Функция Эйлера φ(n) – функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним.

**Дискретное логарифмирование**— это метод взлома системы безопасности, основанной на данной эллиптической кривой и нахождения [секретного ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)). Решение уравнения S=nT (mod m){\displaystyle S=nT{\pmod {m}}} относительно n{\displaystyle n} при известных S{\displaystyle S} и T. {\displaystyle T}

Стойкость шифра – сложность задачи его вскрытия.

Проблема шифрования Эль-Гамаля:

– Защифрованный текст больше, чем исходный

– Дискретное логаримфирование.

Проблема шифрования с РСА:

– факторизация больших чисел

Проблема шифрования Диффи-Хелльмана:

– Дискретное логарифмирование