

# Классическая криптография Квантовые вычисления

Мурашко И. В.

Санкт Петербургский Государственный Политехнический Университет

# Введение

Это введение TBD

# Алгоритм RSA. Генерация ключей

- Выбираются два простых числа  $p$  и  $q$
- Вычисляется произведение выбранных простых чисел  $n = p \cdot q$
- Вычисляется функция Эйлера  $\phi(n) = (p - 1)(q - 1)$
- Выбирается целое число  $e$  такое что  $1 < e < \phi(n)$  и  $e$  и  $\phi(n)$  взаимно просты, т. е.  $\text{НОД}(e, \phi(n)) = 1$ .
- вычисляем  $d \equiv e^{-1} \pmod{\phi(n)}$ , т. е.  $d \cdot e \equiv 1 \pmod{\phi(n)}$ .

Открытый ключ состоит из двух чисел: модуля  $n$  и открытой экспоненты  $e$ . Именно эти два числа используются для шифрования исходного сообщения.

Закрытый ключ состоит тоже из двух чисел: модуля  $n$  и закрытой экспоненты  $d$ .

# Алгоритм RSA. Генерация ключей. Пример

## Example

(RSA. Генерация ключей) Выбираем два простых числа  $p = 3$  и  $q = 7$ . Произведение этих чисел  $n = 21$ . Функция Эйлера  $\phi(n) = (p - 1)(q - 1) = 2 \cdot 6 = 12$ .

Выбираем число  $e$  (открытая экспонента), таким образом, что  $1 < e < 12$  и  $\text{НОД}(e, 12) = 1$ . Очевидно  $e = 5$  удовлетворяет заявленным условиям.

Вычисляем закрытую экспоненту  $d \equiv 5^{-1} \pmod{12}$ , т. е.  $d = 5$ . Действительно  $5 \cdot 5 = 25 = 2 \cdot 12 + 1$ , т. е.  $5 \cdot 5 \equiv 1 \pmod{12}$ .

Т. о. получаем

- Открытый ключ ( $n = 12, e = 5$ )
- Закрытый ключ ( $n = 12, d = 5$ )

TBD