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. НОД $(e, \phi(n)) = 1$.
- вычисляем $d \equiv e^{-1} \mod \phi(n)$, т. е. $d \cdot e \equiv 1 \mod \phi(n)$.

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 НОД$(e, 12) = 1$. Очевидно $e = 5$ удовлетворяет заявленным условиям.
Вычисляем закрытую экспоненту $d \equiv 5^{-1} \mod 12$, т. е. $d = 5$.
Действительно $5 \cdot 5 = 25 = 2 \cdot 12 + 1$, т. е. $5 \cdot 5 \equiv 1 \mod 12$.
Т. о. получаем

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

Алгоритм RSA. Шифрование

Допустим надо зашифровать некоторое сообщение M. Вначале оно переводится в целое число(числа) m такое, что $0 < m < \phi(n)$. Далее вычисляется за зашифрованный текст c:

$$c \equiv m^e \mod n \tag{1}$$

Example

(RSA. Шифрование) Допустим у нас есть открытый ключ $(n = 12, e = 5)$ (см. прим. 1) и мы хотим зашифровать следующее сообщение $m = 1101_2 = 11_{10}$. Шифротекст вычисляется по формуле (2) $c \equiv 11^5 \mod 21 = 2$.

Алгоритм RSA. Дешифрование

Допустим надо зашифровать некоторое сообщение M. Вначале оно переводится в целое число(числа) m такое, что $0 < m < \phi(n)$. Далее вычисляется за зашифрованный текст c:

$$c \equiv m^e \mod n \tag{2}$$

Example

(RSA. Шифрование) Допустим у нас есть открытый ключ $(n = 12, e = 5)$ (см. прим. 1) и мы хотим зашифровать следующее сообщение $m = 1101_2 = 11_{10}$. Шифротекст вычисляется по формуле (2) $c \equiv 11^5 \mod 21 = 2$.

TBD