Авторство Лабораторных работ принадлежит СОСТАВИТЕЛЮ: Е.А. Зуева. Программирование на языках высокого уровня.Методические указания к выполнению лабораторных работ для студентов специальности 5В100200– Системы информационной безопасности. - Алматы: АУЭС, 2015. - 40 с.

Материал по каждой лабораторной работе включает в себя цель, рабочее задание, методические указания для выполнения работы и контрольные вопросы для самостоятельной подготовки.

Этапы выполнения лабораторной работы следующие: проработка теоретической части, выполнение рабочего задания, создание отчета и защита работы.

Все лабораторные работы ориентированы на проявление элементов научно-исследовательской деятельности студентов.

Выполнение каждой лабораторной работы должно завершаться оформлением отчета, согласно (1). Выполненная работа и оформленный отчет защищается у преподавателя.

Рабочее задание содержит конкретные работы по выполнению того или иного задания по рассматриваемой теме. Номер варианта задания дается согласно порядковому номеру в группе журнала преподавателя.

Выполнение лабораторных заданий дает возможность выработки навыков и знаний у студентов.

**7 Лабораторная работа №8. Python. Простые методы шифрования:**

# метод Цезаря, Полибианский квадрат, метод Вижинера

**Цель работы:** приобретение навыков работы по трем методам простого шифрования.

## 7.1 Рабочее задание

Реализовать программы кодирования и декодирования:

1. Методом Цезаря (ключ = порядковый номер студента по списку группы, фраза для шифрования = любое словосочетание);
2. Полибианским квадратом (в начале пишется фамилия и имя студента, фраза для шифрования = любое словосочетание);
3. Методом Вижинера (ключ = фамилия и имя студента, фраза для шифрования = любое словосочетание).

## 7.2 Методические указания к выполнению лабораторной работы

1. Метод Цезаря. В примере на рисунке 14 показан результат кодирования фразы «криптография, это наука» с ключом = -1. Необходимо также написать программу декодирования (преподавателем дается фраза для декодирования; определить ключ и фразу, подвергшуюся шифрованию).

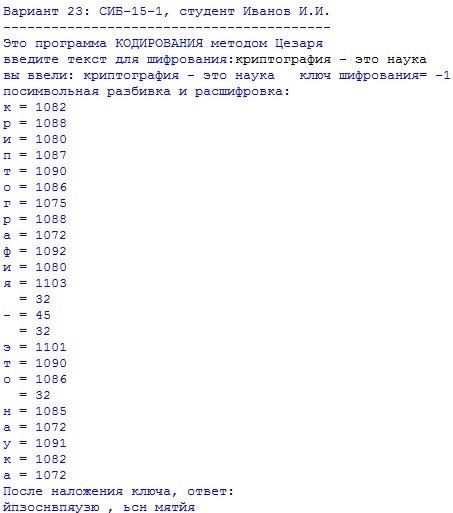


Рисунок 14 – Принскрин работы программы по шифрованию методом Цезаря

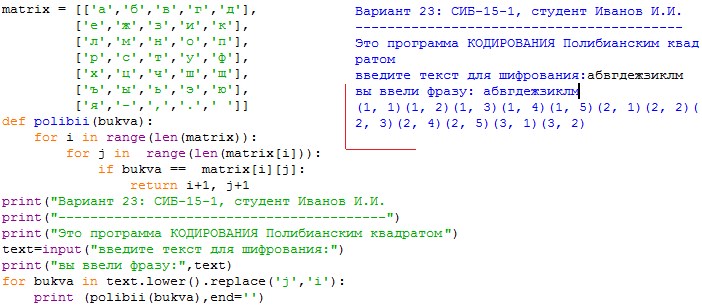
1. Полибианский квадрат (прямоугольник).

На рисунке 15а показан листинг и результат работы программы на абстрактной матрице размером 7∙5; студенту при выполнении задания необходимо ее под себя подкорректировать, вписав в начало таблицы буквы своих фамилии и имени без повторения, как, например, показано в таблице 4. Далее необходимо все полученные цифры при кодировании из матрицы записать без скобок и знаков «,» (вспомогательный принскрин с листингом представлены на рисунке 15б). Потом надо склеить все числа в одну строку – пример результата показан на рисунке 15в. Это и есть закодированная фраза с помощью квадрата Полибия.

Таблица 4 – Пример заполнения данными квадрата Полибия

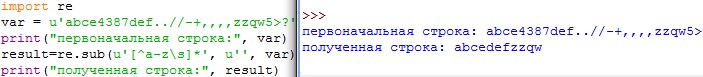
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | З | У | Е | В | А | К |
| **2** | Т | Р | И | Н | Б | Г |
| **3** | Д | Ж | Л | М | О | П |
| **4** | Р | С | Т | Ф | Х | Ц |
| **5** | Ч | Ш | Щ | Ъ | Ь | Э |
| **6** | Ю | Я | - | , | . | ˽ |

а)



б

)



в)



Рисунок 15

–

Листинг и результат работы алгоритма по абстрактной матрице

Декодирование. Дается некоторая строка чисел (подобно данным рисунка 15в) и, имея матрицу значений (подобно таблице 4), надо определить, какая фраза была зашифрована. Учитывая, что все числа состоят из одной цифры, обратная процедура декодирования (разбивки по парам) будет однозначной. Пример принскрина работы декодирования приведен на рисунке 16.

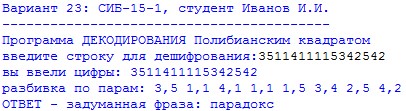


Рисунок 16 – Пример работы программы декодирования

3. Шифр Вижинера.

Ключом выступает фамилия и имя студента (без букв повторения); на фразу накладывается ключ, если же длина ключа маленькая, то ключ дублируется. На рисунке 17 представлен листинг шифрования методом Вижинера по 10-тизначному ключу («ЗуеваЕкатерина») без букв повторения: «зуевактрин». На рисунке 18 представлен принскрин осуществления шифрования по листингу с рисунка 17.



Рисунок 17 – Листинг осуществления шифрования

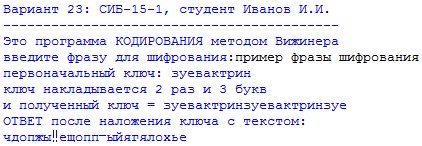


Рисунок 18 – Результат шифрования методом Вижинера

При декодировании надо, имея зашифрованную фразу и первоначальный ключ, восстановить исходный текст (пример результата работы программы декодирования представлен на рисунке 19).

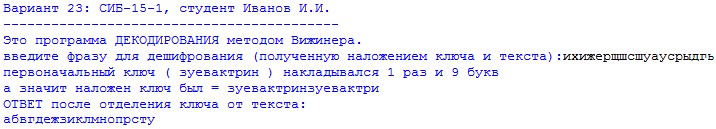


Рисунок 19 – Результат декодирования методом Вижинера

## 7.3 Список контрольных вопросов

1. Какой оператор подставляет числовое значение букве, а какой представляет буквенное значение цифре?
2. По таблице Ascii, в каком диапазоне лежат буквы английского алфавита?
3. По таблице Ascii, в каком диапазоне лежат буквы русского алфавита?

# Список литературы

1 Стандарт организации учебно-методические и учебные работы СТ НАО 56023-1910-04-2014. 2 Язык программирования Python. Сузи Р.А. Учебное пособие. - М.: Интернет Университет информационных технологий, 2007. – 327 с.

1. Марк Лутц. Программирование на Python. Тома 1 и 2, 4-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2011. – 992 с.
2. Саммерфилд М. Программирование на Python 3. Подробное руководство. Пер. с англ. Киселев А. – М.: Символ-Плюс, 2009. – 608 с. 5 Доусон М. Программируем на Python. - СПб.: Питер, 2014. - 416 с. 6 http://pythonworld.ru/ 7 Видеолекции на Youtube (открытая библиотека видеолекций):

https://www.youtube.com/watch?v=xhoX3-NdM9k