Лабораторная работа № 4. Криптосистема [RSA](https://ru.wikipedia.org/wiki/RSA).

Формально как и для любой ассиметричной криптосистемы, для работы RSA необходимо реализовать 3 основные процедуры: генерацию ключей, функцию зашифрования и функцию расшифрования.

Генерация ключей:

1. Выбираются два больших простых числа *p* и *q*.

2. Вычисляется число *n* = *pq*; *n* – открытый параметр.

3. Открытый ключ *e* выбирается случайным образом из Zϕ(*n*) = {0, ..., ϕ(*n*)-1} таким образом, чтобы НОД(*e*, ϕ(*n*)) = 1. (Зная *p* и *q,* можно легко вычислить ϕ(*n*) = (*p*-1)(*q*-1)).

4. Закрытый ключ *d* из Zϕ(*n*); находится по формуле *d* = *e*-1 (mod ϕ(*n*)).

Замечание: Проверить, что случайно выбранное число *e* удовлетворяет условию НОД(*e*, ϕ(*n*)) = 1, и, если условие выполнено, найти закрытый ключ *d* = *e*-1 (mod ϕ(*n*)) можно с помощью [расширенного алгоритма Евклида](http://e-maxx.ru/algo/export_extended_euclid_algorithm).

Сообщение *X*, которое необходимо зашифровать, представляется в виде некоторого числа из Z*n*.

Функция зашифрования: E*e*(*X*) = *Xe* (mod *n*), где *n* – открытый параметр, *e* – открытый ключ.

Замечание: Для возведения в степень рекомендуется использовать [алгоритм быстрого возведения в степень](http://e-maxx.ru/algo/binary_pow). Вычислять остаток от деления необходимо после каждой операции умножения.

Функция расшифрования: D*d*(*Y*) = *Yd* (mod *n*), где *n* – открытый параметр, *d* – закрытый ключ.

Что необходимо сделать:

0) Для выполнения всех заданий необходимо использовать "длинную" арифметику. Разрешается использовать любую библиотеку для этих целей или написать свою.

1) В условиях своего варианта для заданных чисел *p*, *q* и *e*, необходимо вычислить *d*. **Важно**: Использовать готовую реализацию расширенного алгоритма Евклида или вычисления обратного по модулю элемента нельзя! (Можно только для проверки своих результатов).

2) Для заданного сообщения *X*1, вычислить зашифрованное сообщение *Y*1, используя открытый ключ *e*.

3) Расшифровать сообщение *Y*1, использую закрытый ключ *d*, сравнить результат с исходным сообщением *X*1.

4) Для заданного шифртекста *Y*2, вычислить исходный открытый текст *X*2, используя закрытый ключ *d*.

| № Вар. | *p* | *q* | *e* | *X*1 | *Y*2 |
| --- | --- | --- | --- | --- | --- |
| 1 | 563036103490583 | 1063300642915937 | 372585779765210097553647509959 | 399754188907643924420059310699 | 293314580135454643114146935352 |
| 2 | 684391453787369 | 938396705691661 | 245372344253915653531369256899 | 184712154522842417799563173273 | 447204864183801463638208868116 |
| 3 | 950226133300007 | 973747816218557 | 272205786540380931859823391349 | 487590396324873679144487947752 | 371209390170967767404608751313 |
| 4 | 882493304303057 | 565640080106113 | 435510454193522616856570224823 | 33938304564942541056706890572 | 167669363821217143128176537107 |
| 5 | 801410357975153 | 950867021741191 | 110066171603901969362593059313 | 651256495894733822754552878879 | 253970845268857814403399216528 |
| 6 | 877624729981871 | 977289103272413 | 393858705445953556259457155603 | 99213684276131904144063593842 | 3323645942935447942371627841 |
| 7 | 578569278720973 | 976534805568533 | 235108486320061234453015373083 | 402700874043636335474593885222 | 416593343738152120120255791792 |
| 8 | 1102914252601991 | 571301412050021 | 624840313709071966800768010501 | 267222621555915275276288463243 | 291064433434228628162063527294 |
| 9 | 1044779951622553 | 810317495045789 | 657311140049004998195550456065 | 543066057187844905915287549311 | 482438945755863228767362999535 |
| 10 | 749491517671339 | 1074991257344881 | 224872067131777233484376270407 | 469827559223869083025116205997 | 135039041969537192266152584876 |
| 11 | 1003636526287921 | 630114564355681 | 227175758417350578804323023499 | 94380455332205669620317800575 | 493089842126272405947077785493 |
| 12 | 630771436373581 | 786871162464589 | 145903195239272744119599032753 | 153836541207562724815850112591 | 154774251062114172643840396063 |
| 13 | 1101233370547069 | 913071788602213 | 441294907009469893617176298995 | 832192044845038413443817859011 | 381868705201087633178499417569 |
| 14 | 804288300171659 | 819139104388459 | 587862009679843002844824189377 | 201229993267158788910642144722 | 474981332560572636448191786787 |
| 15 | 722227767914309 | 645306156219341 | 188343213856435087990117867713 | 340693830559923670446313718411 | 401641252598150824512742688568 |