Схема Эль-Гамаля

Аметов Имиль, гр. M07-903

25 мая 2020 г.

Задача:

Продемонстрировать зашифрование/расшифрование по схеме Эль-Гамаля. Использовать $p = 71$ и генератор $g = 7$.

Решение:

Порядок группы $\varphi(p) = p - 1 = 71 - 1 = 70$.

Делители 70: 1, 2, 5, 7, 10, 14, 35. Проверяем, является ли $g = 7$ генератором группы:

Элемент	Степени							Порядок элемента
	2	5	7	10	14	35	70	
7	-22	-20	14	-26	-17	-1	1	70

Выбираю случайное $x = 53 \in [0, 70]$.

Вычисляю

$$y = g^x \mod p = 7^{53} \mod 71 = -8 \mod 71.$$

Получаю следующие открытые и закрытые ключи: PK $= (p : 71, g : 7, y : -8)$, SK $= (p : 71, g : 7, x : 53)$.

Пусть нужно зашифровать $m = 42$. Выбираю случайное число $r = 29 \in [1, 70]$.

Вычисляю

$$a = g^r \mod p = 7^{29} \mod 71 = 35 \mod 71.$$
$$b = 42 \cdot (-8)^{29} \mod 71 = 32 \mod 71.$$

Получаю шифртекст

$$c = (a : 35, b : 32).$$

Теперь осуществляю расшифровку

$$m = \frac{b}{a^x} \mod p = 32 \cdot (35^{-1})^{53} \mod 71 =$$
$$= 32 \cdot (-2)^{53} \mod 71 = 42.$$

Получил открытый текст $m = 42$.