**Лабораторная Работа №3**

**По дисциплине Защита Информации**

**Студента группы ПА-16-2**

**Гончарова Ярослава**

**GitHub проекту:** <https://github.com/rasklif/Gost28147Lab>

Припустимо, що користувач А хоче передати користувачеві В

повідомлення в зашифрованому вигляді, використовуючи алгоритм RSA. У

такому випадку користувач А виступає в ролі відправника повідомлення, а

користувач В - в ролі одержувача. Як зазначалося вище, криптосистему RSA

повинен сформувати одержувач повідомлення, тобто користувач В.

Розглянемо послідовність дій користувачів В і А:

1. Користувач В вибирає два довільних великих простих числа Р і

Q.

2. Користувач В обчислює значення модуля N = P \* Q.

3. Користувач В обчислює функцію Ейлера

φ (N) = (P-1) \* (Q-1)

і вибирає випадковим чином значення відкритого ключа K з

урахуванням виконання умов

1 &lt;K≤φ (N), НСД (K, φ (N)) = 1.

4. Користувач В обчислює значення секретного ключа k,

використовуючи розширений алгоритм Евкліда при вирішенні порівняння

що k \* K≡1 (mod φ (N)).

int p = rand() % 100;

int q = rand() % 100;

int p\_simple = sundaram(p);

int q\_simple = sundaram(q);

//Находим число n.

unsigned int n = p\_simple \* q\_simple;

//Генерация числа d и проверка его на взаимопростоту

//с числом ((p\_simple-1)\*(q\_simple-1)).

int d, d\_simple = 0;

while (d\_simple != 1)

{

d = rand() % 100;

d\_simple = gcd(d, ((p\_simple - 1)\*(q\_simple - 1)));

}

//Определение числа e, для которого является истинным

//соотношение (e\*d)%((p\_simple-1)\*(q\_simple-1))=1.

unsigned int e = 0, e\_simple = 0;

while (e\_simple != 1)

{

e += 1;

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

}

5. Користувач В пересилає користувачеві А пару чисел по

незащіщенному каналу (N, K).

Якщо користувач А хоче передати користувачеві В повідомлення М.

він виконує наступні кроки:

6. Користувач А розбиває вихідний відкритий текст М на блоки,

кожен з яких може бути представлений у вигляді числа M = 0, 1, 2, ... N-1

7. Користувач A шифрує текст, представлений у вигляді

послідовності чисел М. за формулою

C = MK (mod N) і відправляє криптограму C1, C2, ... користувачу В.

b = 301;

int m;

for (int j = 0; j < MAX; j++)

{

c = 1;

unsigned int i = 0;

int ASCIIcode = (static\_cast<int>(Text[j])) + b;

while (i < e)

{

c = c \* ASCIIcode;

c = c % n;

i++;

}

CryptoText[j] = c;

b += 1;

}

Користувач В розшифровує прийняту криптограму

використовуючи секретний ключ k за формулою

M = Ck (mod N).

b = 301;

int m;

for (int j = 0; j < MAX; j++)

{

m = 1;

unsigned int i = 0;

while (i < d)

{

m = m \* CryptoText[j];

m = m % n;

i++;

}

m = m - b;

Tdecrypt[j] = m;

b += 1;

}

В результаті буде отримана послідовність чисел М, які представляють

собою вихідне повідомлення М.

Приклад праці розробленоі программи:

