Министерство образования Республики Беларусь
Учреждение образования “Белорусский государственный университет информатики и радиоэлектроники”

Факультет компьютерных систем и сетей
Кафедра информатики
Дисциплина «Методы защиты информации»

Отчет
к лабораторной работе №4

Выполнил:
студент гр.653501
Тимофеев К. А.

Проверил:
Артемьев В.С.

Минск, 2019

Введение

В лабораторной работе необходимо было реализовать алгоритм ElGamal. Схема Эль-Гамаля (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Генерация ключей

1. Генерируется случайное простое число p.
2. Выбирается число g – первообразный корень.
3. Выбирается случайное число x такое, что $1 < x < p - 1$.
4. Вычисляется $y = g^x \bmod p$.
5. Открытым ключом является y, закрытым ключом – число x.

Шифрование

M – сообщение.

1. Выбирается сессионный ключ - случайное целое число k такое, что $1 < k < p – 1$.
2. Вычисляются число $a = g \bmod p$.
3. Вычисляется число b = y Mmod p.
4. Пара чисел (a, b) является шифротекстом.

Расшифрование

Зная закрытый ключ, можно вычислить текст по шифротексту по формуле: $M = ba \bmod p$.

Блок-схема алгоритма

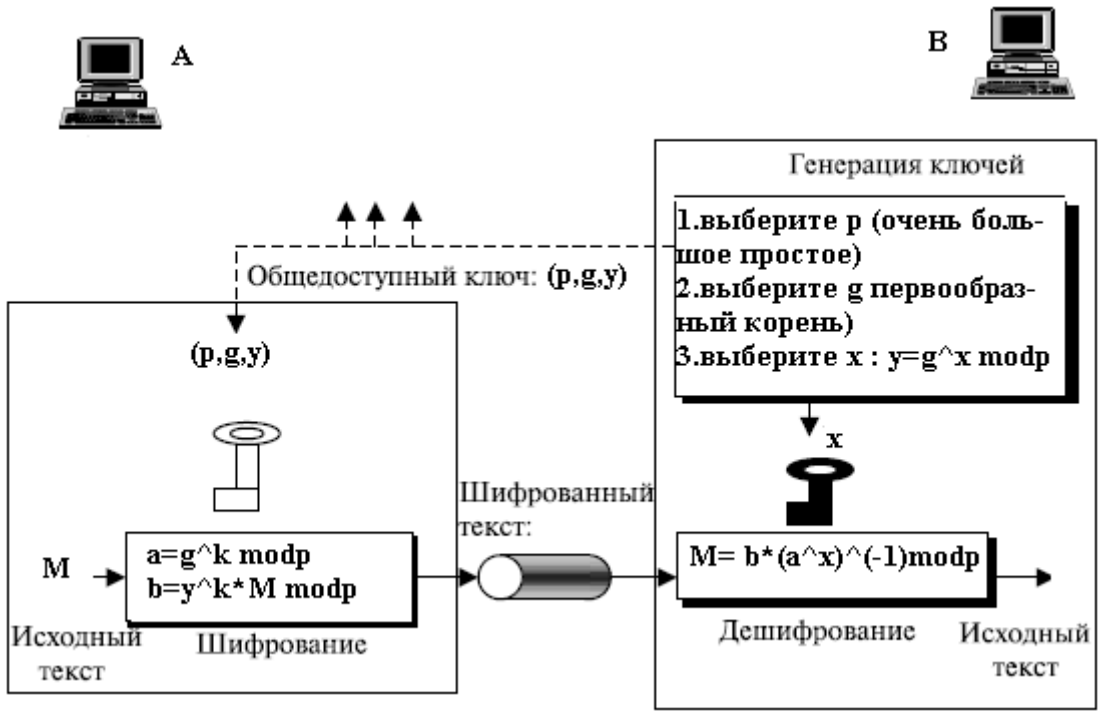

Рис.1 Блок-схема алгоритма

```
key: p = 45197, g = 2, y = 3287, x = 31944
source: 40033
cipher: (32509, 35726)
decrypted: 40033
```

Рис.2 Результат ввода данных и исполнения программы

Вывод

В настоящее время криптосистемы с открытым ключом считаются наиболее перспективными. К ним относится и схема Эль-Гамаля, криптостойкость которой основана на вычислительной сложности проблемы дискретного логарифмирования, где по известным *p*, *g* и *y* требуется вычислить *x*, удовлетворяющий сравнению:

y ≡ g^x (mod p)

ГОСТ Р34.10-1994, принятый в 1994 году в Российской Федерации, регламентировавший процедуры формирования и проверки электронной цифровой подписи, был основан на схеме Эль-Гамаля. С 2001 года используется новый ГОСТ Р 34.10-2001, использующий арифметику эллиптических кривых, определенных над простыми полями Галуа. Существует большое количество алгоритмов, основанных на схеме Эль-Гамаля: это алгоритмы DSA, ECDSA, KCDSA, схема Шнорра.