ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2015

түсінігі берілген. Ол халықаралық тәжірибеде «сертификат» немесе «ашық кілттің сертификаты» ретінде қолданылады.

Қолтаңба Қазақстан Республикасының барлық азаматтары мен азаматшалары үшін қолжетімді.

E-gov электронды үкіметі порталынан алынған сертификатты ашу үшін RSA сертификаты ұсынылады. Халыққа не үшін RSA сертификаты ұсынылады?

- ЭСҚ-ны 2012 жылдың 30 сәуіріне дейін алған ескі қолданушылар үшін: GOST сертификаты сұранысқа қол қою үшін, ал RSA порталдағы аутентификация үшін арналған.
- ЭСҚ-ны 2012 жылдың 1 мамырынан алған жаңа қолданушылар (жеке тұлғалар) үшін: RSA сертификаты сұранысқа қол қою үшін, ал AUTH_RSA порталдағы аутентификация үшін арналған.
- Жаңа қолданушылар үшін (заңды тұлғалар): GOST сертификаты сұранысқа қол қою үшін, ал RSA порталдағы аутентификация үшін арналған.

Еліміз қазіргі күні ақпараттық технологиялар заманы көшінің соңында қалып отырған жоқ. Біріккен Ұлттар Ұйымының электронды үкіметті дамыту жөніндегі рейтингінде еліміз былтырғы жылы 193 мемлекеттің арасынан 28-ші сатыға жайғасты. Бұның алдындағы жылы ел аталған рейтинг бойынша 38-ші орында тұрған еді.

Қазіргі таңда Қазақстан Республикасында 2,4 млн ЭСҚ шығарылған, соның 500000-ы азаматтардың жеке куәліктерін алмастыра алатын ID картада жазылған. Әрі қарай ЭСҚ-ны мобильді құрылғылардың сим картасына жазу жоспарға алынған. ЭСҚ берілуінің мобильді платформасы Қазақстанда 2014-2016 жж құрылады. Мобильді үкімет – Қазақстан Республикасының электронды үкіметінің дамуының жаңа кезеңі.

Қазір еліміздегі 570 мемлекеттік қызмет электрондық түрде көрсетіледі, барлық лицензиялар электрондық форматта беріледі.

Қорытындылай келе, салыстырылған екі алгоритмнің сандық қолтаңбаларының ең сенімдісі ретінде Эль-Гамальді айтуға болады. Жоғарыда айтып өткендей, Эль – Гамаль алгоритмі де кемшіліксіз емес, RSA алгоритмінің артықшылығы – соның дәлелі. Әлем елдерінің біразы, соның ішінде Қазақстан Республикасы да RSA алгоритмін ЭСҚ ретінде қолданады.

Қолданылған әдебиет

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В Основы криптографии. – М.: Гелиос АРВ, 2002, 480 с.

2. Коутинхо С. Введение в теорию чисел алгоритм RSA. – М.: Постмаркет, 2001, 328с.

3. Фороузан Б.А. Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций.

4. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone 11.5.2 The ElGamal signature scheme // Handbook of applied cryptography.

УДК 621.391

ИСПОЛЬЗОВАНИЕ АЛГОРИТМ ПРИМА ДЛЯ РАСЧЕТА СЕТИ ДОСТУПА МИНИМАЛЬНОЙ СТОИМОСТИ

Беков Нурсултан Кабжанулы
Nursultan_bekov@mail.ru
Магистрант группы МРЭТ-22 ЕНУ им.Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Ш.Ж.Сеилов

Введение

При проектировании сетей доступа с использованиеFTTx технологий для определения остова структуры сети решается задача синтеза сети минимальной стоимости. Существуют различные алгоритмы решения данной задачи [1]. В данной статье показана возможность использования алгоритма Прима для расчета сети доступа минимальной стоимости, при условии, что стоимость линий связи является линейной и зависит только от ее длины.

Постановка и алгоритм решения задачи

Задача синтеза сети минимальной стоимости заключается в том, что необходимо соединить некоторое множество абонентов так, чтобы каждая пара получилась связанной напрямую либо через другие точки, а общая весовая характеристика оказалась минимальной.

Например, имеется ряд точек, в которых могут быть расположены пункты телекоммуникационной сети. Известны расстояния между парами точек и стоимость организации одного километра линии связи. Необходимо определить совокупность линий связи, обеспечивающих связность всех пунктов сети и ее минимальную стоимость.

Из теории графов и сетей известно, что решением поставленной задачи является сеть с топологией типа "дерево".

Связный граф (связывающая сеть) называется деревом, если в нем отсутствуют циклы.Говорят, что граф содержит циклы, если в нем можно отыскать замкнутые контуры. Отсутствие циклов определяет особенность графа типа дерево, которая состоит в том, что между любой парой его вершин существует лишь один единственный связывающий их путь, т.е. параметр связности h=1. Количество ребер в дереве всегда на единицу меньше числа его вершин. Дерево, в которое включены все вершины, называется покрывающим.

Математически задача синтеза сети минимальной стоимости формулируется следующим образом.

Пусть задан неориентированный граф G(N,V), где множество вершин N соответствует множеству пунктов сети, общее число которых равно n, а множество ребер V – расстояниям {lij} между парами пунктов. Известна стоимость Cij организации 1 километра линии связи между пунктами i и j. Необходимо найти некоторое покрывающее дерево G'(N,V'), для которого достигается минимум целевой функции:

$$Z = \sum_{i=1}^{n} \sum_{j=1}^{n} C_{ij} l_{ij} \rightarrow \min$$

Для решения поставленной задачи существует ряд эффективных алгоритмов. Приведем один из них, который известен как алгоритм Прима и носящий имя автора. Алгоритм реализуется путем присвоения пометок вершинам, которые вводятся в искомый граф G'(N,V'), и последовательного введения в него, наиболее коротких ребер, общее количество которых не должно превышать (n-1) и обеспечивать связность между всеми n вершинами покрывающего дерева.

Пошаговая форма алгоритма Прима имеет следующий вид:

1) Сначала берётся произвольная вершина и находится ребро, инцидентное данной вершине и обладающее наименьшей стоимостью. Найденное ребро и соединяемые им две вершины образуют дерево.

2) Затем, рассматриваются рёбра графа, ещё не принадлежащие дереву и смежные с последним добавленным в дерево ребром; из этих рёбер выбирается ребро наименьшей стоимости. Выбираемое на каждом шаге ребро присоединяется к дереву.

3) Таким образом, при выполнении каждого шага алгоритма, высота формируемого дерева увеличивается на 1. Рост дерева происходит до тех пор, пока не будут исчерпаны все вершины и рёбра исходного графа.

Результатом работы алгоритма является остовное дерево минимальной стоимости.

Проиллюстрируем работу алгоритма Прима на примере. Пусть задано семь пунктов сети, расстояния между которыми сведены в матрицу L = ||lij||, а именно:

$$L = \begin{vmatrix} & 0 & & 2 & & & \\ 0 & & & & & & \\ & & & & & & 1 \\ 2 & & & & 0 & 6 & 0 \\ & & & 0 & & 2 & \\ & & & 6 & 2 & & 9 \\ & & 1 & 0 & & 9 & \end{vmatrix}$$

На шаге 1 искомый граф G'(N,V') содержит 6 вершин и не содержит ребер. Выберем вершину 3 и пометим ее как выбранную (рис. 1). На шаге 2 выбираем ребро (l35) как ребро с наименьшим весом, у которого вершина i = 3 принадлежит подмножеству "выбранных" вершин (оно пока содержит всего лишь одну вершину 3), а вершина j = 5 – подмножеству "невыбранных" вершин (сейчас это все остальные вершины). На шаге 3 ребро l35 вводится в искомый граф G', а вершина 5 включается в подмножество "выбранных" вершин (рис. 2.).

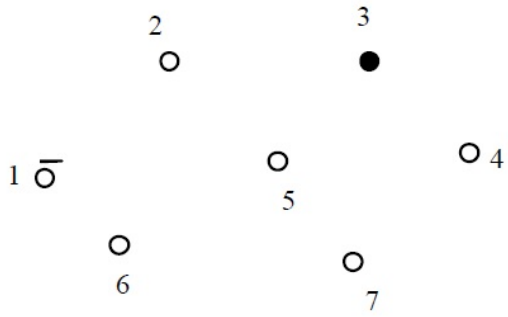

Рисунок 1

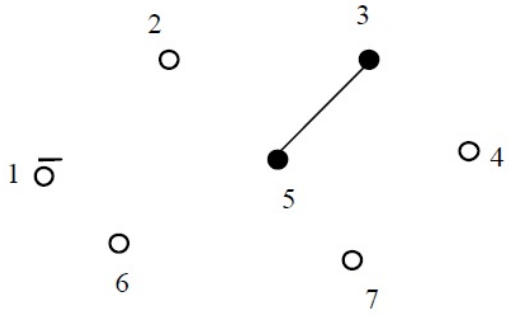

Рисунок 2

Поскольку подмножество "невыбранных" вершин не пустое, повторяем шаг 2. Для этого отыскиваем ребро минимального веса, перебирая сочетания каждой пары "выбранной" и "невыбранной" вершин. Таким оказалось ребро

(рис. 3.). Оно вводится в граф G', а вершина 4 становится "выбранной".

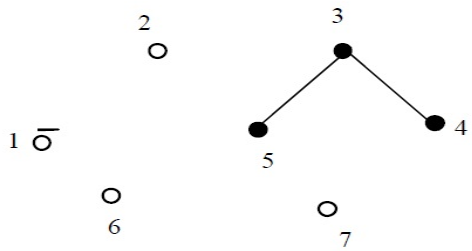

Рисунок 3

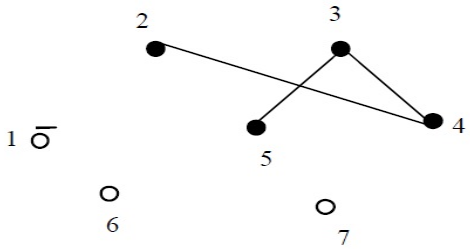

Рисунок 4

После выбираются ребра: l26 (рис. 5.); l31 (рис. 6); l27 (рис. 7). Так как все вершины выбраны, работа алгоритма (т. е. подмножество "невыбранных" вершин – оказалось пустым подмножеством).

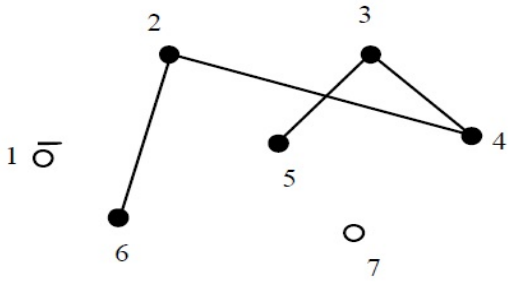

Рисунок 5

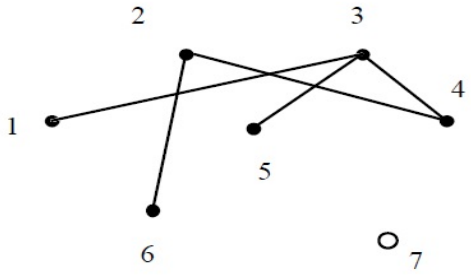

Рисунок 6

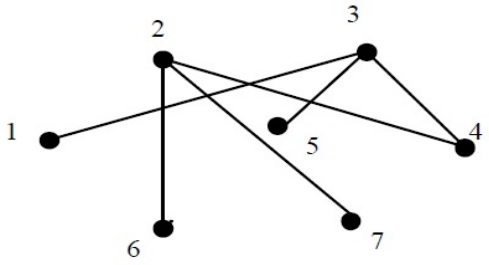

Рисунок 7

Получен искомый граф G'(N, V'), представляющий собой покрывающее дерево, так как он включает все вершины, содержит число ребер на единицу меньшее числа вершин (n = 7, v = 6) и обеспечивает связность каждой пары вершин.

Список использованных источников

1. Рояк М.Э., Теория графов, 1998
2. Носов В.А., Комбинаторика и теория графов, 1999
3. Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн — Алгоритмы: построение и анализ, 2-е издание. Пер. с англ. — М.:Издательский дом "Вильямс", 2010. — с.653 — 656.

УДК 621.39.019.3

АЛГОРИТМ ОЦЕНКИ СТРУКТУРНОЙ ЖИВУЧЕСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Жексенбаев Мейрамбек Еділұлы
zheksenbayev@gmail.com
магистрант кафедры «Радиотехника, электроника и телекоммуникации»
ЕНУ им.Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Сеилов Ш.Ж

Введение

Эффективность функционирования телекоммуникационных сетей (ТКС) зависит от многих свойств ТКС, среди которых одним из важнейших является живучесть сети. Обеспечение живучести ТКС становится все более актуальной проблемой для «новых» операторов связи и интенсивным развитием их телекоммуникаций. В настоящее время