RSA

1. Проверка на простоту - простая задача
2. Если все $N = P \cdot Q$, где P, Q - два больших простых числа то разложение N - задача факторизации, не решается за полином.

Абонент	Секр. ключ	Откр ключ	
Алиса	c_A	d_A, N_A	$N_A = P_A \cdot Q_A$, $c_A \cdot d_A = 1 \bmod \varphi(N_A)$
Боб	c_B	d_B, N_B	$N_B = P_B \cdot Q_B$, $c_B \cdot d_B = 1 \bmod \varphi(N_B)$

Пара c_i d_i находится по алгоритму Евклида (если получили отрицательное то прибавляем $(P_i - 1)\cdot(Q_i - 1)$ а c_i - случайное взаимно простое с $(P_i - 1)(Q_i - 1)$

$(P_i - 1)\cdot(Q_i - 1) = \varphi(N_i)$ — ф-я Эйлера

Передача сообщения: $A: (1)\ x = m^{d_B} \bmod N_B$

(m - сообщение) $y = x^{c_B} \bmod N_B$

Д-во: $y \underset{(2)}{=} x^{c_B} \underset{(1)}{=} m^{d_B c_B} = m^1$

Пример $P_B = 5$, $Q_B = 11$, $m = 2$, $c_B = 7$ (вз простое с $(P-1)(Q-1)$)

$d_B = 23$

$x = 2^{23} \bmod 55 = 8$

$y = 8^7 \bmod 55 = 2$

Нахождение d_B:

	$(P-1)\cdot(Q-1)$ ↓	1	0	
	7	0	1	
c_B →	5	1	-5	div = 5
	2	-1	6	div = 1
	1	3	-17	div = 2
	0			← Прибавляем 40 => 23 (d_B)