ЛАБОРАТОРНАЯ РАБОТА 3

РЕАЛИЗАЦИЯ ЭЛЕМЕНТОВ СХЕМЫ ШИФРОВАНИЯ ЭЛЬ-ГАМАЛЯ

Цель работы: формирование умений шифрования с использованием метода асимметрического шифрования Эль-Гамаля.

Теоретические сведения

Генерация ключей

1. Генерируется случайное простое число p длины q битов.
2. Выбирается случайный примитивный элемент q поля Zp.
3. Выбирается случайное целое число x такое, что $1 < x < p - 1$.
4. Вычисляется $y = g^x \bmod p$.
5. Открытым ключом является тройка чисел (p, g, y), закрытым ключом – x.

Шифрование

Сообщение M шифруется следующим образом:

1. Выбирается сессионный ключ – случайное целое число k, такое, что $1 < k < p - 1$.
2. Вычисляются числа $a = g^k \bmod p$ *и* $b = y^k M \bmod p$.
3. Пара чисел (a, b) является шифртекстом.

Длина шифротекста в схеме Эль-Гамаля вдвое длиннее исходного сообщения M.

Расшифрование

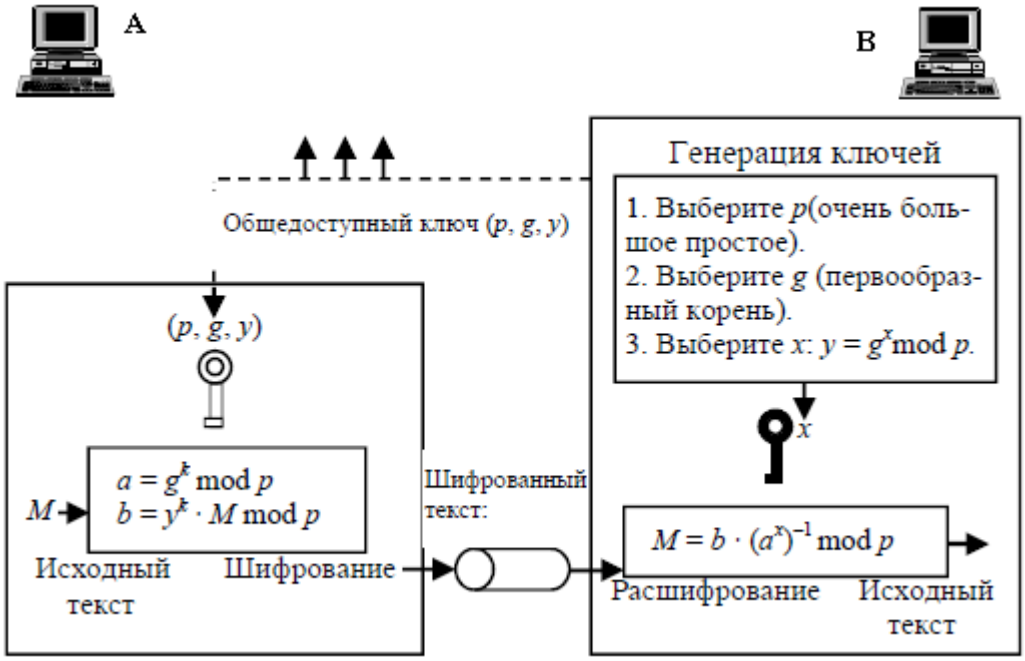
Зная закрытый ключ x, исходное сообщение можно вычислить из шифртекста (a, b) по формуле:

$M = b(a^x)^{-1} \bmod p$. При этом нетрудно проверить, что $(a^x)^{-1} \equiv g^{-kx} \pmod p$, и поэтому

$b(a^x)^{-1} \equiv (y^x N)g^{-xk} \equiv (g^{xk}M)g^{-xk} \equiv M \pmod p$.

Для практических вычислений больше подходит следующая формула:

$M = b(a^x)^{-1} \bmod p = ba^{(p-1-x)} \bmod p$ (рис.1).



Содержание заданий

Разработайте программу, имитирующую реализацию элементов метода криптографической защиты информации Эль-Гамаля. Программа должна выполнять генерацию ключей, шифрование и расшифрования сообщения. В качестве сообщения используйте свою фамилию и имя.

Примечание. P – двузначное число, G, X – однозначные.

Контрольные вопросы

1. Что такое криптосистемы с открытым ключом?
2. Отличие схемы Эль-Гамаля от RSA?
3. Перечислите преимущества и недостатки алгоритма Эль-Гамаля?