**Лабораторная работа 11 (алгоритм Эль-Гамаля)**

Алгоритм Эль-Гамаля может использоваться для формирования электронной подписи или для шифрования данных. Он базируется на трудности вычисления дискретного логарифма.

Также, как в протоколе Диффи-Хеллмана, сначала генерируется пара ⟨p, g⟩, состоящая из большого простого числа p и генератора g поля Fp. Эти параметры являются открытыми параметрами протокола Эль-Гамаля. Далее генерируются открытый и закрытый ключи:

Генерация ключей пользователя:

1. Сначала генерируется закрытый ключ пользователя, как произвольное

число x, 1 <x <p,

2. Вычисляет открытый ключ по формуле y = gx mod p,

2. Шифрование сообщения M:

1. Сначала генерируется случайное число k, 1 <k <p, взаимно-простое

с p − 1, т.е. Н.О.Д(p − 1, k) = 1,

2. Вычисляем a = gk mod p,

3. Вычисляем b = yk ·M mod p.

Пара ⟨a, b⟩ является шифром сообщения M.

3. Расшифровка кода ⟨a, b⟩:

Вычисляем исходное сообщение M по формуле: M = b · a−x mod p

Отметим, что поскольку ap−1 mod p = 1, то чтобы не вычислять обратные элементы в поле Fp, можно использовать прямое вычисление M по формуле:

M = b · ap−1−x mod p.

**Задание**: написать программу для шифрования и расшифрования сообщения алгоритмом Эль-Гамаля.

1. technology – студент 1

2. experiment – студент 2

3. algorithm – студент 3

4. schedule – студент 4

5. application – студент 5

6. sunlight – студент 6

7. mylocket – студент 7

8. glorious – студент 8

9. gigantic – студент 9

10. incredible – студент 10

11. corruption – студент 11

12. scientific – студент 12

13. tremendous – студент 13

14. foundation – студент 14