ствует *конечное множество* сетей Штейнера. Для нахождения кратчайшего пути среди множества точек нужно найти все сети Штейнера, а потом выбрать самую короткую. Однако точное решение задачи требует рассмотрения огромного количества вариантов, так что даже лучшие из существующих алгоритмов, выполняющиеся на самых быстродействующих компьютерах, не в состоянии дать решение для большого множества заданных точек за реально приемлемое время. Более того, задача Штейнера принадлежит к классу задач, для которых, по мнению многих современных исследователей, эффективные алгоритмы так никогда и не будут найдены. В силу востребованности задачи для практических приложений, актуальным является построение новых алгоритмов, в том числе дающих приближенное решение задачи Штейнера [2].

ЛИТЕРАТУРА

1. Алгоритмы о выборе дороги и сетях. Сети Штейнера. Лекция Владимира Протасова в Яндексе [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/yandex/blog/215931/. Дата доступа: 04.04.2018

2. Алгоритм Штейнера (Поиск кратчайших сетей) [Электронный ресурс]. – Режим доступа: http://lmatrix.ru/news/practice/algoritm-shtejjnera-poisk-kratchajjshikh-setejj_137.html Дата доступа: 08.04.2018

УДК 511.34

Студ. К.С. Марчук
Науч. рук. доц. И.К. Асмыкович
(кафедра высшей математики, БГТУ)

ПРИМЕНЕНИЕ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ В АЛГОРИТМЕ RSA

Много великих открытий и изобретений было сделано в Китае: печатные книги, фарфор, шёлк, зеркала, зонтики и бумажные змеи – это лишь малая часть. Но сегодня мы поговорим о "китайской теореме об остатках"[1].

Если натуральные числа $a_1, a_2, \dots, a_n$ попарно взаимно просты, то для любых целых $r_1, r_2, \dots, r_n$ таких, что $0 \leq r_i < a_n$при всех $i \in \{1,2,\dots,n\}$, найдётся число N, которое при делении на a_i даёт остаток r_i при всех $i \in \{1,2,\dots,n\}$. Рассмотрим пример использования данной теоремы.

Предположим 797 солдат попросили построиться по 5, 17, 12 человек. Далее мы считаем оставшихся солдат в неполном ряду – 2, 15, 5.

$$\begin{cases} x = 2(mod\ 5) \\ x = 15(mod\ 17) \\ x = 5(mod\ 12) \end{cases}$$

Далее по "остаткам" и делителям восстанавливаем число воинов. Находим произведение всех делителей $M_0 = 5 \cdot 17 \cdot 12 = 1020$, далее произведение по паре делителей $M_1 = 17 \cdot 12 = 204$, $M_2 = 5 \cdot 12 = 60$, $M_3 = 5 \cdot 17 = 85$. Теперь составляем систему уравнений вида $M_i y_i = a_i(mod\ m_i)$:

$$\begin{cases} 204y_1 = 2(mod\ 5) \\ 60y_2 = 15(mod\ 17) \\ 85y_3 = 5(mod\ 12) \end{cases}$$

$$204y_1 = 2(mod\ 5) = 200y_1 + 4y_1 = 2(mod\ 5) = 0 + 4y_1 = 2(mod\ 5).$$

Здесь мы учли, что $200y_1(mod\ 5) = 0$, т.к. 200 делится на 5 без остатка. Аналогично мы делаем с двумя остальными уравнениями. Теперь решаем систему, находя корни каждого уравнения подбором

$$\begin{cases} y_1 = 3 \\ y_2 = 12 \\ y_3 = 5 \end{cases}$$

$$x = M_1y_1 + M_2y_2 + M_3y_3\ (modM_0) = 1817(mod\ 1020) = 797(mod\ 1020)$$

Рассмотрим использование данной теоремы в алгоритме шифрования RSA.

Шифрование – обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней, способ обезопасить передаваемую информацию. Используя разные алгоритмы шифровки,можно, например, вместо сообщения "Привет Алиса!" получить комбинацию из нескольких символов, сложную для расшифровки для тех, кто не знает используемого нами алгоритма. RSA – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших чисел (разложении чисел на множители). Нам стоит разобрать данный алгоритм.

Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующим свойством:

Если известно x{\displaystyle x}, то {\displaystyle f(x)}f(x) вычислить относительно просто.

Если известно {\displaystyle y=f(x)}f(x), то для вычисления {\displaystyle x}x нет простого (эффективного) пути.

Разберём пример алгоритма RSA:

Генерация ключей

Выберем два простых числа $p = 53$ и $q = 59$

Вычислим произведение $n = p \cdot q = 53 \cdot 59 = 3127$

Вычислим функцию Эйлера $f(n) = (p-1)(q-1) = 3016$

Выберем открытую экспоненту $e = 3$

Вычислим секретную экспоненту

$d = e^{-1} mod f(n)$ или же $d = (k \cdot \varphi(n) - 1)/e$,$d = (2 \cdot 3016 - 1)/3 = 2011$

Опубликуем открытый ключ $\{e, n\} = \{3, 3127\}$.

Опубликуем закрытый ключ $\{d, n\} = \{2011, 3127\}$.

Шифрование

Выбираем текст для шифрования $m = 89 (= hi)$ слово преобразовано нумерацией букв в алфавите;

Вычисляем шифртекст

$$c = E(m) = m^e mod n = 89^3 mod 3127 = 1394$$

Расшифрование

Вычисляем исходное сообщение:

$$m = D(c) = c^d mod n = 1394^{2011} mod\ 3127 = 89$$

Как видно из примера, процесс расшифрования является очень долгим, но в этом нам и поможет китайская теорема об остатках. Показатель вычисляемой степени – довольно большое число. Поэтому требуется алгоритм, который бы сокращал количество выполняемых операций. Так как числа p и q в разложении N = p*q известны владельцу закрытого ключа. Это можно вычислить:

$$m_p = C^d\ mod\ p = C^{d\ mod\ p-1}\ mod\ p$$

$$m_q = C^d\ mod\ q = C^{d\ mod\ q-1}\ mod\ q$$

Поскольку наши числа p и q – числа порядка 2^{512}, на эти действия потребуется два возведения числа в 512-битовую степень числа. Это гораздо быстрее (для 1024 бит – в 3 раза), чем одно возведение в 1024-битовую степень по модулю 1024-битового числа. Преобразования больших степеней можно проводить по аналогии с примером из [2]. Далее осталось восстановить m по m_p и m_q, что можно сделать с помощью китайской теоремы об остатках.

$$m_p = 1394^{2011} mod\ 53 = 1394^{2011\ mod\ 52} mod\ 53 = 1394^{35} mod\ 53 = 36$$

$$m_q = 1394^{2011} mod\ 59 = 1394^{2011\ mod\ 58} mod\ 59 = 1394^{39} mod\ 59 = 30$$

$$\begin{cases} x = 30 (mod\ 59) \\ x = 36 (mod\ 53) \end{cases}$$

$$M_0 = 59 \cdot 53 = 3127,$$

$$M_1 = 53,\ M_2 = 59.$$

$$\begin{cases} 53y_1 = 30 (mod\ 59) \\ 59y_2 = 36 (mod\ 53) \end{cases}$$

$$59y_2 = 36 (mod\ 53) = 6y_2 = 36 (mod\ 53)$$

$$\begin{cases} y_1 = 54 \\ y_2 = 6 \end{cases} x = M_1 y_1 + M_2 y_2\ (mod M_0) = 3216 (mod\ 3127) = 89 (mod\ 3127)$$

Вот мы и получили наше исходное сообщение, используя при расшифровке китайскую теорему об остатках.

ЛИТЕРАТУРА

1. Википедия, свободная энциклопедия (https://www.wikipedia.org)

2. Чистяков Н.В. Аддитивные цепочки // 68-я научно-техническая конференция учащихся, студентов и магистрантов, 17-22 апреля, Минск: сборник научных работ : в 4 ч. Ч. 4 / - Минск: БГТУ, 2017. с. 272-275

УДК 004.056.55 - 003.26

Студ. Е.М.Лашкевич, Д.А.Ковалевич
Науч. рук. доц. И.К.Асмыкович
(кафедра высшей математики, БГТУ)

ВЕКТОРНАЯ СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА

Векторная схема разделения секрета или же схема Блэкли (англ. Blakley's scheme) — схема разделения секрета между сторонами, основанная на использовании точек многомерного пространства. Предложена Джорджем Блэкли в 1979 году. Схема Блэкли позволяет создать (t, n)-пороговое разделение секрета для любых t, n.

Идея

Разделяемым секретом в схеме Блэкли является одна из координат точки в m-мерном пространстве. Долями секрета, раздаваемые сторонам, являются уравнения (m − 1)-мерных гиперплоскостей. Для восстановления точки необходимо знать m уравнений гиперплоскостей. Менее, чем m сторон не смогут восстановить секрет, так как