МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра дискретной математики и информационных технологий

ЗАДАЧА О РЮКЗАКЕ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Астраханцева Андрея Сергеевича

Научный руководитель
профессор, д. ф.-м. н. _____ В. А. Молчанов

Заведующий кафедрой
доцент, к. ф.-м. н. _____ Л. Б. Тяпаев

Саратов 2020

ВВЕДЕНИЕ

Задача о рюкзаке является одной из задач с комбинаторной оптимизацией. Суть этой задачи в следующем: есть некий набор из конечного числа предметов, который каждый из них имеет свою собственную массу, объем, и ценность. Нужно включить в ранец максимальное количество предметов так, чтобы общая масса не превосходила максимального значения, который может унести турист, объем предметов не превышал объем ранца и ценность вещей должна быть максимальна ценной.

Очевидно, что написание такой программы для собирания рюкзака, чтобы уместить максимальное количество вещей не рациональна, ведь с этой задачей может справиться каждый человек без всяких расчетов. Имеет смысл рассмотрение этой задачи в других областях.

Задача о рюкзаке и различные её модификации имеют широкий спектр областей, где данная проблема решается и применяется на практике:

— прикладные науки;
— логистика;
— генетика;
— загрузка транспортных средств и многое другое.

Из выше перечисленных направлений пользуется популярностью генетика, где задача используется как поиск биологических моделей механизмов естественного отбора: популяция, отбор, мутация, и скрещивание, и загрузка транспортных средств, которая примменяется для сбора больших грузовых транспортных средств разной категории.

В этой работе, в свою очередь, будет рассматриваться данная задача с криптографической стороны, то есть, шифрование и расшифровка открытого текста с помощью задачи о рюкзаке.

Цель данной работы - изучить ранцевую криптосистему и применить её на практике в качестве программы, которая будет шифровать и расшифровывать сообщения.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Дать определение и рассмотреть методы задачи о рюкзаке;
2. Изучить ранцевую криптосистему Меркла-Хеллмана и рассмотреть её модификации;

3. Изучить фреймворк PyQt5;
4. Создать интерфейс приложения;
5. Написать логику приложения;
6. Протестировать готовое приложение.

КРАТКОЕ СОДЕРЖАНИЕ

Задача о рюкзаке является NP-полной задачей комбинаторной оптимизации. Данное название было получено от конечной цели, заключающейся в том, чтобы поместить в рюкзак самое большее количество нужных вещей, учитывая ограниченную вместимость рюкзака. С задачами о рюкзаке в различных вариациях можно встретиться в прикладной математике, экономике, логистике и криптографии.

Задача, в общем виде, может быть сформулирована следующим образом: из имеющегося множества предметов со свойствами «вес» и «стоимость» необходимо отобрать подмножество предметов с наибольшей стоимостью, учитывая при этом ограниченный суммарный вес.

В первом разделе дипломной работы рассматривается задача о рюкзаке, в котором сначала дается общее понятие этой задачи, а далее в трех подразделах рассматривается уже подробное её описание. В первом подразделе говорится о постановке задачи, где дается определение задачи, её классификации, вариации, краткое описание методов с её сложностями. Во втором подразделе рассматриваются методы задачи о рюкзаке: метод полного перебора, смысл которого рассмотреть все возможные варианты перебора; метод динамического программирования, который на каждом шаге выбирает самый оптимальный вариант и в результате, тем самым, дает наилучший вариант; метод ветвей и границ, который рассматривает только оптимальные варианты, исключая ненужные; жадный алгоритм, который работает по принципу собрать наиболее дорогой рюкзак. В третьем подразделе рассказывается про области применений этой задачи, потому что задача о рюкзаке и различные её модификации имеют широкий спектр областей, где данная проблема решается и применяется на практике, так как в любой сфере, нужно максимизировать результат, затратив, при этом, минимум времени и используемых ресурсов в данной области.

Во втором разделе дипломной работы говориться о используемости задачи о рюкзаке в криптографии, то есть рассказывается о ранцевой криптосистемы.

Ранцевая криптосистема Меркла — Хеллмана основана на задаче об рюкзаке, которая была разработана Ральфом Мерклом и Мартином Хеллманом в 1978 году. Шифрование происходит с помощью открытого ключа. Дан-

ная система является асимметричной, то есть, открытый ключ передается по открытому каналу и в дальнейшем используется для шифрования сообщения, а для расшифровки сообщения используют закрытый ключ, который нужно скрывать. Шифрование происходит с помощью задачи о рюкзаке, которая, в свою очередь, является NP-сложной.

Данный раздел состоит из трех подразделов. В первом подразделе говорится о проблеме ранцевой криптосистемы, а конкретней про атаку Ади Шамира. Для ранцевой криптосистемы Меркла-Хеллмана был разработан полиномиальный алгоритм нахождения секретного ключа. Атака Шамира использует метод решения целочисленного линейного программирования, разобранного Хендриком Ленстра. Во втором подразделе дается общее представление ранцеврой криптосистемы, что из себя представляет генерация ключа, шифрование и расшифровка сообщения. Так как, криптосистема является асимметричной, у нее есть два ключа: открытый, который состоит из последовательности, которая была преобразована из иходной последовательности и закрытый, который, в свою очередь, состоит их двух чисел, которые применялись для генерации открытого ключа, и исходной последовательности. Для шифрования понадобится преобразовать открытый текст в бинарную строку, для того, чтобы разбить данную строку на блоки, равной длине открытого ключа. После данной операции получится последовательность, из которой нужно выбрать только те переменные, которые по порядку соответствуют единице в двоичной записи открытого текста. Расшифровка будет являться действительной, если пара чисел, которые используются для генерации открытого ключа, применяется и для преобразования шифртекста в сумму, которые соответствуют элементам последовательности. Далее при помощи задачи о рюкзаке расшифровывается сообщение, получая в итогеисходный текст.

В третьем пункте, который поделен на два подпункта, говорится о ранцевой криптосистеме Меркла-Хеллмана: ранцевая криптосистема Меркла-Хеллмана с супервозростающей последовательностью и мультипликативная криптосистема Меркла-Хеллмана. В каждом из двух этих подходов описывается алгоритм выполнения ранцевой криптосистемы.

В третьем разделе, описывается практическая часть дипломной работы, а именно реализация приложения на базе мультипликативной ранцевой

криптосистеме Меркла-Хеллмана. Этот раздел состоит из шести пунктов, которые описывают поэтапную реализацию приложения. Реализованное приложение шифрует и расшифровывает открытый текст и генерирует открытый и закрытый ключи В первом пункте идет описание работы приложения. Во втором пункте говорится о инструментах, которые нужны для реализации приложения. В третьем пункте поясняется настройка проекта, а именно, что нужно установить, чтобы приступить к реализации. В четвертом пункте говориться о реализации приложения, а именно создания интерфейса, конвертирование ui файла в python файл и запуск интерфейса непосредственно в проекте. В пятом пункте рассказывается про реализацию методов, с помощью которых будет создана ранцевая криптосистема, взаимодействие кнопок с методами. В заключительном шестом пункте третьей части дипломной работы приведены в пример скриншоты, которые показывают работу приложения.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы была изучена задача о рюкзаке, которая является NP-полной задачей комбинаторной оптимизации. Данное название было получено от конечной цели, заключающейся в том, чтобы поместить в рюкзак самое большее количество нужных вещей, учитывая ограниченную вместимость рюкзака. Также были рассмотре методы решения этой задачи: метод полного перебора; метод динамического программирования; метод ветвей; жадный алгоритм. Данные методы делятся на дискретные и непрерывные. С задачами о рюкзаке в различных вариациях можно встретиться в разных областях прикладных и фундаменталтных наук. Одна из них, является криптография, В которой была определена и рассмотрена ранцевая криптосистема Меркла-Хеллмана.

В практической части было реализовано приложение, которое на базе ранцевой криптосистеме Меркла-Хеллмана шифрует и расшифровывает открытый текст. Для реализации данной задачи был изучен фреймфорк PyQt5, с помощью которого реализовывался интерфейс приложения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Руководство по PyQt5 для начинающих - GUI Python [Электронный ресурс] : [сайт]. - URL: https://python-scripts.com/pyqt5#install (Дата обращения: 17.05.2020). - Загл. с экр. - Яз. рус.

2 Python GUI: создаём простое приложение с PyQt и Qt Designer [Электронный ресурс]: [сайт]. - URL: https://tproger.ru/translations/python-gui-pyqt/ (Дата обращения: 22.05.2020). - Загл. с экр. - Яз. рус.

3 Е. Б. Маховенко // Теоретико-числовые методы в криптографии; "Гелиус АРВ 2006. - 273 с.

4 Задача о рюкзаке - Викиконспекты [Электронный ресурс]: [сайт]. - URL: https://neerc.ifmo.ru/wiki/index.php?title=%D0%97%D0%B0%D0%B4%D0%B0%D1%87%D0%B0_%D0%BE_%D1%80%D1%8E%D0%BA%D0%B7%D0%B0%D0%BA%D0%B5#.D0.9D.D0.B5.D0.BF.D1.80.D0.B5.D1.80.D1.8B.D0.B2.D0.BD.D1.8B.D0.B9_.D1.80.D1.8E.D0.BA.D0.B7.D0.B0.D0.BA (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

5 Что такое Python PyQt: функционал, версии, установка и особенности работы [Электронный ресурс]: [сайт]. - URL: https://webformyself.com/rukovodstvo-po-pyqt-python-gui-designer/ (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

6 НОУ ИНТУИТ | Лекция | Криптосистемы [Электронный ресурс]: [сайт]. - URL: https://www.intuit.ru/studies/professional_retraining/940/courses/408/lecture/9373?page=7 (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

7 Т. Ху // Целочисленное программирование и потоки в сетях; "Мир". 1974.

8 Python и динамическое программирование на примере задачи о рюкзаке [Электронный ресурс]: [сайт]. - URL: https://proglib.io/p/python-i-dinamicheskoe-programmirovanie-na-primere-zadachi-o-ryukzake-2020-02-04 (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

9 проблема ранец - Knapsack problem - qwe.wiki [Электронный ресурс]: [сайт]. - URL: https://ru.qwe.wiki/wiki/Knapsack_problem (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

bibitemIten pyperclip · PyPI [Электронный ресурс]: [сайт]. - URL: https://pypi.org/project/pyperclip/ (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. анг.

10 Д. Златопольский // Программирование: типовые задачи, алгоритмы, методы; БИНОМ. Лаборатория знаний. 2012.

11 Уравнение Беллмана — Википедия [Электронный ресурс]: [сайт]. - URL: https://pypi.org/project/pyperclip/ (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

12 С. Скиена // Алгоритмы. Руководство по разработке;БХВ-петербург. 2011.

13 А.М. Миронов // Криптографические протоколы [Электронный ресурс]. - URL: http://intsys.msu.ru/staff/mironov/kp.pdf (дата обращения: 07.06.2020). - Загл. с экрана. - Яз. рус.

14 Vaudenay, S. Cryptoanalysis of the Chor-Rivest Cryptosystem / S. Vaudenay. Journal of Cryptology, 2001, V.14, Issue 2, pp 87–100.

15 Naccache, D. A New Public-Key Cryptosystem / D. Naccache, J. Stern. [Электронный ресурс]. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-69053-0_3.pdf. (Дата обращения: 09.06.2020). - Загл. с экр. - Яз. рус. - Загл. с экр. - Яз. анг.

16 Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. // Введение в теоретико-числовые методы криптографии.

17 2. Черемушкин, А.В. Криптографические протоколы: основные свойства и уязвимости [Электронный ресурс] / А.В. Черемушкин // Институт криптографии, связи и информатики, г. Москва, Россия. - 36 с.- . -URL: http://elearning.paradygma.ru/docs/books/Черёмушкин%20Криптопротоколы+. (дата обращения: 01.06.2020). - Загл. с экрана. - Яз. рус.

18 Студопедия — Система шифрования методом укладки рюкзака. (Ранцевая система шифрования) [Электронный ресурс]: [сайт]. - URL: https://studopedia.info/2-55447.html (Дата обращения: 09.06.2020). - Загл. с экр. - Яз. рус.

19 pyperclip · PyPI [Электронный ресурс]: [сайт]. - URL: https://math.wikia.org/ru/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B5_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5 (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.

20 pyperclip · PyPI [Электронный ресурс]: [сайт]. - URL: https://pypi.org/project/pyperclip/ (Дата обращения: 26.05.2020). - Загл. с экр. - Яз. рус.