Шифр Эль-Гамаля

- Для всех выбирается большое простое число P и число g такие, что различные степени g есть различные числа по $\bmod P$
- Каждый абонент группы выбирает секретное число $c_i \in (1, P-1)$ и вычисляет $d_i = g^{c_i} \bmod P$ (1)

Сообщение - число $m < P$

Абонент	секр. кл.	откр. кл.
Алиса	c_A	d_A
Боб	c_B	d_B

А: 1. Алиса случайно выбирает число r

2. Вычисляет $k = g^r \bmod P$ (2)

$x = m \cdot d_B^r \bmod P$ (3)

3. Высылает $\langle k, x \rangle$

Б: 1. Боб вычисляет

(4) $m' = x \cdot k^{-c_B + (P-1)} \bmod P = m$

Док-во: $y = \underset{(4)}{x} \cdot k^{-c_B + (P-1)} \underset{(3)}{=}$

$= \underset{(3)}{m \cdot d_B^r} \underset{(2)}{(g^r)^{(P-1)-c_B}} =$

$= m \cdot g^{c_B r} \cdot g^{-c_B \cdot r} \cdot \underset{(1'')}{\left(g^{(P-1)}\right)^k} = m$

↑ по теореме Ферма

Пример $c_A = 4$ $d = 16$ $P = 19$ $g = 2$ $m = 3$

$c_B = 5$ $d_B = 13$

$r = 6$ $x = 3 \cdot 13^6 \bmod 19 = 7$

Боб вычисляет $m' = x \cdot k^{-c_B + (P-1)} = 14 \cdot 7^{-5+18} = 3$ ✓