RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — [криптографический алгоритм с открытым ключом](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC), основывающийся на [вычислительной сложности](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C) [задачи факторизации](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), и для [цифровой подписи](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C).

Криптографические системы с открытым ключом используют так называемые [односторонние функции](https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%BD%D1%8F%D1%8F_%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F), которые обладают следующим свойством:

если известно {\displaystyle x}x, то {\displaystyle f(x)}f(x) вычислить относительно просто;

если известно y = f(x) {\displaystyle y=f(x)}, то для вычисления {\displaystyle x}x нет простого (эффективного) пути.

Под односторонностью понимается не теоретическая однонаправленность, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени.

В основу криптографической системы с открытым ключом RSA положена сложность [задачи факторизации](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) произведения двух больших простых чисел. Для шифрования используется операция [возведения в степень по модулю](https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B7%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2_%D1%81%D1%82%D0%B5%D0%BF%D0%B5%D0%BD%D1%8C_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E) большого числа. Для дешифрования (обратной операции) за разумное время необходимо уметь вычислять [функцию Эйлера](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0) от данного большого числа, для чего необходимо знать разложение числа на простые множители.

Что бы зашифровать слово нам надо:

* выбрать два больших простых числа p и q;
* вычислить: n = p ⋅ q, m = (p – 1) ⋅ (q – 1);
* выбрать случайное число d, взаимно простое с m;
* определить такое число e, для которого является истинным выражение: (e⋅d)%(m) = 1;
* числа e и n – это открытый ключ, а числа d и n – это закрытый ключ;

Суть заключается в том, что мы порядковый номер каждой буквы в слове подставляем в формулу

N \*\* e % n

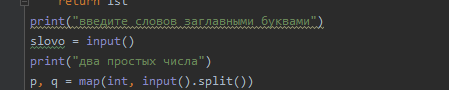
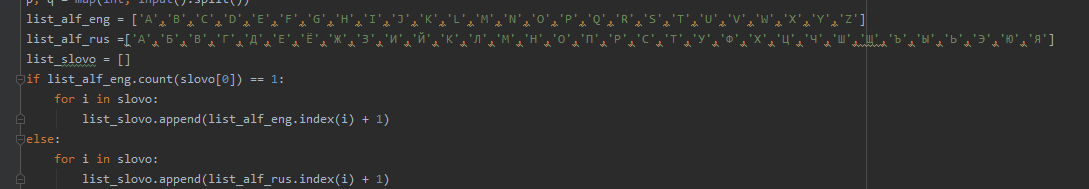
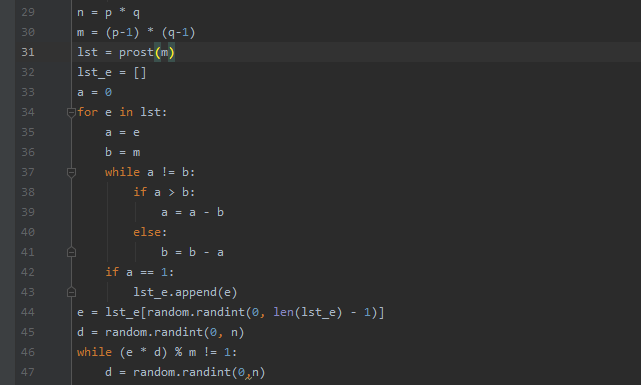
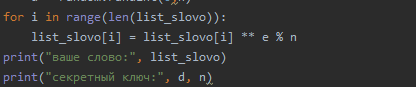
Где e и n являются открытым ключом, а N – номером буквы в алфавите.

Для расшифровки используется тот же самый алгоритм, но вместо e используется b.

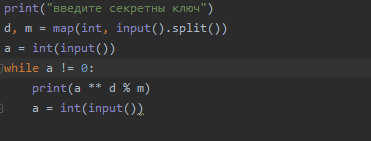
Пример:

* Возьмем слово ТЕКСТ
* Создадим список с порядковыми значениями каждой буквы и получим [18, 6, 12, 17, 18]
* Дальше возьмем 2 простых числа, к примеру 3 и 7
* С их помощью вычислим n = 3 \* 7 = 21 и m = (3 – 1) \* (7 – 1) = 12
* Выберем число e, отвечающее условиям. e = 5
* Подберем число d, удовлетворяющее уравнению (d\*e) % m = 1 и получим 17
* Т = 18 \*\* 5 % 21 = 20
* E = 6 \*\* 5 % 21 = 6
* К = 12 \*\* 5 % 21 = 3
* С = 17 \*\* 5 % 21 = 10
* Получаем [20, 6, 3, 10, 20] с закрытым ключом {17, 21}
* 20 \*\* 17 % 21 = 18
* 6 \*\* 17 % 21 = 6
* 3 \*\* 17 % 21= 12
* 10 \*\* 17 % 21 = 17
* 20 \*\* 17 % 21 = 18
* Получаем первоначальное слово ТЕКСТ

Реализация:

1. вводим наше слово и 2 простых числа для ключей. 
2. создаем 2 списка с русским и английским алфавитами и преобразуем слово в численное значение каждой буквы, проверяя, входит ли 1 буква в английский алфавит и потом находим место данной буквы в списке, прибавляя к этому значению 1 для получения алфавитного порядка. 
3. создаём ключи по выше описанному алгоритму.
4. вычисляем значение для каждой буквы слова и выводим индексы каждого

так же код для дешифрации:



Материалы:

<http://www.michurin.net/computer-science/rsa.html>

<https://ru.wikipedia.org/wiki/RSA>

<https://vscode.ru/prog-lessons/algoritm-rsa.html>

Нильс Фергюсон, Брюс Шнайер / Практическая криптография