МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ имени

Кафедра IT - Инжиниринг

**ЛАБОРАТОРНАЯ РАБОТА №7**

По дисциплине «Проектирование микропроцессорных систем»

На тему: Шифр Эль - Гамаля

Специальность 7M06103-Вычислительная техника и программное обеспечение

Выполнил Сакан Ерлан Группа МВТн-21-2

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_202\_\_\_г.

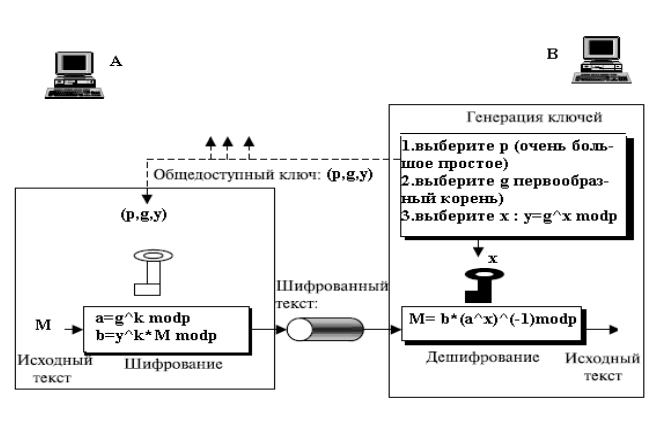
(оценка) (подпись)

Алматы 2022

Цель работы: изучить шифр Эль – Гамаля

Описание работы:

Схему ЭльГамаля можно использовать как для цифровых подписей, так и для шифрования. Алгоритм ЭльГамаля не запатентован, он первый криптографический алгоритм с открытым ключом, пригодный для шифрования и цифровых подписей, применение которого не ограничено патентами США (срок патента Диффи-Хеллмана закончился 29.04.1997 г.). Схема Эль-Гамаля лежит в основе стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-2001).



1.Генерируется случайное простое число p.

2.Выбирается целое число g — первообразный корень p.

3.Выбирается случайное целое число x такое, что

4. (1 < 𝑥 < 𝑝 − 1).

5.Вычисляется 𝑦 = 𝑔 𝑥mod 𝑝 .

6.Открытым ключом является (y,g,p), закрытым ключом — число x.

Шифрование

• Сообщение M должно быть меньше числа p.

• Сообщение шифруется следующим образом:

1.Выбирается сессионный ключ — случайное целое число, взаимно простое с (𝑝 − 1), 𝑘 такое, что 1 < 𝑘 < 𝑝 − 1.

2.Вычисляются числа 𝑎 = 𝑔 𝑘𝑚𝑜𝑑 𝑝 и 𝑏 = 𝑦 𝑘𝑀𝑚𝑜𝑑 𝑝.

3.Пара чисел (𝑎, 𝑏) является шифротекстом.

• Нетрудно заметить, что длина шифротекста в схеме Эль-Гамаля вдвое больше исходного сообщения M

Расшифрование

• Зная закрытый ключ 𝑥, исходное сообщение можно вычислить из шифротекста (𝑎, 𝑏) по формуле:

• 𝑀 = 𝑏 𝑎 𝑥 −1 𝑚𝑜𝑑 𝑝.

• При этом нетрудно проверить, что

• 𝑎 𝑥 −1 = 𝑔 −𝑘𝑥 𝑚𝑜𝑑 𝑝 и поэтому

• 𝑏 𝑎 𝑥 −1 = 𝑦 𝑘𝑀 𝑔 −𝑥𝑘 ≡ (𝑔 𝑥𝑘𝑀)𝑔 −𝑥𝑘 ≡ 𝑀( 𝑚𝑜𝑑 𝑝).

• Для практических вычислений больше подходит следующая формула:

• 𝑀 = 𝑏 𝑎 𝑥 −1 = 𝑏𝑎 𝑝−1−𝑥 (𝑚𝑜𝑑 𝑝)

Ход работы:

Даны рабочие основания (неприводимые многочлены)

M1=110110 1010110 11011

= 3.