САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра вычислительной техники

КУРСОВОЙ ПРОЕКТ

по дисциплине «Программирование»

Тема: Историческая криптография и стеганография.

Студент гр. 8307 _____ Готовский К.В.

Преподаватель _____ Перязева Ю.В.

Санкт-Петербург
2018

ЗАДАНИЕ
НА КУРСОВОЙ ПРОЕКТ

Студент Готовский К.В.

Группа 8307

Тема проекта: Разностный «гамбеттовский» шифр с двойным периодом

Исходные данные:
Текст, требуемый для шифрования, и два шифра.

Содержание пояснительной записки:
Содержание, Введение, Разностный «гамбеттовский» шифр с двойным периодом, Программная реализация шифра, Заключение, Список использованных источников, Приложение А. Блок-схема программы, Приложение Б. Текст программы.

Предполагаемый объем пояснительной записки:
Не менее 10 страниц.

Дата выдачи задания: 08.11.2018

Дата сдачи реферата: 22.12.2018

Дата защиты реферата: 24.12.2018

Студент _____ Готовский К.В.

Преподаватель _____ Перязева Ю.В.

АННОТАЦИЯ

Суть проекта в том, чтобы создать программу, которая будет зашифровывать любой текст на любом языке (русский и английский) с помощью разностного «гамбеттовского» шифра с двойным периодом. Средой реализации является язык программирования Си.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель проекта получить практические навыки в разработке алгоритма и написании программы на языке Си для шифрования строк и работе с файлами. Заданием является зашифровать сообщение разностным «гамбеттовским» шифром с двойным периодом.

1. РАЗНОСТНЫЙ «ГАМБЕТТОВСКИЙ» ШИФР С ДВОЙНЫМ ПЕРИОДОМ

1.1. История шифра

В революционном подполье опыт использования шифров передавался из поколения в поколение. Уже члены организации «Народная воля» применяли так называемый «тюремный шифр» — вариант «шифра Полибия», — обошедший все тюрьмы и крепости, все остроги и централы. Творцом его считается декабрист Михаил Александрович Бестужев, находившийся в 1826 г в Алексеевском равелине Петропавловской крепости. В этом шифре буквы алфавита выписываются в квадрат 6х6 и заменяются биграммой, состоящей из номера строки и номера столбца соответствующей буквы. При перестукивании арестанты передавали буквы ударами, обозначавшими координаты буквы в таблице. Народовольцы стали пользоваться и книжным шифром, о котором речь пойдет ниже. Вообще конспирация и конспиративная переписка (тайнописью — «химией», шифром) были у революционеров в ранний период на достаточно высоком уровне. В какой–то мере ослабление внимания к конспиративным требованиям дало возможность полиции получить и дешифровать переписку народовольцев, в результате чего известная группа членов этой организации была арестована и казнена после убийства царя Александра II 1 марта 1881 г.

С увеличением числа революционных организаций и количеством их членов в 90–е годы XIX в. произошло значительное снижение уровня конспирации. Длительное время не придавалось особого значения обучению членов революционных организаций конспиративным правилам и приемам. О них не писали, не говорили, не дебатировали. Предполагалось как бы, что конспиративные приемы даются от рождения или приобретаются с практикой. Следствием этого явились массовые систематические провалы. Это дало повод одному из лидеров «Бунда» Л. Розенталю (подпольный псевдоним «Бундовец») в своей книге «Шифрованное письмо», изданной в 1904 г. в Женеве, писать: «Если… мы обратимся к социал–демократическим организациям, то… рассматривая вопрос исключительно с точки зрения конспиративной ловкости и выдержки наших революционеров (имеются в виду российские революционеры всех партий и групп того времени вообще. — Т. С.), мы видим, что они не только стоят несравненно ниже деятелей Народной Воли, но почти не делают успехов из году в год»[195]

Еще в конце XIX в., несмотря на уже богатый опыт подпольной борьбы с самодержавием, российским революционерам суровые требования конспирации, осторожности, а главное, выдержки все еще казались невыполнимыми, стеснительными, тормозящими живое дело. Сплошь и рядом осторожность объявлялась трусостью, отсутствием настоящей революционности и товарищеских чувств.

Поистине замечательной была в русском революционере вера в шифры Более 99% писем, которыми обменивались революционеры, были шифрованными. Их отправляли почтой, доверяли им самые важные тайны. «Бундовец» пишет: «На чем основана наша вера в неразрешимость шифра? Что, если мы ошибаемся? Если тайна, доверенная шифру, уже не тайна? Если мы все время пребываем в состоянии мистификации?..

Основываясь на случаях раскрытия писем бюро Департамента полиции и нашем личном опыте, мы не только ставим вышеприведенный вопрос о самообмане, но даем на него вполне определенный утвердительный ответ: да, мы, российские революционеры, в отношении шифров пребываем в состоянии вредного самообмана… И нам, и некоторым товарищам нашим приходилось иногда поневоле предпринимать попытки раскрывать письма без ключа. Это случалось тогда, когда корреспондент перепутывал ключ или, если в отсутствии товарища, обыкновенно ведшего переписку, получалось письмо из такого города, для которого тот позабыл сообщить ключ. И что же? Не было ни одного случая, когда бы шифр оставался неразобранным»[196].

Большое значение придавалось вопросам конспирации в рядах социал–демократии. Сохранение в тайне обширной партийной переписки, которая была не только одним из важных способов связи в нелегальных организациях, но служила и каналом идейного и организационного руководства, требовало соблюдения строжайшей дисциплины. В. И. Ленин лично предъявлял в этом отношении жесткие требования. От одного он требовал писать письма шифром или «химией», другого предупреждал: «Не пишите, пожалуйста, никаких инициалов в письмах — господь их знает, вполне ли здесь надежна почта», третьего предостерегал: «…не пишите прямо в письмах ничего… никто не должен знать, где и кем издано… Все черняки сжечь!». Он указывал: «Ни издания листовок, ни транспорта, ни спевки насчет прокламаций, ни посылки их проектов и пр. и пр. нельзя поставить без правильной конспиративной переписки. В этом гвоздь!»

В январе 1901 г. вышел первый номер «Искры», которой предстояло сыграть решающую роль в образовании РСДРП. Е. Д. Стасова позднее вспоминала, с какой сложной, трудоемкой и кропотливой работой было связано ведение конспиративной переписки: «Прежде всего надо было подготовить текст письма и отметить для последующей шифровки наиболее конспиративные сведения. После этого на отдельном листке нужные места зашифровывались и тщательно проверялись, чтобы не было ошибок, которые чрезвычайно затрудняли дешифровку письма… Требовалось еще на каком–либо иностранном языке написать так называемое внешнее письмо, чтобы не вызвать малейших подозрений… И, наконец, за внешним письмом следовала последняя процедура — между строк явного письма различными химическими составами (химией) вписывалось конспиративное зашифрованное письмо». У «Искры» в России было, помимо комитетов и групп, около ста корреспондентов. В месяц секретарю редакции Н. К. Крупской приходилось так обрабатывать до 300 писем.

Еще в работе «Насущный вопрос», написанной в ссылке в 90–х годах, Ленин писал: «Против нас, против маленьких групп социалистов, ютящихся по широкому русскому «подполью», стоит гигантский механизм

могущественного современного государства, напрягающего все силы, чтобы задавить социализм и демократию. Мы убеждены, что мы сломим в конце концов это полицейское государство, потому что за демократию и социализм стоят все здоровые и развивающиеся слои всего народа, но чтобы вести систематическую борьбу против правительства, мы должны довести революционную организацию, дисциплину и конспиративную технику до высшей степени совершенства»[197].

Как известно, «Искра» наряду с газетой и научно–политическим журналом «Заря» выпускала различные книги, брошюры и прокламации. За три года было выпущено 56 таких изданий, в которых обобщался накопленный революционный опыт, содержались политические и экономические идеи. К числу этих изданий относится и брошюра Бахарева «О шифрах», изданная, как и книга «Бундовца», в Женеве, но несколько раньше, в 1902 г. В ней рассматривались некоторые шифры, применяемые революционерами, приводился их элементарный анализ и давались рекомендации по их использованию «чтобы, — как писал автор, — предостеречь от постоянно допускаемых ошибок». Помимо вопросов о шифрах в брошюре излагались способы «химической переписки» и «перестукивания в тюрьме».

1.2. Описания шифра

Рассмотренные выше шифры основаны на сложении. Но можно с успехом производить и вычитание. Нет смысла на этом останавливаться. Здесь все аналогично.

Мы рассмотрим только усложненную форму разностного периодического шифра, которая встречается в революционной практике. Возьмем ключ: «Шкурный вопрос» и фразу: «Нам нужны наборщики». Первая буква ключа «Ш» (= 24 по тюремной азбуке) больше первой буквы текста «Н» (= 13) на 11 единиц. Это мы выразим так: 1 – 11. В приведенном двучлене единица означает первую букву текста, а 11 – что она меньше первой буквы ключа на 11 единиц.

Вторая буква ключа «К» (= 10) больше второй буквы текста «А» (= 1) на 9. Следовательно пишем: 2 – 9. Третья запишется: 3 – 7. Четвертая: 4 – 3. Пятая буква ключа «Н» (= 13) меньше соответствующей буквы текста «У» (= 19) на 6 единиц. Поэтому эта пара изображается так: 5 + 6. Получаем ряд числовых пар:

1– 11, 2 – 9, 3 – 7, 4 – 3, 5 + 6, …

Но этим дело не кончается. Вводится второй период, представленный коротким числом. Например, 795. Три цифры будем последовательно прибавлять к каждому числу наших двучленов. Получаем шифр: 8 – 20, 7 – 16, 12 – 12, 11 – 12, 10 + 13, …

Такой шифр весьма громоздок в применении, что не оправдывается его надежностью. Однако до сих пор встречается в революционной переписке.

2. ПРОГРАМНАЯ РЕАЛИЗАЦИЯ ШИФРА

2.1. Описание решения

1) Читаю файл (в файле лежат строки на английском/русском языке: текст, первый шифр и второй шифр. Текст и первый шифр одного языка).
2) Обрабатываю полученные данные.
   а) Убираю всё, кроме символов для текста и первого шифра.
   б) Нахожу разности между буквами текста и буквами первого шифра по алфавиту. Если разность отрицательна, то ставлю «-» между порядковым номером буквы и разностью этой буквы. Если разность положительна, ставлю в том же месте «+».
   в) Добавляю 2 шифр к порядковому номеру буквы и к модулю разности из пункта (б).
3) Записываю результат в новый файл.

2.2. Описание переменных

Таблица описание переменных.

Имя переменной	Тип	Назначение
itog	FILE	исходный файл
te	char	строка считанного текста
co1	char	строка считанного шифра 1
tex	char	строка обработанного текста
cox	char	строка обработанного шифра 1
co2	char	строка считанного шифра 2
zn	char	строка знаков
lol	char	строка для зацикливания шифра
n	int	длинна текста
m	int	длинна обрабатываемой строки
k	int	счётчик для массива
i	int	счётчик для массива
j	int	счётчик для массива

2.3. Контрольные примеры

Программа корректно работает с лишними символами, пробелами, знаками препинания и заглавными буквами:

1) I hid1234e 532;"][;not32h4i54n5g

Se`123'c'214`'ret

1337

2.4. Примеры работы программы

Входные данные:

I hide nothing
Secret
1337

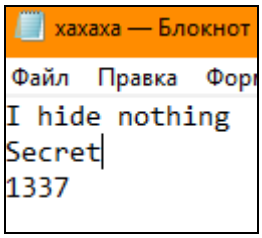
Промежуточные действия:

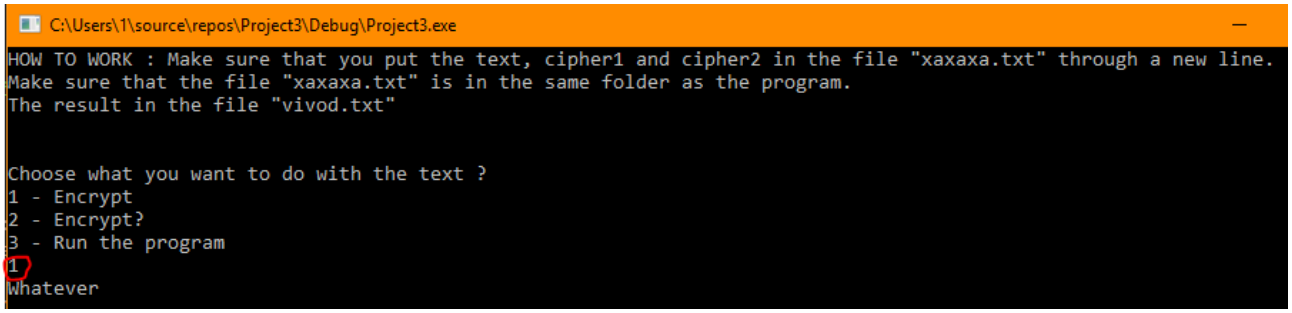
«I» =9, «S» =19
9-(-19) = -10
«h» =8, «e» =5
8-5=3
«i» =9, «c» =3
9-3=6
… (и так далее)
Получаю:
1-10, 2+3, 3+6, 4-14, 5+0, 6-6, 7-4, 8+15, 9+5, 10-9, 11+9, 12-13,
Применяю 2 шифр:
(1+1)-(10+3), (2+3)+(3+7), (3+1)+(6+3), (4+3)-(14+7), (5+1)+(0+3), (6+3)-(6+7), (7+1)-(4+3), (8+3)+(15+7), (9+1)+(5+3), (10+3)-(9+7), (11+1)+(9+3), (12+3)-(13+7),

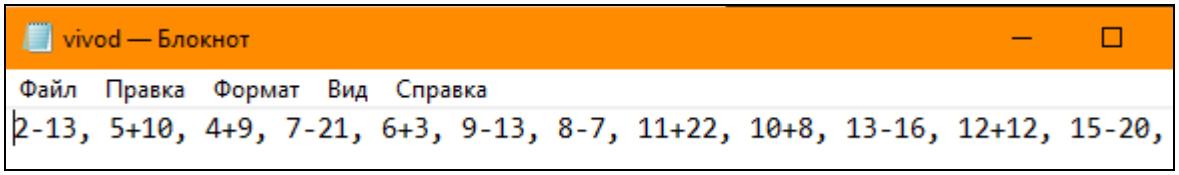
Вывод:

2-13, 5+10, 4+9, 7-21, 6+3, 9-13, 8-7, 11+22, 10+8, 13-16, 12+12, 15-20,

Отображение работы на мониторе:







ЗАКЛЮЧЕНИЕ

При выполнении курсового проекта были получены практические навыки в работе с переменными, функциями, одномерными динамическими массивами, строками, файлами, шифрами. Был реализован в виде программы шифрование с помощью разностного «гамбеттовского» шифра с двойным периодом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

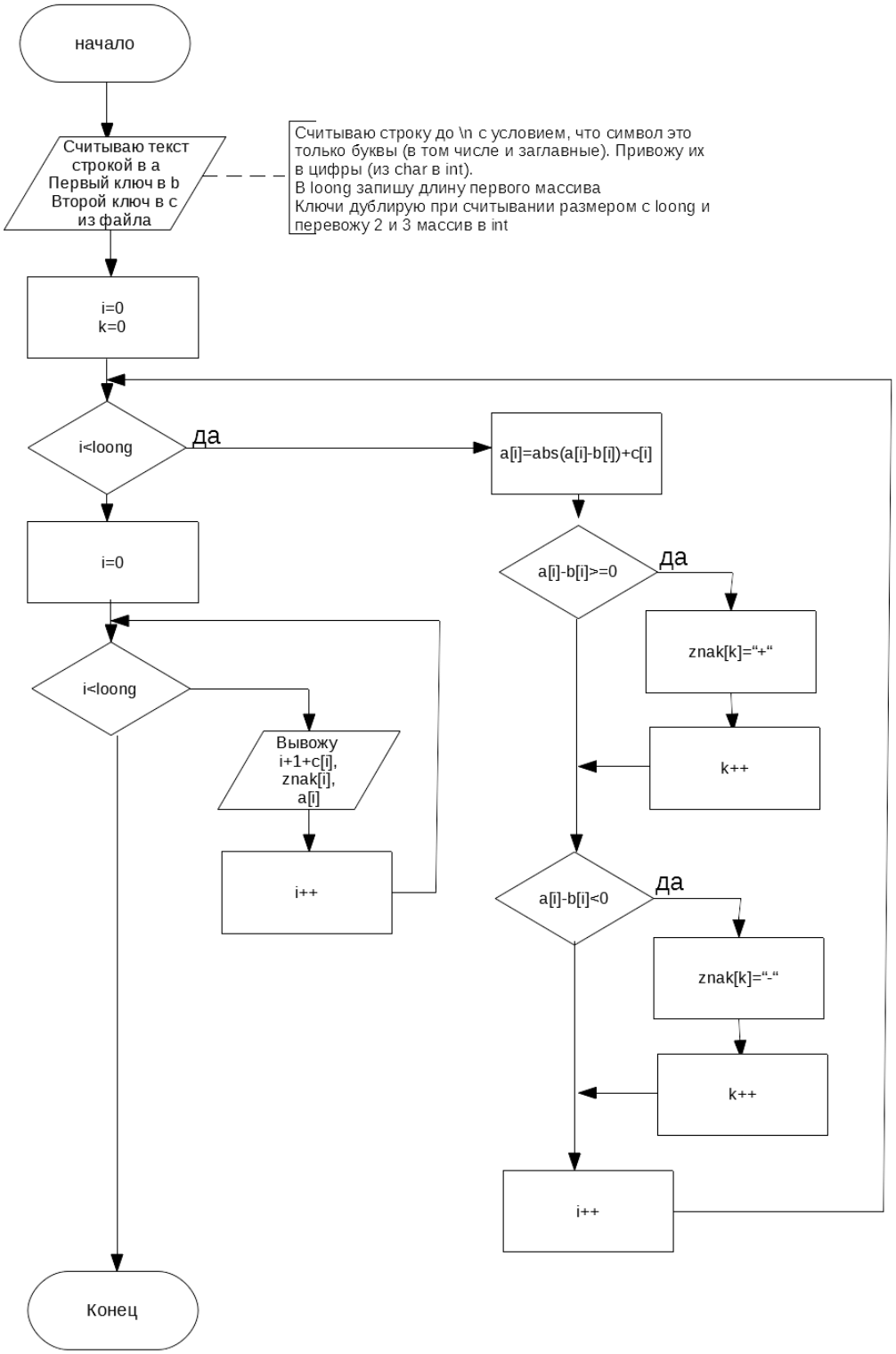
1. Библиотека Хроноса. URL: http://www.hrono.ru/libris/lib_s/shifr22.html (дата обращения 20.12.2018)

2. Рефераты, Курсовые, Конспекты. URL: http://allrefs.net/c2/46lxz/p10/ (дата обращения 22.12.2018)

3. Презентация без автора URL: http://www.imkn.ru/KIB/Nissenbaum/Shared%20Documents/%D0%98%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8/%D0%98%D1%81%D1%82_%D0%BA_%D1%82%D0%B5%D0%BC%D0%B07.ppt
стр 12.

ПРИЛОЖЕНИЕ А

БЛОК-СХЕМА ПРОГРАММЫ



ПРИЛОЖЕНИЕ Б

ТЕКСТ ПРОГРАММЫ

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#define M 200
#define MA 400

void menu () {
     puts("HOW TO WORK : Make sure that you put the text, cipher1
and cipher2 in the file \"xaxaxa.txt\" through a new line.");
     puts("Make sure that the file \"xaxaxa.txt\" is in the same
folder as the program.");
     puts("The result in the file \"vivod.txt\"");
     puts("\n\nChoose what you want to do with the text ?\n1 -
Encrypt\n2 - Encrypt?\n3 - Run the program");
     getchar();
     puts("Whatever");
     getchar();
}

void chitau(char *te,char *co1,char *co2) {
     FILE *text;
     int i = 0;
     if ((text = fopen("xaxaxa.txt", "r")) == NULL) {
          printf("Cannot open file.\n");
          exit(1);
     }
     fgets(te, M, text);
     fgets(co1, M, text);
     fgets(co2, M, text);
     fclose(text);
}

void oba(char *te,char *tex) {
     int j = 0, m = strlen(te);
     for (int i = 0; i < m; i++) {
          if ((te[i] >= 'a') && (te[i] <= 'z')) {
               tex[j] = te[i];
               j++;
          }
          if ((te[i] >= 'A') && (te[i] <= 'Z')) {
               tex[j] = te[i] - 'A' + 'a';
               j++;
          }
          if ((te[i] >= 'а') && (te[i] <= 'я')) {
               tex[j] = te[i];
               j++;
          }
          if ((te[i] >= 'А') && (te[i] <= 'Я')) {
               tex[j] = te[i] - 'А' + 'а';
               j++;
          }
     }
     tex[j] = '\0';
     free(te);
}
```

```
void polnie(char *co1, int n) {
     int m = strlen(co1);
     char *lol = NULL;
     lol = (char*)malloc(m * sizeof(char));
     if (co1[m - 1] == '\n')
          co1[m - 1] = '\0';
     if (lol != NULL) {
          memcpy(lol, co1, m);
          for (int i = 0; i < 2*n; i += m)
               strncat(co1, lol, m);
          free(lol);
     }
     else {
          puts("Error of memory");
          free(lol);
          exit(1);
     }
}

void znaki(char *zn, int n) {
     for (int i = 0; i < n; i++)
          zn[i] = '+';
}

int main() {
     FILE *itog;
     char *te = NULL, *tex = NULL, *co1 = NULL, *cox = NULL, *co2
= NULL, *zn = NULL;
     int n,k=0;
     te = (char*)malloc(M * sizeof(char));
     tex = (char*)malloc(M * sizeof(char));
     co1 = (char*)malloc(M * sizeof(char));
     cox = (char*)malloc(M * sizeof(char));
     co2 = (char*)malloc(MA * sizeof(char));
     zn = (char*)malloc(M * sizeof(char));
     if (te == NULL || tex == NULL || co1 == NULL || cox == NULL
|| co2 == NULL || zn == NULL) {
          puts("Error of memory");
          free(te);
          free(co1);
          free(cox);
          free(co2);
          free(zn);
          free(tex);
     }
     else {
          menu();
          chitau(te, co1, co2);
          n = strlen(te)-1;
          oba(te, tex);
          oba(co1, cox);
          n = strlen(tex);
          polnie(cox,n);
          znaki(zn, n);
          for (int i = 0; i < n; i++) {
               if (tex[i] - cox[i] < 0)
                    zn[i] = '-';
               tex[i] = abs(cox[i] - tex[i]);
          }
          polnie(co2, n);
```

```
            itog = fopen("vivod.txt", "a");
            for (int i = 0; i < n; i++, k += 2)
                 fprintf(itog, "%d%c%d, ", i + 1 + co2[k] - '0',
zn[i], tex[i] + co2[k + 1] - '0');
            fprintf(itog, "\n");
            fclose(itog);
            free(cox);
            free(co2);
            free(zn);
            free(tex);
      }
      return 0;
      }
```