку базы $base(N-1)$. В список $inf$ запишем $pos$ — длина списка $line(S-1)$ и $max$ — наибольшее число в этом списке, $inf(N-1) = (pos, max)$.

Предположим, что проведено формирование $line(st)$, $st > 2$, и покажем, как провести формирование $line(st-1)$. Для этого надо сохранить числа $pos_1$ и $pos_2$ — границы дублирующего интервала, завершающего строку $line(st)$. Далее конструкция разветвляется.

Если $pr(st-1) = 1$, то есть на этом шаге участник с номером $np(st-1)$ узнает код, то его строка в базе пуста, как и список $line(st-1)$. Записываем в $line(st-1)$ кодовый моноинтервал (с первой позиции по $pos_1 - 1$), далее балластный интервал на позиции с $pos_1$ по $pos_2$ и затем интервал, дублирующий кодовый. Готовая строка записывается в строку базы $base(np(st-1))$. В список информации о строке базы $inf$ запишем $inf(np(st-1)) = (pos, max)$.

Если $pr(st-1) = 0$, то есть на этом шаге участник с номером $np(st-1)$ не узнает кода, то в список $line(st-1)$ заносится строка базы с номером $np(st-1)$. Далее надо продол-

жить $line(st-1)$. Для продолжения списка из списка $inf(np(st-1))$ надо извлечь информацию о последней заполненной позиции и наибольшем числе $pos,\ max$. Из анализа построения легко увидеть, что всегда справедливо неравенство $pos < pos_1$. С учетом этого замечания можно сделать первый шаг продолжения: поставить на позиции с $pos+1$ по $pos_1-1$ балластный интервал (если $pos = pos_1-1$, то этот шаг пропускаем), начинающийся с $max+1$, далее на позиции с $pos_1$ по $pos_2$ — пустой моноинтервал и затем дублирующий его интервал. Готовая строка записывается в строчку базы $base(np(st-1))$. В список информации о строке базы $inf$ запишем $inf(np(st-1)) = (pos, max)$.

Осталось рассмотреть формирование базы на заключительном этапе $st = 1$. Исключим тривиальный случай $pr(1) = 1$, когда участник узнает код на первом шаге. На предшествующем шаге был сформирован список $line(2)$ ($np(2)$ строка базы), завершающийся дублирующим интервалом на позициях с $pos_1$ по $pos_2$. В список $line(1)$ заносится строка базы с номером $np(1)$). Для продолжения списка $line(1)$ (строки базы с номером $np(1)$) восстанавливаем информацию о строке $inf(np(1)) = (pos, max)$. Если $pos < pos_1 - 1$, то на позиции с $pos+1$ по $pos_1-1$ записываем балластный интервал, начинающийся с числа $max+1$, а далее на позициях с $pos_1$ по $pos_2$ ставим пустой моноинтервал. Это окончательный вид строки базы с номером $np(1)$. Строка базы с номером $np(2)$ имеет ту же длину, ее построение завершено. Остальные строки базы имеют меньшую длину, их надо выровнять, поставив в конце балластные интервалы. База построена.

## 5. ПРИМЕР

Рассмотрим пример, в котором 4 участника за 9 шагов узнают код.

**Таблица 4.** Протокол и нумерация участников

| шаг | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| протокол | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| номер | 1 | 4 | 1 | 2 | 3 | 2 | 4 | 3 | 4 |

В последней строке стоит номер участника, делающего ход. Номера участников определяются тем, что $st_1 = 3$, $st_2 = 6$, $st_3 = 8$, $st_4 = 9$. Номера строк в базе те же, что и номера участников.

Приведенная ниже таблица 5 показывает ход формирования базы. $ln(3,8)$ — обозначение для 3-й строки базы на 8-м шаге. Здесь указано число элементов, составляющих различные интервалы базы. Какие именно, помечено в верхней строчке. Использованные обозначения:

$k$ — кодовый моноинтервал, $dk$ — интервал, дублирующий кодовый,

$e$ — пустой моноинтервал, $de$ — интервал, дублирующий пустой,

$ba$ — балластный интервал.

Кроме того, в строчках содержится вспомогательная информация:

$ps$ — число занятых позиций в строке (длина строки),

$mx$ — наибольшее число в строке,

$ps_1$ — позиция начала дублирующего интервала.

Пробел после второго столбца таблицы означает, что интервал длинный. Из таблицы хорошо видно, как очередной ход открывает моноинтервал для следующего хода. В базе все строки, кроме первой и четвертой, должны быть дополнены до длины 112; как было отмечено, способ заполнения может быть случайным.

**Таблица 5.** Формирование строк базы

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $k$ | $ba$ | $dk$ | | $ps$ | $mx$ | $ps_1$ | | | | | | |
| $ln(4,9)$ | 2 | 2 | 2 | | 6 | 3 | 4 | | | | | | |
| | $k$ | | $ba$ | $dk$ | | $ps$ | $mx$ | $ps_1$ | | | | | |
| $ln(3,8)$ | 4 | | 2 | 4 | | 14 | 7 | 10 | | | | | |
| | $ol$ | | | $e$ | $de$ | | $ps$ | $mx$ | $ps_1$ | | | | |
| $ln(4,7)$ | 6 | | | 4 | 4 | | 14 | 7 | 10 | | | | |
| | $k$ | | | | $ba$ | $dk$ | | $ps$ | $mx$ | $ps_1$ | | | |
| $ln(2,6)$ | 10 | | | | 4 | 10 | | 24 | 12 | 14 | | | |
| | $ol$ | | | | $ba$ | $e$ | $de$ | | $ps$ | $mx$ | $ps_1$ | | |
| $ln(3,5)$ | 10 | | | | 4 | 10 | 10 | | 34 | 17 | 24 | | |
| | $ol$ | | | | | | $e$ | $de$ | | $ps$ | $mx$ | $ps_1$ | |
| $ln(2,4)$ | 24 | | | | | | 10 | 10 | | 44 | 22 | 34 | |
| | $k$ | | | | | | | $ba$ | $dk$ | | $ps$ | $mx$ | $ps_1$ |
| $ln(1,3)$ | 34 | | | | | | | 10 | 34 | | 78 | 39 | 44 |
| | $ol$ | | | | | | | $ba$ | $e$ | $de$ | | $ps$ | $mx$ | $ps_1$ |
| $ln(4,2)$ | 14 | | | | | | | 30 | 34 | 34 | | 112 | 56 | 78 |
| | $ol$ | | | | | | | | | $e$ | | $ps$ | $mx$ | |
| $ln(1,1)$ | 78 | | | | | | | | | 34 | | 112 | 73 | |

Таблица 6 позволяет почувствовать, как быстро растут длины строк по мере ее заполнения.

**Таблица 6.** Структура построенной базы

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| участник 1 | $k$ | $k$ | $k$ | $k$ | $k$ | $k$ | $k$ | $ba$ | $dk$ | $e$ |
| участник 2 | $k$ | $k$ | $k$ | $k$ | $ba$ | $dk$ | $e$ | $de$ | $ba$ | $ba$ |
| участник 3 | $k$ | $k$ | $ba$ | $dk$ | $ba$ | $e$ | $de$ | $ba$ | $ba$ | $ba$ |
| участник 4 | $k$ | $ba$ | $ba$ | $e$ | $de$ | $ba$ | $ba$ | $ba$ | $e$ | $de$ |

## 6. ЗАКЛЮЧЕНИЕ

Предложенный здесь алгоритм не может быть использован для передачи секретного кода. База слишком регулярна. Если посторонний человек понимает, что код может содержаться в моноинтервалах, оставшихся после удаления всех блоков, являющихся «лишними», то задача сведется к поиску кода в блоке кодового моноинтервала участника, делающего последний ход. Однако процедура вскрытия кода сильно усложнится, если на каждом шаге каждый участник видит моноинтервал в своей строке. В отсутствие информации о наличии кодового интервала это значительно увеличит число переборов.

## Список литературы


1. *Венбо Мао.* Современная криптография. Теория и практика. М.: Вильямс, 2005.
2. *Menezes A. J., Van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. CRC Press, 1996.
3. *Щербаков А. Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный Мир, 2009.
4. *Пременко Э. А.* Алгебраически основа криптографии. М.: Либерком, 2014.
5. *Гуров С. И.* Булевы алгебры, упорядоченные множества, решетки. М.: Либерком, 2013.


*Поступила в редакцию 11.09.2017, окончательный вариант — 12.10.2017.*

Computer tools in education, 2017
№ 5: 5–11
http://ipo.spb.ru/journal

# SHARING CODE

Kotochigov A. M.[1], Levicki D. V.[1], Nosova O. A.[1]

[1]Saint-Petersburg Electrotechnical University, Saint Petersburg, Russia

**Abstract**

A group of people must find out a secret code by analyzing a table available to all. Each participant knows his line in the table and one word from the code. A participant is allowed to announce to all others only one of two messages — s/he knows the code or does not know it. The article describes an algorithm allowing the construction of the table, with the help of which, after a few exchanges of messages, all participants will recognize the code.

**Keywords:** *cryptographic algorithm with open key, crypto-system RSA, authentication, simultaneous subscription of contract.*

**Citation:** A. M. Kotochigov, D. V. Levicki, and O. A. Nosova, "Sharing code," *Computer tools in education*, no. 5, pp. 5–11, 2017 (in Russian).

*Received 11.09.2017, the final version — 12.10.2017.*

**Aleksandr M. Kotochigov, Professor, doctor of science, Head of Department of Higher Mathematics-2; 197022 Saint-Petersburg, Professora Popova str., 5, Department of Higher Mathematics-2, amkotochigov@gmail.com**
**Daniil V. Levicki, Student of Faculty of Computer Science and Technology, happydvilopro@gmail.com**
**Olga A. Nosova, Student of Faculty of Computer Science and Technology, nosova-olenka@mail.ru**

**Коточигов Александр Михайлович, доктор физико-математических наук, профессор, заведующий кафедрой ВМ-2; 197022 Санкт-Петербург, ул. Профессора Попова, д. 5, кафедра ВМ-2, amkotochigov@gmail.com**

**Левицкий Даниил Владимирович, студент Факультета Компьютерных технологий и информатики, happydvilopro@gmail.com**

**Носова Ольга Андреевна, студентка Факультета Компьютерных технологий и информатики, nosova-olenka@mail.ru**