Учреждение образования

«Минский государственный колледж цифровых технологий»

Учебный предмет

«Защита компьютерной информации»

Отчет

по лабораторной работе №6

Тема «Исследование ассиметричных криптоалгоритмов»

|  |  |
| --- | --- |
| Выполнил:  учащийся 82ТП | Шатуха А.К. |
| Проверил:  преподаватель | Оскерко В.С. |

Минск, 2024

**Цель**: **Изучить и закрепить умение реализации криптосистемы RSA и криптосистемы Эль-Гамаля.**

**Порядок выполнения работы:**

1. Изучить теоретический материал
2. Выбрать язык программирования
3. Выполнить практическую часть.
4. Оформить отчет.

**Практическая часть**

**Задание №1**

Написать программу которая зашифрует и расшифрует текст введенный с клавиатуры, зашифрует и расшифрует его алгоритмом RSA.

Числа p и q выбрать самим.

#include <iostream>

#include <string>

#include <cmath>

using namespace std;

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

base %= modulus;

long long result = 1;

while (exp > 0) {

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

base = (base \* base) % modulus;

exp >>= 1;

}

return result;

}

string encryptRSA(string text, long long e, long long n) {

string encryptedText = "";

for (char c : text) {

long long m = c;

long long encryptedChar = modpow(m, e, n);

encryptedText += to\_string(encryptedChar) + " ";

}

return encryptedText;

}

string decryptRSA(string encryptedText, long long d, long long n) {

string decryptedText = "";

size\_t pos = 0;

while ((pos = encryptedText.find(" ")) != string::npos) {

long long encryptedChar = stoll(encryptedText.substr(0, pos));

long long decryptedChar = modpow(encryptedChar, d, n);

decryptedText += char(decryptedChar);

encryptedText.erase(0, pos + 1);

}

return decryptedText;

}

int main() {

setlocale(LC\_ALL, "ru");

long long p = 61;

long long q = 53;

long long n = p \* q;

long long m = (p - 1) \* (q - 1);

long long e = 17;

long long d = 2753;

string text;

cout << "Введите текст для шифрования: ";

getline(cin, text);

string encryptedText = encryptRSA(text, e, n);

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

string decryptedText = decryptRSA(encryptedText, d, n);

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

return 0;

}

В отчете должно сдержаться код программы, полученные результаты.

**Задание №2**

Написать программу которая сгенерирует ключи, зашифрует и расшифрует текст введенный с клавиатуры алгоритмом Эль-Гамаля.

#include <iostream>

#include <string>

#include <cmath>

#include <ctime>

#include <cstdlib>

using namespace std;

bool isPrime(long long number) {

if (number <= 1) return false;

for (long long i = 2; i \* i <= number; i++) {

if (number % i == 0) return false;

}

return true;

}

long long generatePrimeNumber() {

srand((unsigned int)time(0));

long long primeNumber;

do {

primeNumber = (rand() % 1000) + 100;

} while (!isPrime(primeNumber));

return primeNumber;

}

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

base %= modulus;

long long result = 1;

while (exp > 0) {

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

base = (base \* base) % modulus;

exp >>= 1;

}

return result;

}

string encryptElGamal(string text, long long p, long long g, long long y, long long k) {

string encryptedText = "";

for (char c : text) {

long long m = c;

long long c1 = modpow(g, k, p);

long long c2 = (m \* modpow(y, k, p)) % p;

encryptedText += to\_string(c1) + " " + to\_string(c2) + " ";

}

return encryptedText;

}

string decryptElGamal(string encryptedText, long long p, long long x) {

string decryptedText = "";

size\_t pos = 0;

while ((pos = encryptedText.find(" ")) != string::npos) {

long long c1 = stoll(encryptedText.substr(0, pos));

encryptedText.erase(0, pos + 1);

pos = encryptedText.find(" ");

long long c2 = stoll(encryptedText.substr(0, pos));

encryptedText.erase(0, pos + 1);

long long m = (c2 \* modpow(modpow(c1, x, p), p - 2, p)) % p;

decryptedText += char(m);

}

return decryptedText;

}

int main() {

setlocale(LC\_ALL, "ru");

long long p = generatePrimeNumber();

long long g = 2;

long long x = 10;

long long y = modpow(g, x, p);

string text;

cout << "Введите текст для шифрования: ";

getline(cin, text);

long long k = 5;

string encryptedText = encryptElGamal(text, p, g, y, k);

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

string decryptedText = decryptElGamal(encryptedText, p, x);

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

return 0;

}

**Контрольные вопросы:**

* + 1. Дать определение понятию «Ассиметричный криптоалгоритм»

Ассиметричный криптоалгоритм - это тип криптоалгоритма, который использует два различных ключа для шифрования и дешифрования данных.

* + 1. Описать принцип крипросистемы RSA

 Крипросистема RSA - это один из наиболее широко используемых ассиметричных криптоалгоритмов. Принцип работы RSA основан на математической задаче факторизации больших чисел.

* + 1. Описать принцип крипросистемы Эль-Гамаля

Крипросистема Эль-Гамаля - это еще один ассиметричный криптоалгоритм, который основан на математической задаче дискретного логарифма. Алгоритм Эль-Гамаля использует два ключа: открытый ключ для шифрования и закрытый ключ для дешифрования.

* + 1. Описать зашифровку текста алгоритмом Эль-Гамаля

Сначала выбирается открытый ключ, состоящий из числа p и числа g.

Затем выбирается случайное число k, которое используется для шифрования.

Каждый символ текста преобразуется в число m.

Затем вычисляются два числа: c1 = g^k mod p и c2 = m \* y^k mod p, где y = g^x mod p.

Зашифрованный текст представляет собой последовательность пар чисел (c1, c2).

* + 1. Описать расшифровку текста алгоритмом Эль-Гамаля

Сначала выбирается закрытый ключ, состоящий из числа x.

Затем для каждой пары чисел (c1, c2) в зашифрованном тексте вычисляется число m = c2 \* (c1^x)^(-1) mod p.

Число m преобразуется в символ текста.

Таким образом, расшифрованный текст представляет собой исходный текст.