Министерство образования республики Беларусь

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Индивидуальная работа №2

по дисциплине «Методы защиты информации»

Студент 4 курса

Группы № 493551

Рыбак Артем Владимирович

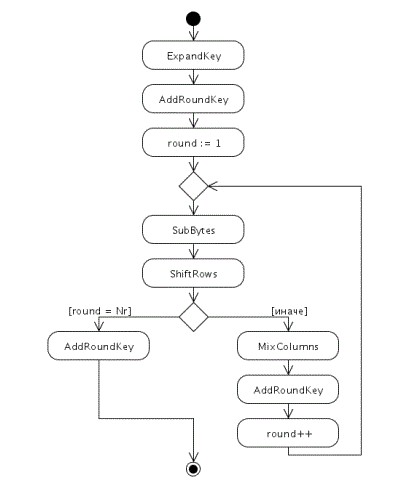
Минск, 2018

**Введение**

Практическая работа № 2 подразумевает реализацию алгоритма асимметричного шифрования RSA.

Целью работы является создание программы шифрования, осуществляющей криптографическое преобразование введенного текста с помощью алгоритма асимметричного шифрования RSA.

**Блок-схема алгоритма**



**Результаты ввода данных и исполнения программы**

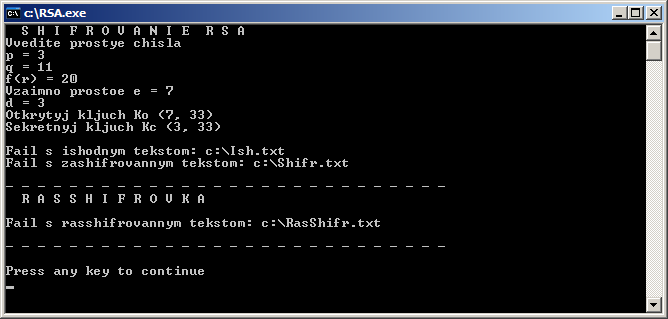


Рисунок 1 ‑ Работа программы

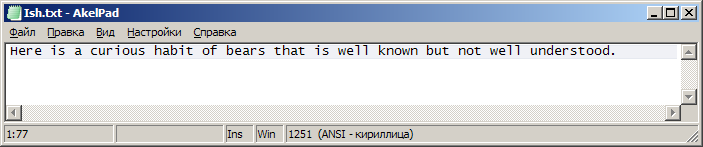


Рисунок 2 ‑ Исходный текст



Рисунок 3 ‑ Зашифрованный текст

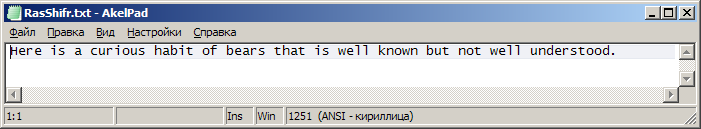


Рисунок 4 ‑ Расшифрованный текст

**Программный код**

*#include <conio.h>*

*#include <stdio.h>*

*#include <string.h>*

*#include <fstream.h>*

*char \*TextFile = "c:\\Work\\Text.txt";*

*char \*EncryptFile = "c:\\Work\\Encrypt.txt";*

*char \*DecryptFile = "c:\\Work\\Decrypt.txt";*

*unsigned long x1, Y1, p, q, e, r;*

*char \*simv = "ABCDHabcdefghijklmnopqrstuvwxyz .";*

*void main(void)*

*{*

*unsigned long fr, d;*

*int i, j, k;*

*cout << "Enter simply number \n";*

*cout << "p = "; cin >> p;*

*if (p < 1) {*

*p = 3;*

*printf("p < 1. => p = %d", p);*

*}*

*cout << "q = "; cin >> q;*

*if (q < 1) {*

*q = 11;*

*printf("q < 1. q = %d", q);*

*}*

*r = p \* q;*

*fr = (p - 1) \* (q - 1);*

*cout << "f(r) = " << fr << endl;*

*e = 7;*

*cout << "e = " << e << endl;*

*EvklidMethod(fr, e);*

*if (Y1 < 0)*

*Y1 += fr;*

*d = Y1;*

*cout << "d = " << d << endl;*

*cout << "Open kKey Ko (" << e << ", " << r << ")" << endl;*

*cout << "Secret Key Kc (" << d << ", " << r << ")" << endl;*

*cout << "\nText = : " << TextFile << endl;*

*encryptMethod();*

*cout << "Fail Encrypt text =: " << EncryptFile << endl;*

*decryptMethod(d);*

*cout << "Decrypt text = : " << DecryptFile << endl;*

*cout << "\nPress any key to continue" << endl;*

*getch();*

*}*

*unsigned long mod(unsigned long a, unsigned long n)*

*{*

*unsigned long q;*

*q = a % n;*

*if (q < 0) q += n;*

*return q;*

*}*

*void EvklidMethod(unsigned long a, unsigned long n)*

*{*

*int i;*

*unsigned long u[3], v[3], t[3], q;*

*u[0] = 0; u[1] = 1; u[2] = n;*

*v[0] = 1; v[1] = 0; v[2] = a;*

*t[0] = 0; t[1] = 0; t[2] = 0;*

*while (u[2] != 1)*

*{*

*q = u[2] / v[2];*

*for (i = 0; i<3; i++)*

*t[i] = u[i] - v[i] \* q;*

*for (i = 0; i<3; i++)*

*{*

*u[i] = v[i];*

*v[i] = t[i];*

*}*

*}*

*x1 = u[0];*

*Y1 = u[1];*

*}*

*int speedPow(unsigned long a, unsigned long k, unsigned long n)*

*{*

*unsigned long b;*

*b = 1;*

*while (k != 0)*

*{*

*if (k % 2 == 0)*

*{*

*k /= 2;*

*a = mod((a\*a), n);*

*}*

*else*

*{*

*k--;*

*b = mod((b\*a), n);*

*}*

*}*

*return b;*

*}*

*void encryptMethod(void)*

*{*

*char ch;*

*unsigned long i;*

*FILE \*f\_t, \*file2;*

*f\_t = fopen(TextFile, "r");*

*file2 = fopen(EncryptFile, "w");*

*while (fscanf(f\_t, "%c", &ch) != EOF)*

*for (i = 0; i < strlen(simv); i++)*

*if (simv[i] == ch)*

*fprintf(file2, "%d ", speedPow(i, e, r));*

*fclose(f\_t);*

*fclose(file2);*

*}*

*void decryptMethod(unsigned long d)*

*{*

*unsigned long j;*

*FILE \*fi, \*fo;*

*fi = fopen(EncryptFile, "r");*

*fo = fopen(DecryptFile, "w");*

*while (fscanf(fi, "%d", &j) != EOF) {*

*fprintf(fo, "%c", simv[speedPow(j, d, r)]);*

*}*

*fclose(fo);*

*fclose(fi);*

*}*

**Вывод**

Система RSA используется для защиты программного обеспечения и в схемах цифровой подписи.

Также она используется в открытой системе шифрования PGP и иных системах шифрования (к примеру, DarkCryptTC и формат xdc) в сочетании с симметричными алгоритмами.

Из-за низкой скорости шифрования (около 30 кбит/с при 512 битном ключе на процессоре 2 ГГц), сообщения обычно шифруют с помощью более производительных симметричных алгоритмов со случайным сеансовым ключом (например, AES, IDEA, Serpent, Twofish), а с помощью RSA шифруют лишь этот ключ, таким образом реализуется гибридная криптосистема. Такой механизм имеет потенциальные уязвимости ввиду необходимости использовать криптографически стойкий генератор псевдослучайных чисел для формирования случайного сеансового ключа симметричного шифрования.