**Лабораторная работа №7**

**Тема:** Исследование криптоалгоритма шифрования Эль-Гамаля.

**Цель работы:** Исследование структуры алгоритма и методики практической реализации криптосистемы шифрования Эль-Гамаля.

1. **Основные теоретические положения**

Схема шифрования Эль-Гамаля может быть использована как для формирования цифровых подписей, так и шифрования данных. Безопасность схемы Эль-Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

При использовании алгоритма шифрования Эль-Гамаля длина шифротекста вдвое больше длины исходного открытого текста ***М***. В реальных схемах шифрования необходимо использовать в качестве модуля **n** большое простое число, имеющее в двоичном представлении длину ***512… 1024 бит***.

1. **Схема алгоритма шифрования данных Эль-Гамаля**

**2.1. Определение открытого “*y*” и секретного “*x*” ключей**

2.1.1. Выбор двух взаимно простых больших чисел ***p*** и ***q***, ***q < p***

2.1.2. Выбор значения секретного ключа  ***x, x < p***

2.1.3. Определение значения открытого ключа ***y*** из выражения:

***y = qx (mod p)***

**2.2. Алгоритм шифрования сообщения M**

2.2.1. Выбор случайного числа ***k***, удовлетворяющего условию:

***0*** ≤  ***k < p-1***и ***НОД******(k, p-1) = 1***

2.2.2. Определение значения ***a*** из выражения: ***a = qk(mod p)***

2.2.3. Определение значения ***b*** из выражения: ***b = yk M (mod p)***

2.2.4. Криптограмма ***C,***  состоящая из ***a*** и ***b,***  отправляется получателю

2.2.5. Получатель расшифровывает криптограмму с помощью выражения:

***M ax = b (mod p)***

**2.3. Пример**

Для удобства расчётов используем числа малой разрядности:

2.3.1. Выбираем два взаимно простых числа ***p = 11*** и ***q = 2;***

2.3.2. Выбираем значение секретного ключа ***x, (x < p), x = 8;***

2.3.3. Вычисляем значение открытого ключа **y** из выражения ***x***

***y = qx (mod p) = 28 (mod 11) = 256 (mod 11) = 3;***

2.3.4.Выбираем значение открытого сообщения ***M = 5;***

2.3.5. Выбираем случайное число ***k = 9; НОД (9, 10) = 1***;

2.3.6. Определяем значение **a** из выражения:

***a = q k (mod p) = 29 (mod 11) = 512 (mod 11) = 6;***

2.3.7. Определяем значение ***b*** из выражения:

***b = yk M (mod p) = 39\*5 (mod 11) = 98415 (mod 11) = 9.***

Таким образом, получаем зашифрованное сообщение как ***(a, b) =*** ***(6, 9)*** и отправляем получателю.

2.3.8. Получатель расшифровает данный шифротекст, используя секретный ключ x и решая следующее сравнение:

***M\*ax*** =  ***b (mod p)***

***5\*68*** =  ***9 (mod 11)***

***8398080*** =  ***9 (mod 11)***

Вычисленное значение сообщения  ***M = 5*** представляет собой заданное исходное сообщение.

**3. Содержание отчёта**

3.1. Составить блок-схему и программу алгоритма шифрования Эль-Гамаля.

3.2. Листинг программы шифрования и дешифрования заданного сообщения с использованием алгоритма Эль-Гамаля.

3.3. Выводы.