**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

**Цель работы:** Овладение основными криптографическими алгоритмами шифрования.

**Теоретический раздел**

Криптография - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Шифрованием называют процесс преобразования открытых данных в зашифрованные или зашифрованных данных в открытые по определенным правилам с применением ключей.

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

* отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
* отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
* получатель получает сообщение и расшифровывает его.

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

* шифры перестановки (transposition, permutation, P-блоки);
* шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Различают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы: моноалфавитные (код Цезаря) и полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

**Шифрование с помощью аффинной системы подстановок Цезаря**

В данном методе используется ключ шифрования в виде пары целых чисел (**A**, **K**). Число **A** задает переход при шифровании вперед на **A\*J** букв, а число **K** – дополнительное смещение по алфавиту на **K** букв. Следовательно, аффинную систему подстановок Цезаря можно описать следующей формулой:

(6.1)

где A>=0, K<M, НОД(A,M) = 1, I – значение кода символа в результирующей таблице, J – значение кода символа в исходной таблице.

Например, пусть M = 26, A = 3, K = 5. Тогда, очевидно, НОД (3,26) = 1, и мы получаем следующее соответствие между числовыми кодами букв:

Таблица 7.1– таблица кодов символов

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| J | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 3t+5 | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 1 | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 | 2 |

Преобразуя числа в буквы английского языка, получаем следующее соответствие для букв открытого текста и шифртекста:

Таблица 7.2– таблица символов

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| F | I | L | O | R | U | Х | А | D | G | J | М | Р | S | V | Y | В | Е | Н | K | N | Q | Т | W | Z | C |

Функция дешифровки выглядит следующим образом:

(6.2)

**Система Цезаря с ключевым словом**

Выберем некоторое число к, 0 **<= K <25** , и слово или корот­кую фразу в качестве ключевого слова. Желательно, чтобы все буквы ключевого слова были различными. Пусть выбраны слово DIPLOMAT в качестве ключевого слова и число **K = 5**. Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числом **К**:

Таблица 7.3– шифр Цезаря с ключевым словом

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| V | W | X | Y | Z | D | I | P | L | O | M | A | T | B | C | E | F | G | H | J | K | N | Q | R | S | U |

**Практический раздел**

**Генерация секретного ключа методом Диффи-Хелмана**

Пример генерации секретного ключа методом Диффи-Хелмана:

* p и g – простые числа;
* a – секретный ключ 1-го человека;
* b – секретный ключ 2-го человека;
* A – открытый ключ 1-го человека;
* B – открытый ключ 2-го человека;
* s – секретный ключ.

Решение задачи генерации секретного ключа данным методом представлен в таблице 7.1.

Таблица 7.4 – генерация ключа методом Диффи-Хелмана

|  |  |  |  |
| --- | --- | --- | --- |
| 1-й человек | | 2-й человек | |
| Знает | Не знает | Знает | Не знает |
| p = 10 | b = ? | p = 10 | a = ? |
| g = 7 | g = 7 |
| a = 18 | b = 4 |
| A = 718 mod 10 = 9 | A = 74 mod 10 = 1 |
| B = 7b mod 10 = 1 | B = 7a mod 10 = 9 |
| s = 16 mod 10 = 1 | s = 94 mod 10 = 1 |
| s = 1 | s =1 |

**Шифр Цезаря**

Необходимо зашифровать сообщение «хочузачётавтоматом» с использованием шифра Цезаря и секретного ключа, полученного при решении задачи из предыдущего подраздела. Исходный алфавит русского языка и его смещённый аналог представлены в таблице 7.2.

Таблица 7.5 – алфавит русского языка и его смещение на один символ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю |

Следовательно, сообщение «хочузачётавтоматом», зашифрованная с использованием шифра Цезаря и заданного ключа s=1, будет иметь следующий вид: «фнцтжяцесябснляснл».

**Программа генерации секретного ключа методом Диффи-Хелмана**

#include <iostream>

**int** power(**int** a, **int** b, **int** n);

**using** **namespace** std;

**int** main()

{

setlocale(LC\_ALL, "Rus");

**int** p, g, a, b, A, B, S1, S2;

cout << "Введите первое простое число: "; cin >> p;

cout << "Введите второе простое число: "; cin >> g;

cout << "Введите секретный ключ 1-го человека: "; cin >> a;

cout << "Введите секретный ключ 2-го человека: "; cin >> b;

A = power(g, a, p);

B = power(g, b, p);

cout << "Открытый ключ 1-го человека: "; cout << A;

cout << endl << "Открытый ключ 2-го человека: "; cout << B;

S1 = power(A, b, p);

S2 = power(A, b, p);

cout << endl << "Секретный ключ, полученный 1-м человеком: "; cout << S1;

cout << endl << "Секретный ключ, полученный 2-м человеком: "; cout << S2;

}

**int** power(**int** a, **int** b, **int** n)

{// a^b mod n

**int** tmp = a;

**int** sum = tmp;

**for** (**int** i = 1; i < b; i++) {

**for** (**int** j = 1; j < a; j++) {

sum += tmp;

**if** (sum >= n) {

sum -= n;

}

}

tmp = sum;

}

**return** tmp;

}

Листинг 7.1 – генерация секретного ключа методом Диффи-Хелмана

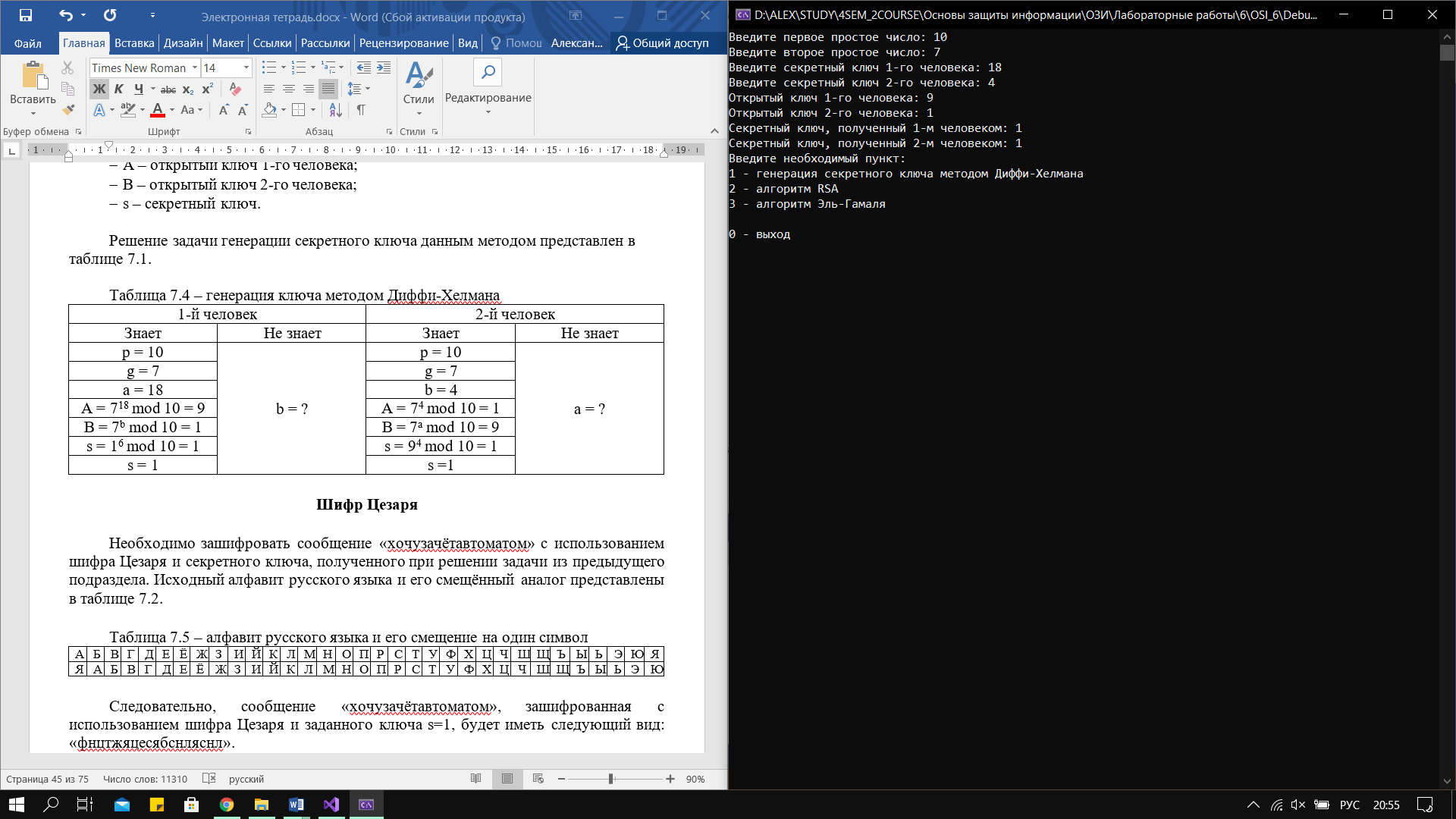


Рисунок 7.1 – результат работы программы

**Программа алгоритма RSA**

#include <iostream>

**template** <**typename** T>

T modpow(T base, T exp, T modulus);

**using** **namespace** std;

**int** main()

{

setlocale(LC\_ALL, "Rus");

**int** e, n, d; **int** text; **int** output, result;

cout << "Введите открытую экспоненту: "; cin >> e;

cout << "Введите модуль: "; cin >> n;

cout << "Введите секретную экспоненту: "; cin >> d;

cout << "Введите текст для шифрования: "; cin >> text;

output = modpow(text, e, n);

cout << "Зашифрованный текст: "; cout << output << endl;

result = modpow(output, d, n);

cout << "Расшифрованный текст: "; cout << result << endl;

}

**template** <**typename** T>

T modpow(T base, T exp, T modulus) {

base %= modulus;

T result = 1;

**while** (exp > 0) {

**if** (exp & 1) result = (result \* base) % modulus;

base = (base \* base) % modulus;

exp >>= 1;

}

**return** result;

}

Листинг 7.2 – алгоритм RSA

Таблица 7.1 – условие задания

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер варианта** | **e** | **n** | **d** |
| 9 | 17 | 493 | 369 |

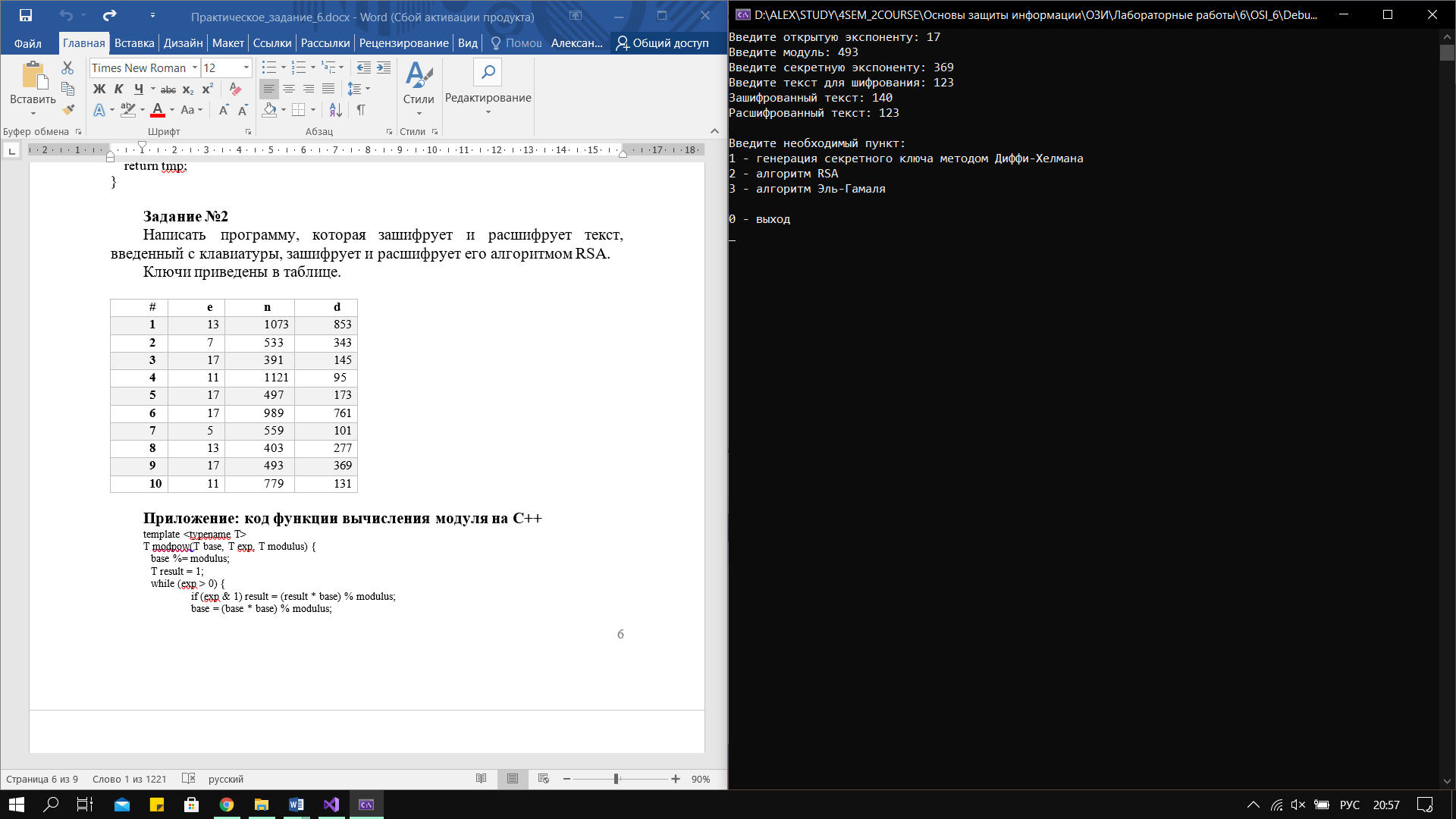


Рисунок 7.2 – результат работы программы

**Программа алгоритма Эль-Гамаля**

#include <iostream>

**using** **namespace** std;

**int** main()

{

setlocale(LC\_ALL, "Rus");

**int** p, g, x, b;

string inFileName = "D:\\ALEX\\STUDY\\4SEM\_2COURSE\\Основы защиты информации\\ ОЗИ \\Лабораторные работы\\6\\OSI\_6\\OSI\_6\\test.txt";

string outFileName = "D:\\ALEX\\STUDY\\4SEM\_2COURSE\\Основы защиты информации\\ ОЗИ \\Лабораторные работы\\6\\OSI\_6\\OSI\_6\\out.txt";

string result = "D:\\ALEX\\STUDY\\4SEM\_2COURSE\\Основы защиты информации\\ ОЗИ \\Лабораторные работы\\6\\OSI\_6\\OSI\_6\\result.txt";

srand(time(0));

p = 2 + rand() % 100;

g =1 + rand() % p;

cout << "Первый ключ p: "; cout << p << endl;

cout << "Второй ключ g : "; cout << g << endl;

x = 1 + rand() % p ;

cout << "Случайное число x (1<x<p): " << x << endl;

crypt(p, g, x, inFileName, outFileName);

decrypt(p, x, outFileName, result);

**break**;

}

**void** crypt(**int** p, **int** g, **int** x, string inFileName, string outFileName) {

ifstream inf(inFileName.c\_str());

ofstream outf(outFileName.c\_str());

**int** y = power(g, x, p);

cout << "Открытый ключ (p,g,y)=" << "(" << p << "," << g << "," << y << ")" << endl;

cout << "Закрытый ключ x=" << x << endl;

wcout << "Открытый ключ (p,g,y)=" << "(" << p << "," << g << "," << y << ")" << endl;

wcout << "Закрытый ключ x=" << x << endl;

wcout << "\nШифруемый текст:" << endl;

cout << "\nШифруемый текст:" << endl;

**while** (inf.good()) {

**int** m = inf.get();

**if** (m > 0) {

wcout << (**char**)m;

cout << (**char**)m;

**int** k = rand() % (p - 2) + 1; // 1 < k < (p-1)

**int** a = power(g, k, p);

**int** b = mul(power(y, k, p), m, p);

cout << "(" << a << "," << b << ")" << endl;

outf << a << " " << b << " " ;

}

}

wcout << endl;

inf.close();

outf.close();

}

**void** decrypt(**int** p, **int** x, string inFileName, string outFileName) {

ifstream inf(inFileName.c\_str());

ofstream outf(outFileName.c\_str());

cout << "\nДешифрованый текст:" << endl;

**while** (inf.good()) {

**int** a = 0;

**int** b = 0;

inf >> a;

inf >> b;

**if** (a != 0 && b != 0) {

//wcout<<a<<" "<<b<<endl;

Листинг 7.3 – алгоритм Эль-Гамаля

**int** deM = mul(b, power(a, p - 1 - x, p), p);// m=b\*(a^x)^(-1)mod p =b\*a^(p-1-x)mod p - трудно было найти нормальную формулу, в ней вся загвоздка

**char** m = **static\_cast**<**char**>(deM);

outf << m;

cout << m;

}

}

wcout << endl;

inf.close();

outf.close();

***}***

Листинг 7.3 – алгоритм Эль-Гамаля (продолжение)

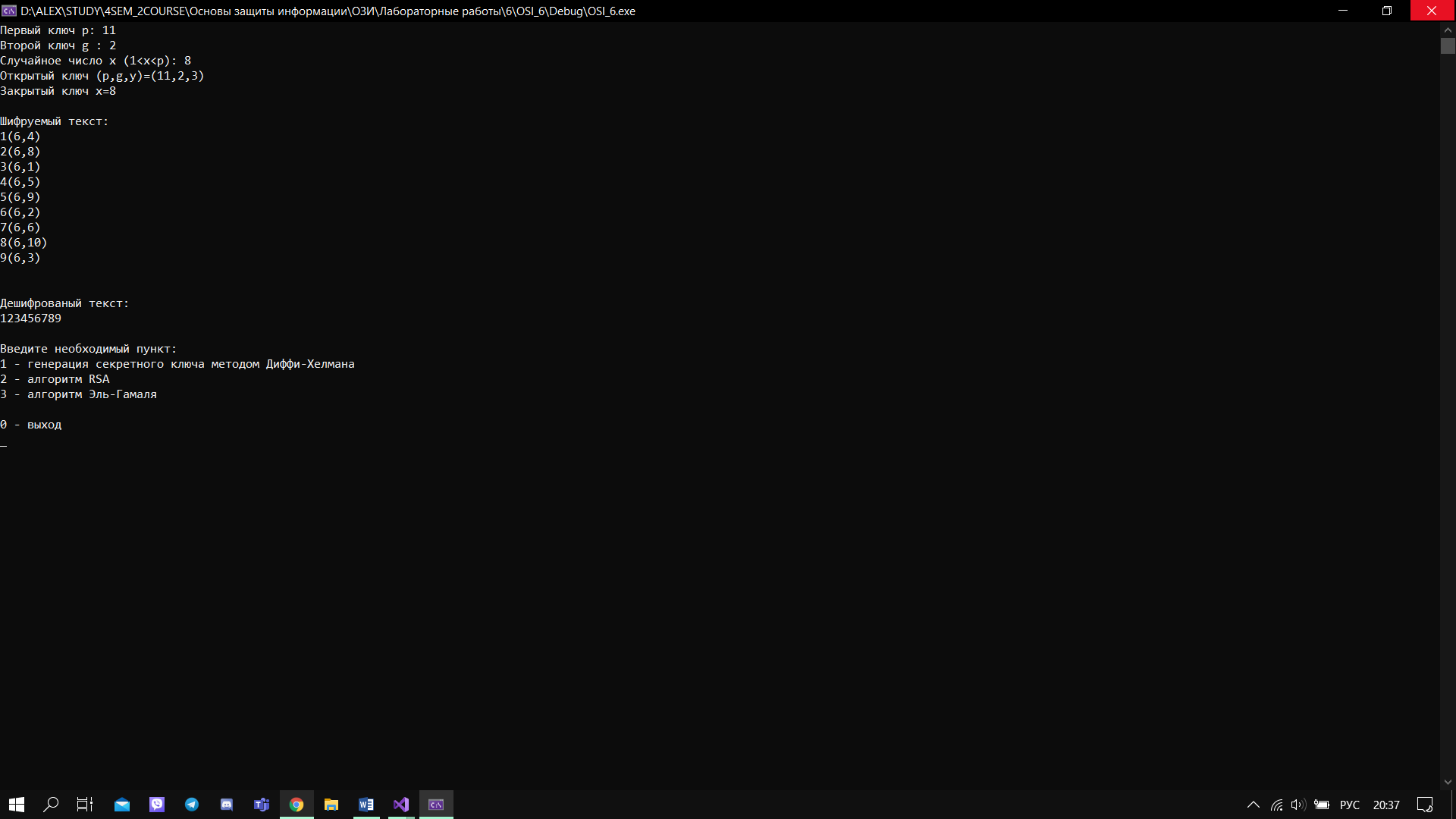


Рисунок 7.3 – результат работы программы

**Генерация ЭЦП**

int main()

{

int l = 1;

setlocale(LC\_ALL, "Rus");

SetConsoleCP(1251);

SetConsoleOutputCP(1251);

while (l != 0)

{

cout << endl << "Введите необходимый пункт: ";

cout << endl << "1 - генерация ЭЦП";

cout << endl << "0 - выход" << endl;

cin >> l;

system("cls");

switch (l)

{

case 1: {

int e, n,p,q, d; int text; int output, result;

cout << "Введите открытую экспоненту: "; cin >> e;

cout << "Введите первое простое число: "; cin >> p;

cout << "Введите второе простое число: "; cin >> q;

cout << "Введите число для шифрования: "; cin >> text;

n = p \* q;

d = (((p - 1) \* (q - 1)) - ((p-1)\*(q-1)/ e));

cout << "-------------------------" << endl;

cout << "Секретная экспонента: "; cout << d << endl;

cout << "Модуль: "; cout << n << endl;

cout << "-------------------------" << endl;

int H1, H2, S1, S2;

H1 = text / 5 \* 3;

cout << "Хеш-образ: "; cout << H1 << endl;

S1 = power(H1, d, n);

cout << "Сообщение для 2-го человека (исходное сообщение; ЭЦП): "; cout << '(' << text << ';' << S1 << ')' << endl;

H2 = text / 5 \* 3;

S2 = power(S1, e, n);

cout << "Вычисленное значение из хеш-образа: "; cout << S2 << endl;

break;

}

default: break;

}

}

}

int power(int a, int b, int n)

{// a^b mod n

int tmp = a;

int sum = tmp;

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

for (int j = 1; j < a; j++) {

sum += tmp;

if (sum >= n) {

sum -= n;

}

}

tmp = sum;

}

return tmp;

}

template <typename T>

T modpow(T base, T exp, T modulus) {

base %= modulus;

T result = 1;

while (exp > 0) {

if (exp & 1) result = (result \* base) % modulus;

base = (base \* base) % modulus;

exp >>= 1;

}

return result;

}

Листинг 7.4 – генерация ЭЦП

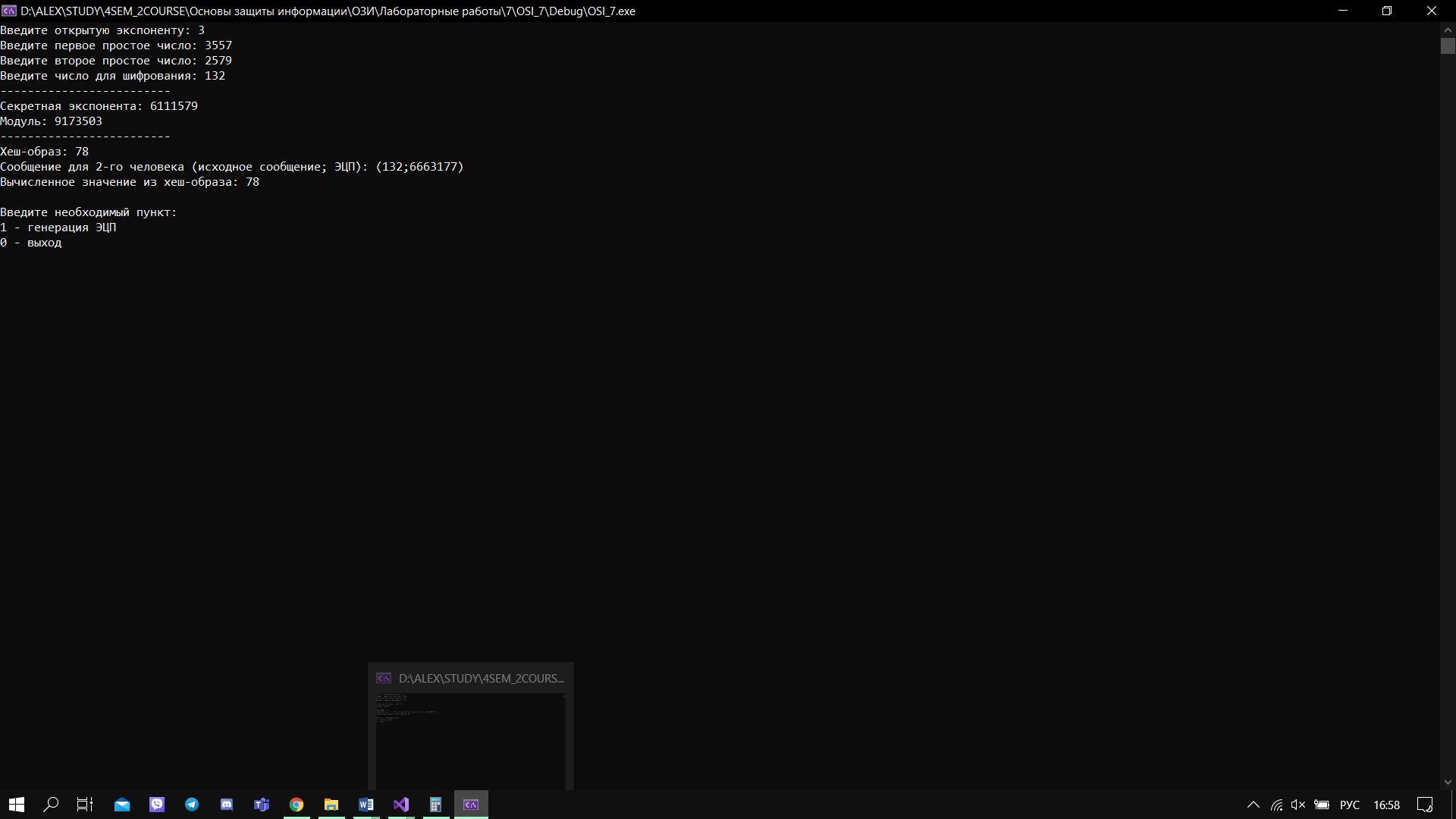


Рисунок 7.4 – результат работы программы

**Вывод:** было изучено понятие криптографии. Получены знания об основных криптографических алгоритмах шифрования, а также на практике продемонстрированы знания алгоритма Диффи-Хелмана и шифра Цезаря.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

**Цель работы:** Овладение навыками работы с известными криптографическими алгоритмами.

**Теоретический раздел**

Несмотря на достаточно большое число различных систем с открытыми ключами, одной из наиболее популярных остается криптосистема RSA.

Рассмотрим математические результаты, которые положены в основу этого алгоритма.

Определение 1. Сравнением целых чисел a и b будем называть соотношение между ними вида a = b + mk, означающее, что их разность (a – b) делится на заданное положительное число m, называемое модулем сравнения. При этом а называется вычетом числа b по модулю m.

Определение 2. Говорят, что два целых числа a и b сравнимы между собой и обозначают этот факт через a = b (mod m), если a и b имеют одинаковые остатки при делении на m.

Определение 3. Функцией Эйлеpа Ф(n) называется число положительных целых, меньших n и простых относительно числа n.

Теорема 1. (Малая теорема Ферма). Если p – простое число, то (x в степени (p – 1)) = 1 (mod p) для любого х, простого относительно p, и (x в степени p) = х (mod p) для любого х.

Теорема 2. Если n = pq, (p и q – отличные друг от друга простые числа), то Ф(n) = (p – 1)(q – 1).

Теорема 3. Если n = pq, (p и q – отличные друг от друга простые числа) и х – простое относительно p и q, то (x в степени Ф(n)) = 1 (mod n).

Итак, в реальных системах RSA реализуется следующим образом:

Каждый пользователь выбирает два больших простых числа p и q, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d; как результат умножения первых двух чисел устанавливается n. После этого {e, n} образует открытый ключ, а {d, n} – секретный (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно дешифровать с помощью открытого ключа. Владелец же секретного ключа без труда может pасшифpовать принятое сообщение.

**Практический раздел**

Необходимо осуществить шифрование сообщения с использованием ключей RSA.

**Вариант 15**

Таблица 8.1 – условия задачи

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Сообщение | p | q |
| 15 | DAA | 59 | 43 |

Данные *p* и *q* – два простых числа. Необходимо вычислить их произведение: *n = p \* q = 43 \* 59 = 2537*. Следующим шагом необходимо вычислить функцию Эйлера: *φ(n) = (59-1)\*(43-1) = 2436*. Функция Эйлера определяет количество целых положительных чисел, не превосходящих n и взаимно простых с *n*. Целые числа называются взаимно простыми, если они не имеют никаких общих делителей, кроме *1*.

Далее необходимо выбрать произвольное целое число *0 < е < n* взаимно просто с полученным значением функции Эйлера. Возьмём *e = 5*. Пара чисел *(e,n)* объявляется открытым ключом шифра. В нашем случае *(e,n) = (5,2537).*

После, вычисляется числа *d* (обратное число по модулю от *е*) по формуле:

(8.1)

Необходимо придавать *k* последовательно значения *1,2,3,..* до тех пор, пока не будет получено целое число *d:*

487,4; k = 1;

974,6; k = 2;

1 461,8; k = 3;

1 949; k = 4;

Таким образом,  *= 1949*.

RSA-шифрование сообщения T выполняется с помощью открытого ключа получателя (e, n) по формуле:

(8.2)

где Ti и Ci числовые эквиваленты символов исходного и зашифрованного сообщений (см. табл. 8.2 и 8.3).

Таблица 8.2 – числовые эквиваленты русских букв, цифр и символа пробела

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** | **34** | **35** | **36** | **37** | **38** | **39** | **40** | **41** | **42** | **43** | **44** |
| Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | пробел | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **65** | **66** | **67** | **68** | **69** | **70** | **71** | **72** | **73** | **74** | **75** | **76** | **77** | **78** | **79** | **80** | **81** | **82** | **83** | **84** | **85** | **86** | **87** | **88** | **89** |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Таблица 8.3 – Числовые эквиваленты латинских букв

Произведём вычисление шифрограммы (с открытым ключом (5,2537)):

Таблица 8.4 – Вычисление шифрограммы

|  |  |  |
| --- | --- | --- |
| Символ исходного сообщения, | Коды символов | Зашифрованные коды символов |
| D | 68 | 685 mod 2537 = 1701 |
| A | 65 | 655 mod 2537 = 1286 |
| A | 65 | 655 mod 2537 = 1286 |

Таким образом, исходное сообщение в виде шифрограммы представляет из себя следующую последовательность чисел: «1701,1286,1286».

Расшифровка RSA-закодированного сообщения T выполняется с помощью закрытого ключа получателя *(d, n)* по формуле:

(8.3)

Произведём вычисление шифрограммы (с закрытым ключом (1 949,2537)):

Таблица 8.4 – Вычисление шифрограммы

|  |  |  |
| --- | --- | --- |
| Зашифрованные коды символов | Дешифрованные коды символов | Зашифрованные коды символов |
| 1701 | 17011949 mod 2537 = 68 | D |
| 1286 | 12861949 mod 2537 = 65 | A |
| 1286 | 12861949 mod 2537 = 65 | A |

Таким образом, было восстановлено сообщение «DAA».

**Шифр Цезаря**

Необходимо зашифровать сообщение «ковалевалександралександрович» с использованием шифра Цезаря и секретного ключа «1».Исходный алфавит русского языка и его смещённый аналог представлены в таблице 8.5.

Таблица 8.5 – алфавит русского языка и его смещение на один символ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю |

Следовательно, сообщение «ковалевалександралександрович», зашифрованная с использованием шифра Цезаря и заданного ключа s=1, будет иметь следующий вид: «йнбякдбякдйрямгпкдйрямгпнбзц».

**Шифр Тритемиуса**

Уравнение зашифрования для шифра Тритемиуса имеет следующий вид:

(8.4)

Некоторые варианты вычисления шага смещения k:

(8.5)

(8.6)

Алгоритм шифрования с использованием системы Трисемуса:

1. Определяем порядковый номер шифруемой буквы в тексте.
2. Определяем код буквы в алфавите.
3. Вычисляем смещение k.
4. Находим код зашифрованной буквы, пользуясь нашим уравнением зашифрования.
5. По коду L восстанавливаем очередную букву криптограммы.
6. Повторяем пункты 1..5 до окончания текста шифрограммы.

Для (k=2p^2+5p+3) и русского алфавита:

Таблица 8.6 – алфавит русского языка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Следовательно, сообщение «ковалевалександралександрович», зашифрованная с использованием шифра Тритемиуса, будет иметь следующий вид: «ёщвапувма.кп, ывамцукйё.цуавысм».

**Шифр Плейфера**

Таблица 8.7 – матрица символов

|  |  |  |  |
| --- | --- | --- | --- |
| З | А | Щ | И |
| Т | Б | В | Г |
| Д | Е | Ж | Й |
| К | Л | М | Н |
| О | П | Р | С |
| У | Ф | Х | Ц |
| Ч | Ш | Ъ | Ы |
| Ь | Э | Ю | Я |

Сообщение «ковалевалександралександрович», разбитое на биграммы: «ко ва ле ва ле кс ан др ал ек са нд ро ви чъ».

Зашифрованное сообщение: «ОУ БЩ ПЛ БЩ ПЛ НО ИЛ ЖО БП ДЛ ПИ КЙ СП ГЩ ШЫ».

**Шифр Вижинера**

Таблица 8.7 – матрица символов русского языка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** | **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **А** | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| **Б** | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А |
| **В** | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б |
| **Г** | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В |
| **Д** | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г |
| **Е** | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д |
| **Ё** | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е |
| **Ж** | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё |
| **З** | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж |
| **И** | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З |
| **Й** | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И |
| **К** | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й |
| **Л** | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К |
| **М** | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л |
| **Н** | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М |
| **О** | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н |
| **П** | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О |
| **Р** | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |
| **С** | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р |
| **Т** | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С |
| **У** | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т |
| **Ф** | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У |
| **Х** | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| **Ц** | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| **Ч** | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц |
| **Ш** | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч |
| **Щ** | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш |
| **Ъ** | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ |
| **Ы** | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ |
| **Ь** | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы |
| **Э** | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь |
| **Ю** | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э |
| **Я** | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю |

Таблица 8.8 – шифруемое сообщение и ключ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| К | О | В | А | Л | Е | В | А | Л | Е | К | С | А | Н | Д | Р | А | Л | Е | К | С | А | Н | Д | Р | О | В | И | Ч |
| З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З | А | Щ | И | Т | А | З | А | Щ | И | Т |

Зашифрованное сообщение будет иметь следующий вид: «ЩОЫИЮУЙАЕНЭСНЭШТЛМККИАДШОЫСЙ.»

**Расшифровка сообщения**

Таблица 8.8 – условие задания

|  |  |  |
| --- | --- | --- |
| № | Сообщение | Способ |
| 15. | **\_ \_еоовипи\_ \_ \_ы\_о\_ввв\_тттыыытуоо\_ \_ \_атмтерем\_у,сес,б\_ \_тшт \_ычкьиьгттт,л,дь** | Расшифровать с помощью **Одиночной перестановки по ключу.**  **Ключ – ФЕВРАЛЬ Таблица 10х7** |

Таблица 8.9 – зашифрованное сообщение

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ф** | **Е** | **В** | **Р** | **А** | **Л** | **Ь** |
| **6** | **3** | **2** | **5** | **1** | **4** | **7** |
| ­– | – | е | о | о | в | и |
| п | и | – | ы | – | о | – |
| в | в | в | – | т | т | т |
| ы | ы | ы | т | к | о | о |
| – | – | – | а | т | м | т |
| е | р | е | м | – | у | , |
| с | е | с | , | б | – | – |
| т | ш | т | – | ы | ч | к |
| ь | и | ь | г | т | т | т |
| , | л | , | д | ь | – | – |

Таблица 8.9 – расшифрованное сообщение

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **А** | **В** | **Е** | **Л** | **Р** | **Ф** | **Ь** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| о | е | – | в | о | ­– | и |
| – | – | и | о | ы | п | – |
| т | в | в | т | – | в | т |
| к | ы | ы | о | т | ы | о |
| т | – | – | м | а | – | т |
| – | е | р | у | м | е | , |
| б | с | е | – | , | с | – |
| ы | т | ш | ч | – | т | к |
| т | ь | и | т | г | ь | т |
| ь | , | л | – | д | , | – |

**Вывод:** были изучены основные теоретические знание по известным криптографическим алгоритмам и получены практические навыки работы с алгоритмом шифрования RSA.