

Классическая криптография Квантовые вычисления

Мурашко И. В.

Санкт Петербургский Государственный Политехнический Университет

Agenda

- Квантовая механика
- Квантовые вычисления
- Методы симметричного шифрования и алгоритм Гровера
- Методы несимметричного шифрования (RSA, Diffie-Hellman, Elliptic curve) и алгоритм Шора.

Двухуровневый атом

TBD

Кот Шредингера

TBD

Отрицательные вероятности

TBD

Базовые блоки квантового компьютера

TBD

Задача о поиске иголки в стоге сена

TBD

Алгоритм Гровера

TBD

Влияние на рекомендации к использованию

$$AES_{128} \rightarrow AES_{256}$$

RSA и задача факторизации чисел

TBD

Diffie-Hellman, Elliptic curve и дискретный логарифм

TBD

Задача о нахождении периода функций и алгоритм Шора

TBD

Влияние на рекомендации к использованию

NSA не рекомендует использование алгоритмов на эллиптических кривых для внутреннего использования.

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 $(n = 12, d = 5)$

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 :

$$c \equiv m^e \pmod{n} \quad (1)$$

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) $c \equiv 11^5 \pmod{21} = 2$.

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 :

$$c \equiv m^e \pmod{n} \quad (2)$$

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) $c \equiv 11^5 \pmod{21} = 2$.

TBD

Алгоритм Шора

Algorithm 1 Алгоритм Шора

$a \leftarrow 0$

repeat

 Выбрать новое число a такое, что $0 < a < N$

if $\text{НОД}(a, N) \neq 1$ **then**

return a

end if

 Найти период r функции $f(x, a) = a^x \bmod N$

until $(r \not\equiv 0 \bmod 2)$ **or** $(a^{\frac{r}{2}} \equiv -1 \bmod N)$

return $\text{НОД}(a^{\frac{r}{2}} \pm 1, N)$

Алгоритм Гровера

TBD