Лабораторная работа №1

Классические криптосистемы

Дедлайн: 06.10.2019

1 Введение

В данной лабораторной работе вам необходимо программно реализовать шесть классических криптосистем:

- Шифр сдвига
- Аффинный шифр
- Шифр простой замены
- Шифр Хилла
- Шифр перестановки
- Шифр Виженера

Данные криптосистем не отличаются высокой криптостойкостью, однако хорошо иллюстрируют приемы, которые могут применяться для шифрования сообщений. Дополнительную информацию вы можете получить в материалах лекции и книге.

2 Условие лабораторной работы

Ваша задача – реализация всех шести классических криптосистем. Под реализацией следует понимать компьютерную программу, написанную на одном из доступных языков программирования: {C/C++, C#, Java, Python[1]}, которая обладает определенной функциональностью.

Функциональность программы:

- зашифрование сообщения любой из указанных выше криптосистем;
- расшифрование сообщения, зашифрованного любой из указанных выше криптосистем;
- корректная обработка некорректного алфавита;

[1] Но не Jupyter Notebook

- корректная обработка некорректного ключа;
- корректная обработка не входящих в алфавит символов входного текста.

Входные данные программы:

- файл с алфавитом (alphabet.txt);
- файл с открытым текстом / шифртекстом (in.txt);
- файл с ключом (key.txt);
- указание, какую нужно проводить операцию (зашифрование или расшифрование);
- указание, какую криптосистему нужно использовать.

Выходные данные программы

- файл с открытым текстом (decrypt.txt) / шифртекстом (encrypt.txt) в зависимости от выбранной операции;
- сообщение об успешном выполнение операции, либо сообщение об ошибке (с указанием причины ошибки).

3 Описание входных данных

3.1 Файл с алфавитом

Файл с алфавитом содержит единственную строку, в которой записан набор попарно различных символов Это могут быть заглавные и строчные символы латинского и русского алфавитов, а также спецсимволы. По умолчанию (нет файла alphabet.txt) должен использоваться следующий алфавит: 33 заглавные русский буквы от «А» до «Я», а также символ « » (пробел): «АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ ». При этом считаем, что «А« = 0, «Б« = 1, ..., «Я« = 32, « » = 33. Следует иметь в виду, что файл с алфавитом может иметь некорректный формат. Программа должна каким-либо образом корректно обработать эту ситуацию. Далее будем считать, что алфавит имеет мощность M.

3.2 Файл с открытым текстом / шифртекстом

Файл содержит единственную строку, в которой записан открытый текст / шифртекст, состоящий из символов алфавита. При этом следует учитывать, что открытый текст / шифртекст может иметь некорректный формат. Программа должна каким-либо образом корректно обработать эту ситуацию.

3.3 Файл с ключом

Файл содержит единственную строку, в которой записан ключ. Для каждой криптосистемы ключ имеет собственную форму записи. Ниже описаны форматы корректных клюевых данных для каждой из криптосистем. При этом следует учитывать, что ключ может иметь некорректный формат. Программа должна каким-либо образом корректно обработать эту ситуацию.

3.3.1 Шифр сдвига

В качестве ключа задается символ из алфавита. При этом его числовое представление $k \in Z_M$.

3.3.2 Аффинный шифр

В качестве ключа задается пара символов из алфавита (k_1, k_2), записанных подряд (без разделителей). При этом их числовое представление $(k_1, M) = 1$ и $k_1, k_2 \in Z_M$.

3.3.3 Шифр простой замены

В качестве ключа задается вторая строка подстановки. При этом она должна содержать все символы алфавита, записанные в произвольном порядке по одному разу каждый, а числовое представление любого символа ключа $k_i \in Z_M$.

3.3.4 Шифр Хилла

В качестве ключа задаются четыре символа из алфавита, $(k_{11}, k_{12}, k_{21}, k_{22})$, записанных подряд (без разделителей). Из них и формируется ключевая матрица $2*2$ $K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$. При этом их числовое представление $(k_{11} * k_{22} - k_{12} * k_{21})$ mod $M \neq 0$, $(k_{11} * k_{22} - k_{12} * k_{21}, M) = 1$ и $k_{11}, k_{12}, k_{21}, k_{22} \in Z_M$. Если длина открытого текста не кратна 2, то в его конец необходимо дописать любой символ алфавита.
Внимание! Для шифрования следует умножать вектор с открытым текстом на матрицу-ключ (но не наоборот!), а для расшифрования – вектор с шифротекстом на обратную матрицу ключа (но не наоборот!).

3.3.5 Шифр перестановки

В качестве ключа задается строка, состоящая из попарно различных символов алфавита, длиной не более M символов. Положение символов ключа в алфавите определяет нижнюю строку подстановки. При этом числовое представление любого символа ключа $k_i \in Z_M$. Если длина открытого текста не кратна длине ключа, то в его конец необходимо дописать один и тот же символ алфавита таким образом, чтобы длина получившегося открытого текста была кратна длине ключа.

3.3.6 Шифр Виженера

В качестве ключа задается строка произвольной длины, состоящая из символов алфавита. При этом числовое представление любого символа ключа $k_i \in Z_M$.

3.4 Указания

Указания, определяющий криптосистему и процедуру (зашифрование или расшифрование) могут поступать на вход любым удобным автору программы способом, в том числе из консоли, из файла и через оконный интерфейс.

4 Бонусные задания

4.1 Бонусное задание №1

Реализовать программу, которая применяет частотный анализ, для раскрытия (взлома) шифртекстов, полученный с помощью шифра простой замены. Необходимо получить программу, на вход в которую поступает только шифртекст, зашифрованный шифром простой замены, а на выходе программа возвращает открытый текст и ключ. Язык открытых текстов: английский или русский (по выбору выполняющего задание).

4.2 Бонусное задание №2

Реализовать программу, которая применяет метод Касиски, для раскрытия (взлома) шифртекстов, полученный с помощью шифра Виженера. Необходимо получить программу, на вход в которую поступает только шифртекст, зашифрованный шифром Виженера, а на выходе программа возвращает открытый текст и ключ. Язык открытых текстов: русский.

4.3 Бонусное задание №3

Реализовать программу, которая применяет метод индекса совпадений, для раскрытия (взлома) шифртекстов, полученный с помощью шифра Виженера. Необходимо получить программу, на вход в которую поступает только шифртекст, зашифрованный шифром Виженера, а на выходе программа возвращает открытый текст и ключ. Язык открытых текстов: русский.

4.4 Бонусное задание №4

Реализовать программу, которая используется для раскрытия (взлома) шифртекстов, полученный с помощью шифра Хилла. Необходимо получить программу, на вход в которую поступает только шифртекст, зашифрованный шифром Хилла, а на выходе программа возвращает открытый текст и ключ. Известно, что для шифрования всегда используется матрица $2 * 2$. Язык открытых текстов: русский.

4.5 Особенности бонусных заданий

- Бонусное задание №1 может выполнить неограниченное число студентов.
- Бонусное задание №1 можно выполнять как индивидуально, так и парами (в этом случае каждый получит по половине баллов).
- В зависимости от результатов, за бонусное задание №1 можно получить от 20 до 40 баллов.
- Бонусные задания №2 – №4 могут выполнить по два студента, которое первыми напишут о своем желании в Telegram-канале *BSUCrypto2020-2021*. При этом два студента, которые делают одно и то же задание, должны использовать разные языки программирования.
- Один студент может делать не более одного задания (из бонусных заданий №2 – №4).
- За бонусные задания №2 – №4 можно получить по 20 баллов.
- Бонусные задания можно выполнить и сдать до конца семестра.

5 Порядок сдачи лабораторной работы

- Вам необходимо создать архив формата «.zip», название которого должно иметь вид «Ivanov_1.zip», где «Ivanov» – ваша фамилия латинскими буквами. В архиве должен быть исходный код вашей реализации (НЕ весь проект целиком, а только файлы с исходным кодом (.c, .cpp, .java и т.п.)), а также файлы, которые необходимы для сборки проекта (если такие имеются). При отправке бонусных заданий наименование файла сохраняется, лишь в самый конец дописывается символ «b».
- Не позже, чем за 24 часа до сдачи лабораторной работы преподавателю в университете, вы должны отправить архив по одному из контактов, указанных в ответе на вопрос №3 в файле «FAQ.pdf».