Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №4

По дисциплине «Методы защиты информации»
По теме «Ассимметричная криптография. Алгоритм Эль-Гамала»

Выполнил:
студент гр. 653501
М.Л.Спасёнов
Проверил:
В.С.Артемьев

Минск 2019

Введение

Схема Эль-Гамаля (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле.

Схема была предложена Тахером Эль-Гамалем в 1985 году.[1] Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию. Считается, что алгоритм попадает под действие патента Диффи-Хеллмана.

Алгоритм

Генерация ключа

1. Генерируется простое число p
2. Выбирается целое число g - первообразный корень
3. Выбирается случайное число x, такое, что $1 < x < p - 1$
4. Вычисляется $y = g^x mod\ p$
5. y - открытый ключ, x - закрытый

Шифрование

M - сообщение

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

Расшифрование

Зная закрытый ключ, можно вычислить текст по шифротексту по формуле:

$M = ba^{p-x-1} mod\ p$

Выполнение программы

Текст для шифрования - qwerty

Вывод

Шифрование алгоритмом Эль-Гамала, является отличной альтернативой алгоритма RSA, т.к не был запатентован, следовательно не требует взнос за лицензию. А так же криптостойкость алгоритма при равной длине ключа равна RSA.