Криптосистема Эль-Гамаля

Данная криптосистема основана на дискретном логарифмировании в конечном поле или группе точек эллиптической кривой.

Используются следующие параметры

1. p - большое простое число
2. g - элемент мультипликативной группы поля F_p

Алгоритм:

Генерация ключей:

1. А выбирает случайное x в интервале $1 < x < p-1$
2. А вычисляет $h = g^x \pmod p$
3. А получает - h (открытый ключ) и x (закрытый ключ

Шифрование:

1. Б получает аутентичную копию h (открытого ключа А)
2. Б представляет сообщение в виде числа m, в интервале $1 < m < p-1$, либо же разбивает сообщение на несколько блоков, которые представляет, как число m
3. Б выбирает k - сеансовый ключ, в интервале $1 < k < p-1$
4. Б вычисляет:

$$C_1 = g^k \pmod p$$

$$C_2 = m \cdot h^k \pmod p$$

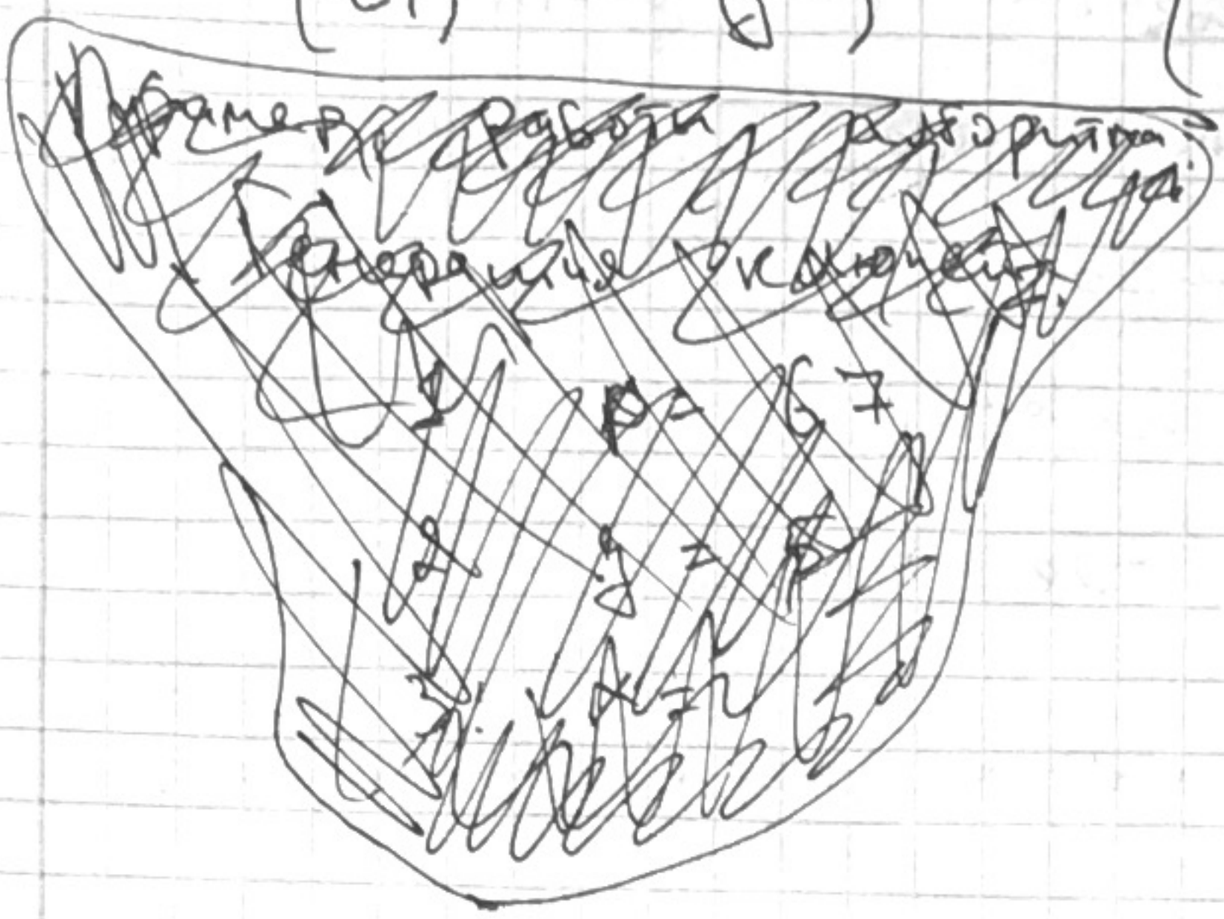
5. Б отправляет (C_1, C_2) А

Расшифрование:

1. А получает шифртекст - (C_1, C_2)
2. А использует свой секретный ключ и

расшифровывает по формуле:

$$\frac{C_2}{(C_1)^x} = \frac{m \cdot h^k}{(g^k)^x} = \frac{m \cdot (g^x)^k}{(g^k)^x} = m$$



Пример работы алгоритма:

$p = 67 \quad g = 5$

Генерация ключей

1). $x = 11$

2). $h = 5^{11} \bmod 67 = 66$

Шифрование:

1). $k = 66$

2). $m = 47$

3). $k = 27$

4). $C_1 = 5^{27} \bmod 67 = 43$

$C_2 = 47 \cdot 66^{27} \bmod 67 = 20$

Расшифрование:

1). $(C_1, C_2) = (43, 20)$

2). $m = \frac{20}{(43)^{11}} = 47$

Построить и исследовать группу точек эллиптической кривой $E_{-2,-2}(F_{13})$

$$y^2 = x^3 + 2x - 2 \ (F_{13})$$

Задача сводится к тому, что нужно

- Найти все точки
- Найти порядок каждой точки
- Определить является ли группа циклической
- Записать все подгруппы и построить диаграмму

$$F_{13} = \{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$$

$x = -6, y^2 = 4$

$x = -5, y^2 = 6$

$x = -4, y^2 = 4$

$x = -3, y^2 = 4$

$x = -2, y^2 = 12$

$x = -1, y^2 = 8$

$x = 0, y^2 = -2$

$x = 1, y^2 = 11$

$x = 2, y^2 = 1$

$x = 3, y^2 = 10$

$x = 4, y^2 = 5$

$x = 5, y^2 = 5$

$x = 6, y^2 = 3$

$$E_{2,-2}(F_{13}) = \{0, (-6, -2), (-6, 2), (-4, -2), (-4, 2), (-3, -2), (-3, 2), (-2, -5), (-2, 5), (1, -1), (1, 1), (2, -6), (2, 6), (5, -4), (5, 4)\}$$

$$|E_{2,-2}| = 15$$