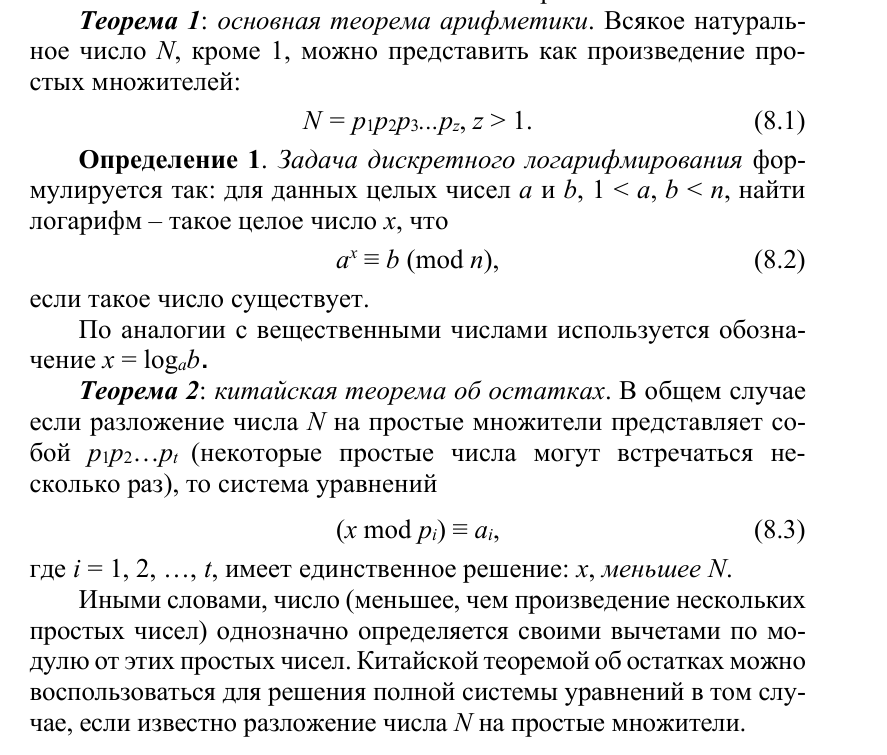
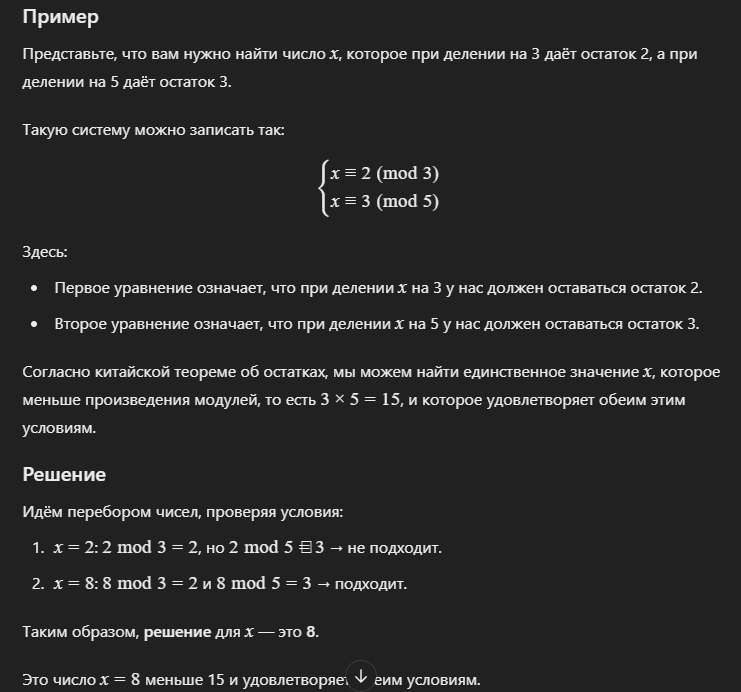
RSA и Эль-Гамаль

Сложность асимметричной криптографии основывается на решении двух задач:

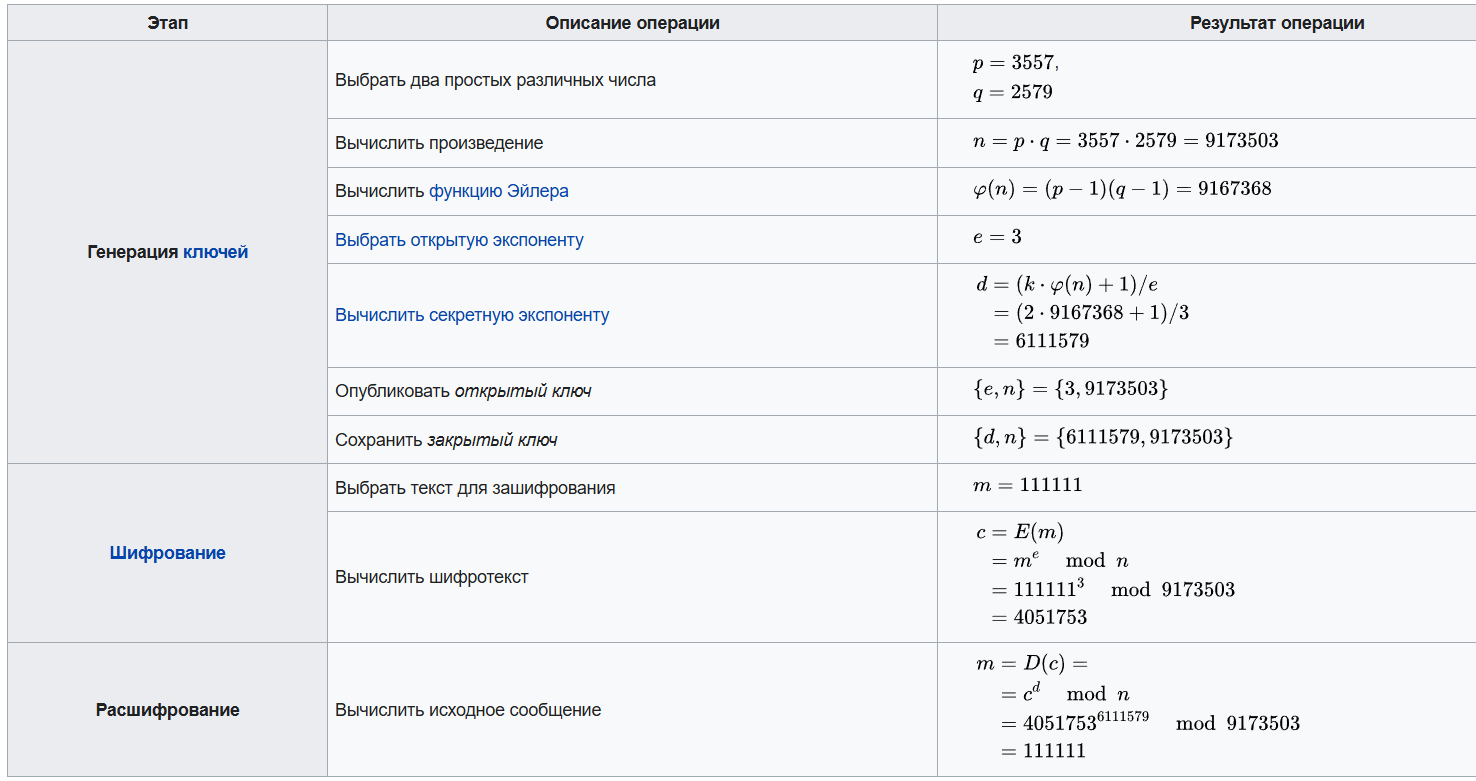
1. Разложение больших множителей на простые (задача факторизации) (RSA)
2. Вычисление дискретного логарифма в конечном поле, и вычислительные операции над точками эллиптической кривой (Эль-Гамаль).



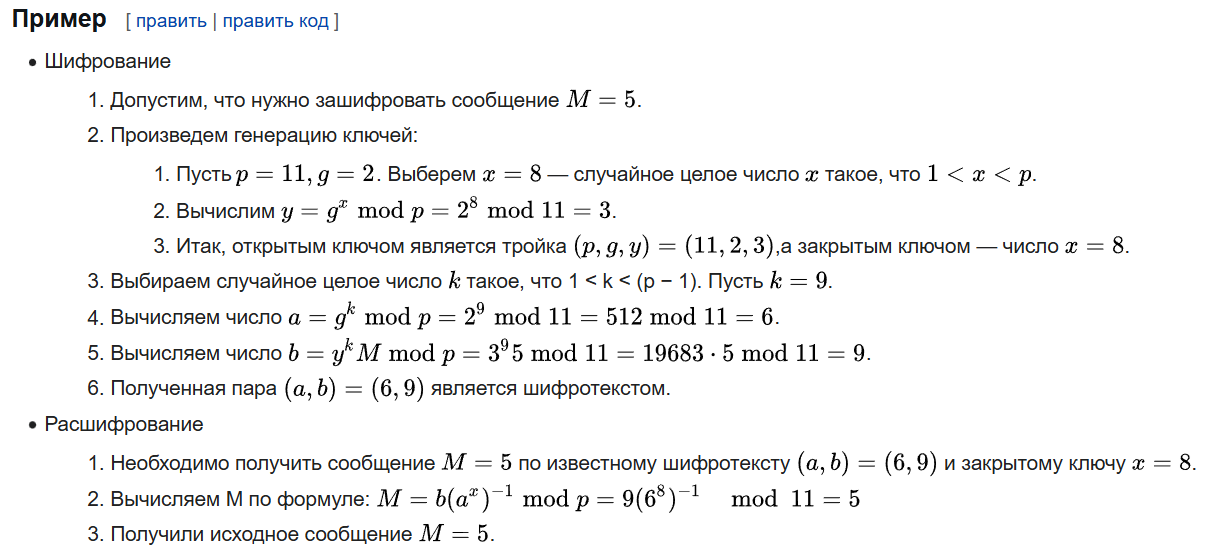
Пояснение к китайской теореме



Алгоритм RSA



Эль-Гамаль



Вместо расшифрования на шаге 2 лучше использовать следующую формулу:

