Алгоритм RSA

1) Выбираем простые числа p и q (длиной по 1024 бита)

2) Вычисляем $N = p \cdot q$

3) Вычисляем $\varphi(N) = (p - 1) \cdot (q - 1)$

4) Выбираем e ($e < N$)

5) Вычисляем d, такое, что $d \cdot e \equiv 1 \pmod{\varphi(N)}$

(эта запись означает, что $d \cdot e + x \cdot \varphi(N) = 1$)

6) Шифруем сообщение m: $c = E(m) = m^e \bmod N$

7) Получаем и расшифровываем c: $m = D(c) = c^d \bmod N$

Какие числа нужно опубликовать, чтобы алгоритмом можно было воспользоваться?
Какие числа необходимо держать в строжайшем секрете?
Сколько десятичных цифр должно быть в простом числе длиной 1024 бита?

Задача 1. Напишите программу, получающую на вход два натуральных числа и вычисляющую их НОД. Можно использовать рекурсию.

Задача 2. Напишите функцию, вычисляющую корни уравнения $ax + by = 1$.
Используйте расширенный алгоритм Евклида (задача 22.12). Можно использовать рекурсию.

Задача 3. Напишите программу, вычисляющую простые числа методом вычёркивания (решето Эратосфена). Проверьте экспериментально, какой максимальной длины простые числа можно получить таким способом на вашем компьютере за время меньше минуты.

Задача 4. Напишите программу быстрого возведения большого числа m в степень e по модулю k. Используйте представление степени в двоичной записи.
Какие числа e лучше брать, чтобы возведение в степень происходило быстрее?

Задача 5. Выполните шаги 1 — 5 алгоритма RSA. Вычислите необходимые для зашифровки и расшифровки числа.

Задача 6. Напишите программу, которая получает на вход сообщение (число) и зашифровывает его (необходимые параметры можно включить в программу в виде констант.)

Задача 7. Напишите программу, которая получает на вход зашифрованное сообщение и расшифровывает его (необходимые параметры можно включить в программу в виде констант). Проверьте, что расшифрованное сообщение такое же, как отправленное.

Задача 8. Зашифруйте и расшифруйте таким способом текстовую строку.
Зачем при шифровании к текстовой строке подмешивают «соль», прежде чем применить к ней алгоритм шифрования?

Задача 9. Напишите программу, взламывающую шифр. Пользуемся тем, что наши простые числа недостаточно большие.