МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Лабораторная работа №2

по дисциплине

«Информатика и программирование»

Классы и шифры

Группа: **АБс-822**

Студент: **Соленый Н.Е.**

Преподаватель:

НОВОСИБИРСК

2019

**Задача:**

Реализовать интерфейс для теста алгоритмов шифрования на выбор пользователя. Реализовать и сами алгоритмы на C++, применив ООП. Для секретной информации использовать атрибуты private. Задачу выполнить для алгоритмов с заранее заданными ключами.

**Структура проекта**

**Интерфейс взаимодействия с пользователем**

// (main.cpp)

#include <iostream>

#include <typeinfo>

#include "shifres.hpp"

using namespace std;

enum class Type {SHAMIR=1, DIFFI\_HELLMAN, RSA, EL\_GHAMAL, CAESAR, ATBASH, GRONSFIELD, TABLET};

template <typename Enumeration>

auto as\_integer(Enumeration const value) -> typename std::underlying\_type<Enumeration>::type {

return static\_cast<typename std::underlying\_type<Enumeration>::type>(value);

}

template<>

constexpr auto as\_integer<Type>(Type const value) -> typename std::underlying\_type<Type>::type {

int n = static\_cast<typename std::underlying\_type<Type>::type>(value);

if (n < 1 || n > 8)

throw std::runtime\_error("Incorrect input");

return n;

}

Type chooseEncode() {

int t;

inputerror:

cout << "1 - Shamir`s\n"

"2 - Diffi-Hellman`s\n"

"3 - RSA\n"

"4 - El-Ghamal`s\n"

"5 - Caesar\n"

"6 - Atbash\n"

"7 - Gronsfield\n"

"8 - By table\n"

"Enter type of simulated encryption algorythm: ";

cin >> t;

cout << endl;

try {

Type encode = static\_cast<Type>(t);

cout << as\_integer(encode) << endl;

return encode;

}

catch (std::exception &e) {

cerr << e.what() << endl;

goto inputerror;

}

}

void emulateRecipient(Type type) {

init(".recipient", ".dispatcher"); /// this is a crutch. it shouldn't be here, but we have it

switch (type) {

case Type::DIFFI\_HELLMAN: {

Diffi\_Hellman session;

cout << "\nMy shared key is " << session.sharedKey <<

". Just reporting, nothing more. I won`t tell you my secret key." << endl;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "\nI`m abonent B. My secret number is " << session.getEvaluatedNumber() <<

"; abonent A has equal secret number" << endl;

break;

}

case Type::EL\_GHAMAL: {

El\_Ghamal session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

case Type::SHAMIR: {

Shamir session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

case Type::RSA: {

RSA session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

case Type::CAESAR: {

Caesar session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

case Type::ATBASH: {

Atbash session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

case Type::GRONSFIELD: {

Gronsfield session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

case Type::TABLET: {

Tablet session;

cout << "processing..." << endl;

session.recipient\_protocol();

cout << "Got message! (output.txt)" << endl;

break;

}

}

}

void emulateDispatcher(Type type) {

init(".dispatcher", ".recipient"); /// this is a crutch. it shouldn't be here, but we have it

switch (type) {

case Type::DIFFI\_HELLMAN: {

Diffi\_Hellman session;

cout << "\nMy shared key is " << session.sharedKey <<

". Just reporting, nothing more. I won`t tell you my secret key." << endl;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "\nI`m abonent A. My secret number is " << session.getEvaluatedNumber() <<

"; abonent B has equal secret number" << endl;

break;

}

case Type::EL\_GHAMAL: {

El\_Ghamal session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

case Type::SHAMIR: {

Shamir session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

case Type::RSA: {

RSA session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

case Type::CAESAR: {

Caesar session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

case Type::ATBASH: {

Atbash session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

case Type::GRONSFIELD: {

Gronsfield session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

case Type::TABLET: {

Tablet session;

cout << "processing..." << endl;

session.dispatcher\_protocol();

cout << "Message input.txt was sent" << endl;

break;

}

}

}

void chooseMode(Type type) {

int m;

err:

cout << "1 - Emulate recipient\n"

"2 - Emulate dispatcher to encrypt file (shared key of any recipient required)\n"

"Choose mode: ";

cin >> m;

cout << endl;

switch(m) {

case DISPATCHER:

emulateDispatcher(type);

break;

case RECIPIENT:

emulateRecipient(type);

break;

default:

goto err;

}

};

int main(int argc, char\*argv[]) {

if(argc==1) {

Type type = chooseEncode();

chooseMode(type);

system("pause");

} else {

Environment &Environment = Environment::Instance();

Type type = static\_cast<Type>(0);

void (\*f)(Type) = nullptr;

for(int i = 1; i < argc; i++) {

if(argv[i][0]!='-') throw std::runtime\_error("Incorrect input\n");

else {

switch(argv[i][1]) {

case 'i':

Environment.input = string(argv[++i]);

break;

case 'o':

Environment.output = string(argv[++i]);

break;

case 'b':

Environment.enableBinary = true;

break;

case '-': {

string str(argv[i]+2);

if(str==string("diffi-hellman")) type = Type::DIFFI\_HELLMAN;

else if (str==string("shamir")) type = Type::SHAMIR;

else if (str==string("el-ghamal")) type = Type::EL\_GHAMAL;

else if (str==string("rsa")) type = Type::RSA;

else if (str==string("caesar")) type = Type::CAESAR;

else if (str==string("atbash")) type = Type::ATBASH;

else if (str==string("gronsfield")) type = Type::GRONSFIELD;

else if (str==string("tablet")) type = Type::TABLET;

else throw std::runtime\_error("Incorrect input\n");

break;

}

case 'r':

f = emulateRecipient;

break;

case 'd':

f = emulateDispatcher;

break;

}

}

}

if(f == nullptr || type == static\_cast<Type>(0)) throw std::runtime\_error("Incorrect input\n");

f(type);

}

return 0;

}

Выбор, какого клиента эмулировать, отправителя или получателя. Выбор алгоритма для теста. Защита ввода. Пользователю нужно запустить два экземпляра программы и дождаться выполнения (передачи файла или удачного соединения). Также присутствует небольшой скрипт для тестов:

// (bin/Release/script.sh)

echo '1 - Shamir`s

2 - Diffi-Hellman`s

3 - RSA

4 - El-Ghamal`s

5 - Caesar

6 - Atbash

7 - Gronsfield

8 - by table

Enter type of simulated encryption algorythm: '

read T

if [ $T == 2 ]

then

echo "$T 1 " | ./001.exe | grep ' secret number is ' &

echo "$T 2 " | ./001.exe | grep ' secret number is '

else

echo "$T 1 " | ./001.exe > /dev/null &

echo "$T 2 " | ./001.exe > /dev/null

if [ -e ./.dispatcher ]

then

rm ./.dispatcher

fi

if [ -e ./.recipient ]

then

rm ./.recipient

fi

cat output.txt

fi

**Описание классов алгоритмов через наследование**

// (shifres.hpp)

#include "locker.h"

#include <fstream>

#include <iostream>

#include <boost/multiprecision/cpp\_int.hpp> //1\_71\_0 // I could place this only in .hpp?

#include <boost/random.hpp> //

#undef EXIT\_SUCCESS

enum Mode {RECIPIENT=1, DISPATCHER};

using namespace std;

using namespace boost::multiprecision;

class Environment {

public:

string input, output;

bool enableBinary;

static Environment& Instance() { static Environment s; return s; }

private:

Environment() { input = "input.txt", output = "output.txt"; }

~Environment() { }

Environment(Environment const&) = delete;

Environment& operator= (Environment const&) = delete;

};

class Encoded\_Structure {

public:

virtual void recipient\_protocol();

virtual void dispatcher\_protocol();

enum class FileStat{ EXIT\_SUCCESS, FAILED, UNNAMED\_ERROR };

protected:

virtual void decode(void\* data) = 0;

virtual void encode(void\* data) = 0;

virtual void takeSharedKey();

virtual void giveSharedKey();

void waitTilReady(WaitMode m);

uint8\_t takeByte();

uint8\_t sendByte(uint8\_t data);

void sendEOF();

void write(int byte);

int read();

};

class Caesar : public Encoded\_Structure {

public:

Caesar();

private:

inline void decode(void\* data) override;

inline void encode(void\* data) override;

static const int key;

};

class Atbash : public Encoded\_Structure {

public:

Atbash();

private:

inline void decode(void\* data) override;

inline void encode(void\* data) override;

};

class Gronsfield : public Encoded\_Structure {

public:

Gronsfield();

private:

inline void decode(void\* data) override;

inline void encode(void\* data) override;

static const int key[];

};

class Tablet : public Encoded\_Structure {

public:

Tablet();

private:

inline void decode(void\* data) override;

inline void encode(void\* data) override;

static const uint8\_t table[256];

};

Классы алгоритмов наследуются от основного класса, реализующего некоторые общие методы (чтения, записи данных, реализацию каналов их передачи). При этом, наследуясь от базового класса, потомки должны реализовать некоторые виртуальные методы родителя.

**Реализация алгоритмов**

0. Общий класс

Реализация общих, одинаковых для некоторых подклассов методов обмена сообщениями и ключами. Реализация служебных методов: чтение, запись, ожидание готовности потока.

// (encoded\_structure.cpp)

#include "shifres.hpp"

//#define DEB

#ifdef DEB

#define LOG(N) cout << N;

#else

#define LOG(N)

#endif

void Encoded\_Structure::waitTilReady(WaitMode m) {

switch(m) {

case REV\_STRT\_UNLOCKED: {

do {

LOG(1);

trylock\_reverse\_channel();

} while(errno != 0);

do {

LOG(2);

trylock\_straight\_channel();

} while(errno != 0);

break;

}

case OREV\_LOCKED: {

do {

LOG(3);

trylock\_reverse\_channel();

} while(errno != EACCES);

do {

LOG(4);

trylock\_straight\_channel();

} while(errno != 0);

break;

}

case REV\_LOCKED: {

do {

LOG(5);

trylock\_reverse\_channel();

} while(errno != EACCES);

break;

}

case REV\_UNLOCKED: {

do {

LOG(6);

trylock\_reverse\_channel();

} while(errno != 0);

break;

}

}

}

int Encoded\_Structure::read() {

Environment &Environment = Environment::Instance();

static ifstream file(Environment.input, ios::binary|ios::in);

uint8\_t data;

file.get((char&)data);

if(file.eof()) {

file.close();

throw FileStat::EXIT\_SUCCESS;

}

return data;

}

void Encoded\_Structure::write(int data) {

Environment &Environment = Environment::Instance();

static ofstream file(Environment.output, ios::binary|ios::out);

if (data == EOF) {

file.close();

return;

}

file << static\_cast<uint8\_t>(data);

}

uint8\_t Encoded\_Structure::takeByte() { /// deprecated, dye to the impossibility of mixed use with sendByte

waitTilReady(OREV\_LOCKED);

lock\_straight\_channel();

waitTilReady(REV\_UNLOCKED);

int data;

data = readByte();

unlock\_reverse\_channel();

unlock\_straight\_channel();

if (data == EOF)

throw FileStat::EXIT\_SUCCESS;

return data;

}

uint8\_t Encoded\_Structure::sendByte(uint8\_t data) { /// deprecated, dye to the impossibility of mixed use with takeByte

// not turned out to write nice abstraction of transmission protocol

waitTilReady(REV\_STRT\_UNLOCKED);

putByte(data);

waitTilReady(REV\_LOCKED);

unlock\_straight\_channel();

waitTilReady(REV\_STRT\_UNLOCKED);

uint8\_t answer = readByte();

unlock\_reverse\_channel();

return answer;

}

void Encoded\_Structure::sendEOF() {

waitTilReady(REV\_STRT\_UNLOCKED);

putByte(EOF);

waitTilReady(REV\_LOCKED);

unlock\_straight\_channel();

}

void Encoded\_Structure::recipient\_protocol() {

int sz = 1;

Encoded\_Structure\* r = dynamic\_cast<RSA\*>(this);

if(r)sz = 34;

r = dynamic\_cast<El\_Ghamal\*>(this);

if(r)sz = 2;

takeSharedKey();

while(true) {

waitTilReady(OREV\_LOCKED);

lock\_straight\_channel();

waitTilReady(REV\_UNLOCKED);

int byte[sz] = {0};

if(readBytes(byte, sz\*4) == EOF) { write(EOF); unlock\_reverse\_channel(); unlock\_straight\_channel(); break; }

unlock\_reverse\_channel();

unlock\_straight\_channel();

decode(byte);

write(byte[0]);

}

}

void Encoded\_Structure::dispatcher\_protocol() {

int sz = 1;

Encoded\_Structure\* r = dynamic\_cast<RSA\*>(this);

if(r)sz = 34;

r = dynamic\_cast<El\_Ghamal\*>(this);

if(r)sz = 2;

giveSharedKey();

try {

while(true) {

int byte[sz] = {0};

byte[0] = read();

encode(byte);

waitTilReady(REV\_STRT\_UNLOCKED);

putBytes(byte, sz\*4);

waitTilReady(REV\_LOCKED);

unlock\_straight\_channel();

}

}

catch (FileStat) {

sendEOF();

}

}

void Encoded\_Structure::takeSharedKey() {

waitTilReady(OREV\_LOCKED);

putBytes(&sharedKey, 4);

waitTilReady(REV\_UNLOCKED);

readBytes(&takenSharedKey, 4);

unlock\_reverse\_channel();

unlock\_straight\_channel();

}

void Encoded\_Structure::giveSharedKey() {

waitTilReady(REV\_STRT\_UNLOCKED);

putBytes(&sharedKey, 4);

waitTilReady(REV\_LOCKED);

unlock\_straight\_channel();

waitTilReady(REV\_STRT\_UNLOCKED);

readBytes(&takenSharedKey, 4);

unlock\_reverse\_channel();

}

// (other\_shifres.cpp)

#include "shifres.hpp"

// 1. Шифр Цезаря

const int Caesar::key = -28;

Caesar::Caesar() { }

inline void Caesar::decode(void\* data) {

uint8\_t r = \*((int\*)data) - key;

\*((int\*)data) = r;

}

inline void Caesar::encode(void\* data) {

uint8\_t r = \*((int\*)data) + key;

\*((int\*)data) = r;

}

// 2. Шифр атбаш

Atbash::Atbash() { }

inline void Atbash::decode(void\* data) {

uint8\_t r = \*((int\*)data);

\*((int\*)data) = 255-r;

}

inline void Atbash::encode(void\* data) {

uint8\_t r = \*((int\*)data);

\*((int\*)data) = 255-r;

}

// 3. Шифр Гронсфиельда

const int Gronsfield::key[5] = { 250, 14, -6, -84, 55 };

Gronsfield::Gronsfield() { }

inline void Gronsfield::decode(void\* data) {

static int i = 0;

i%=5;

uint8\_t r = \*((int\*)data) + key[i++];

\*((int\*)data) = r;

}

inline void Gronsfield::encode(void\* data) {

static int i = 0;

i%=5;

uint8\_t r = \*((int\*)data) - key[i++];

\*((int\*)data) = r;

}

// 4. Табличное шифрование

Tablet::Tablet() { }

const uint8\_t Tablet::table[256] = { 34, 50, 37, 129, 68, 251, 159, 147, 130, 145, 55, 153, 170, 205, 217, 72, 4, 51, 244, 146, 137, 167, 41, 250, 181, 240, 122, 178, 192, 124, 189, 195, 21, 242, 112, 121, 19, 107, 82, 25, 224, 148, 39, 17, 202, 57, 52, 154, 23, 155, 143, 190, 20, 234, 0, 218, 235, 200, 97, 71, 177, 74, 201, 172, 152, 80, 33, 7, 60, 253, 81, 119, 40, 111, 193, 239, 183, 207, 27, 125, 133, 123, 219, 213, 75, 56, 59, 241, 254, 30, 61, 255, 157, 160, 236, 194, 89, 228, 106, 141, 101, 163, 67, 38, 11, 100, 73, 65, 215, 144, 247, 196, 24, 70, 16, 211, 231, 180, 149, 93, 118, 36, 222, 86, 42, 83, 126, 139, 77, 66, 95, 5, 108, 94, 88, 32, 103, 233, 249, 162, 114, 214, 165, 173, 22, 131, 151, 48, 26, 232, 128, 46, 156, 79, 150, 223, 216, 203, 227, 185, 221, 191, 140, 92, 96, 1, 225, 187, 58, 78, 2, 109, 105, 18, 120, 243, 179, 9, 209, 238, 166, 54, 136, 115, 14, 85, 208, 169, 226, 76, 15, 206, 47, 63, 220, 174, 53, 64, 245, 117, 199, 90, 138, 104, 252, 182, 210, 229, 29, 84, 158, 28, 69, 188, 43, 113, 164, 87, 12, 168, 45, 134, 197, 31, 116, 132, 230, 44, 184, 171, 10, 142, 175, 6, 98, 212, 246, 237, 161, 3, 198, 248, 110, 176, 99, 135, 186, 8, 127, 91, 62, 102, 13, 49, 35, 204 };

inline void Tablet::decode(void\* data) {

uint8\_t r = \*((int\*)data);

int i = -1;

while(table[++i]!=r);

\*((int\*)data) = i;

}

inline void Tablet::encode(void\* data) {

uint8\_t r = \*((int\*)data);

\*((int\*)data) = table[r];

}

**Реализация канала двойной связи**

Если провести мысленный эксперимент, нетрудно догадаться, что одного файла не хватит, чтобы провести передачу данных синхронно. Потребуется как минимум два файла-канала, один будет выступать в роли прямого канала, другой – обратного.

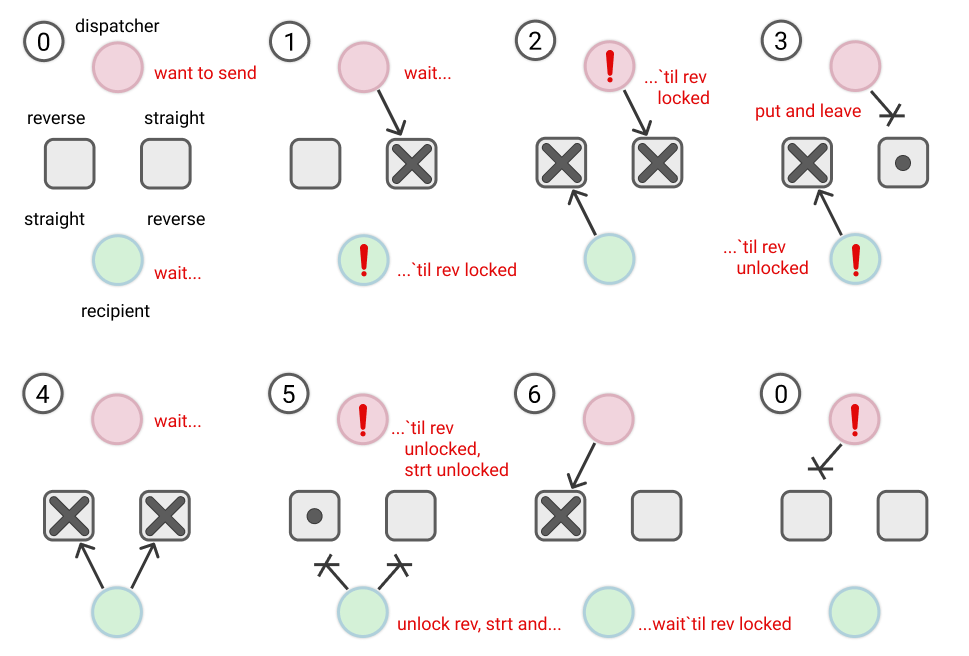
****

Рис.1 Единственный способ синхронной передачи данных через двойной канал

Имея возможности (реализованные в виде функций из библиотеки ниже) блокирования/разблокирования файла, чтения/записи(с блокировкой соответственно) и проверки, заблокирован ли файл, передачу организовать можно только изображенным на схеме образом.

UPD: Зачем передавать через файлы, ведь это можно сделать через localhost или разделяемую память? Это была первая идея. К тому же функции отправки можно заменить на использующие localhost, не трогая остальной код. Почти.

**Реализация блокировки файловых потоков**

// (locker.h)

#ifdef BUILD\_DLL

#define DLL\_EXPORT \_\_declspec(dllexport)

#else

#define DLL\_EXPORT \_\_declspec(dllimport)

#endif

#include <stdint-gcc.h>

#define EOF (-1)

enum WaitMode { OREV\_LOCKED=1, REV\_LOCKED=2, REV\_UNLOCKED=3, REV\_STRT\_UNLOCKED=5 };

#ifdef \_\_cplusplus

extern "C"

{

#endif

void DLL\_EXPORT init(const char\* straightChannel, const char\* inverseChannel);

int DLL\_EXPORT readByte(); /// only from reverse channel

int DLL\_EXPORT readBytes(void \*bytes, int cnt); /// only from reverse channel

void DLL\_EXPORT putByte(int data); /// only to straight channel

void DLL\_EXPORT putBytes(void \*bytes, int cnt); /// only to straight channel

void DLL\_EXPORT unlock\_straight\_channel();

void DLL\_EXPORT unlock\_reverse\_channel();

void DLL\_EXPORT lock\_reverse\_channel();

void DLL\_EXPORT lock\_straight\_channel();

void DLL\_EXPORT trylock\_reverse\_channel(); /// this function don`t tell, if file locked 100% probability

void DLL\_EXPORT trylock\_straight\_channel(); /// this function don`t tell, if file locked 100% probability

#ifdef \_\_cplusplus

}

#endif

// (locker.cpp)

#include "locker.h"

#include <stdio.h>

#include <share.h>

#include <string.h>

#include <errno.h>

static FILE \*stFile, \*invFile;

static char straightFilename[40] = {0}, inverseFilename[40] = {0};

void DLL\_EXPORT init(const char\* straight, const char\* inverse) {

int i = 0;

while(straight[i++]);

memcpy(straightFilename, straight, i);

i = 0;

while(inverse[i++]);

memcpy(inverseFilename, inverse, i);

fclose(fopen(straightFilename, "wb")), fclose(fopen(inverseFilename, "wb"));

}

void DLL\_EXPORT unlock\_straight\_channel() { fclose(stFile); }

void DLL\_EXPORT unlock\_reverse\_channel() { fclose(invFile); }

void DLL\_EXPORT lock\_reverse\_channel() {

do {

errno=0;

invFile = \_fsopen(inverseFilename, "rb", \_SH\_DENYRW);

} while(errno!=0);

}

void DLL\_EXPORT lock\_straight\_channel() {

do {

errno=0;

stFile = \_fsopen(straightFilename, "wb", \_SH\_DENYRW);

} while(errno!=0);

}

void DLL\_EXPORT trylock\_reverse\_channel() {

FILE \*f = \_fsopen(inverseFilename, "rb", \_SH\_DENYNO);

if(f) fclose(f), errno=0; /// anyway, fclose locks file

else errno=EACCES;

}

void DLL\_EXPORT trylock\_straight\_channel() {

FILE \*f = \_fsopen(straightFilename, "rb", \_SH\_DENYNO);

if(f) fclose(f), errno=0;

else errno=EACCES;

}

int DLL\_EXPORT readByte() {

do{ errno=0;

invFile = \_fsopen(inverseFilename, "rb", \_SH\_DENYRW);

}while(errno!=0);

int n = fgetc(invFile);

fgetc(invFile);

return feof(invFile) ? n : EOF;

}

int DLL\_EXPORT readBytes(void \*bytes, int cnt) {

do{ errno=0;

invFile = \_fsopen(inverseFilename, "rb", \_SH\_DENYRW);

}while(errno!=0);

for(int i = 0; i < cnt; i++) {

int n = fgetc(invFile);

if(feof(invFile)) return EOF;

\*((uint8\_t\*)bytes+i) = n;

}

return 0;

}

void DLL\_EXPORT putByte(int data) {

do{ errno=0;

stFile = \_fsopen(straightFilename, "wb", \_SH\_DENYRW);

}while(errno!=0);

if(0 <= data && data < 256)

fputc(data, stFile);

else if (data == EOF) {

fputc(0xff, stFile);

fputc(0x01, stFile);

}

}

void DLL\_EXPORT putBytes(void \*bytes, int cnt) {

do{ errno=0;

stFile = \_fsopen(straightFilename, "wb", \_SH\_DENYRW);

}while(errno!=0);

for(int i = 0; i < cnt; i++) {

fputc( \*((uint8\_t\*)bytes+i), stFile);

}

}

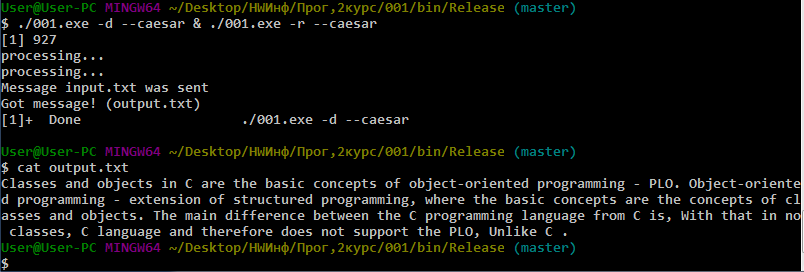
int \_\_attribute\_\_((\_\_stdcall\_\_)) DllMainCRTStartup(int hinstDLL, int fdwReason, void\* lpvReserved){

if(fdwReason == 0) remove(inverseFilename), remove(straightFilename);

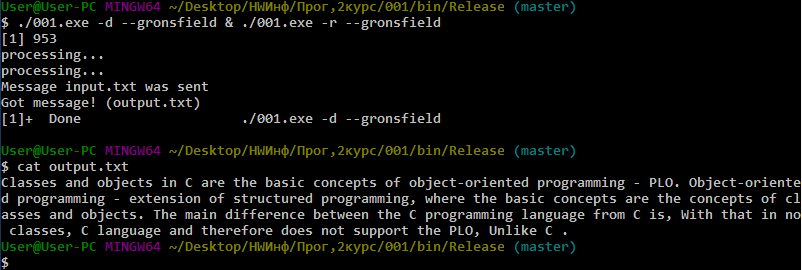
return 1;

}

**Результат работы программы:**

****

****

****

****