RSA Decryption

$M = C^d \bmod n$ ← d is the inverse of $e \bmod (P-1)(Q-1)$

M: unencrypted (decrypted) message (integer) (block) → convert to letters for final answer

C: Given, encrypted message (integer) (block)

Given $n = P \cdot Q$ (primes)

Still need to figure out block size with decryption.

key (n, e) it's given

$\gcd(e, (P-1)(Q-1)) = 1$

ex: Decrypt the message 2545 using RSA with $n = 53 \cdot 61$ and $e = 17$

Solution

$n = 53 \cdot 61 = 3233$

Largest grouping of 25's not exceeding 3233 is 2525. ↑ 4 digits

so block size is 4 digits

d is called the decryption exponent

d is the inverse of $e \bmod (P-1)(Q-1)$

$17 \bmod (52 \cdot 60)$

$17 \bmod 3120$

Euclidean:

$3120 = 17 \cdot 183 + 9$

$17 = 9 \cdot 1 + 8$

$9 = 8 \cdot 1 + 1$

$8 = 1 \cdot 8 + 0$

Backward pass:

$1 = 9 - 8$

$8 = 17 - 9$

$9 = 3120 - 17 \cdot 183$

$1 = 9 - 8 = 9 - (17 - 9) = 9 - 17 + 9 = 2 \cdot 9 - 17$

$= 2 \cdot (3120 - 17 \cdot 183) - 17 = 2 \cdot 3120 - 17 \cdot 366 - 17$

$= 2 \cdot 3120 - 17 \cdot 367 = 2 \cdot 3120 - 367 \cdot 17$ ← Bezout Identity

$d = 3120 - 367 = 2753$

$M = C^d \bmod n$

$= 2545^{2753} \bmod 3233$ ← use modular exponentiation

$= 2015$

UP

ex: decrypt 2222 using RSA with $n = 43 \cdot 59$ and $e = 5$

Solution

$n = 43 \cdot 59 = 2537$

$2525 < 2537$

Block size is 4.

d is inverse of $5 \bmod (42 \cdot 58)$

$5 \bmod 2436$

$2436 = 5 \cdot 487 + 1$

$5 = 1 \cdot 5$

$1 = 2436 - 5 \cdot 487 = 2436 - 487 \cdot 5$

$d = 2436 - 487 = 1949$

$M = C^d \bmod n$

$= 2222^{1949} \bmod 2537$

Modular Exponentiation

$= 1725$

RZ

$i = \sqrt{-1}$

↖ imaginary variable

number in front of i means imaginary number

ex: $5i$, $-4i$

a real number is a number that's not imaginary

a real number + imaginary number is a complex number

$\sqrt{36} = \sqrt{9 \cdot 4} = \sqrt{9} \cdot \sqrt{4} = 3 \cdot 2 = 6$

$\sqrt{36} = \sqrt{(-9)\cdot(-4)} \neq \sqrt{-9} \cdot \sqrt{-4}$

.real x.real

.imag x.imag

from Plotting import plot

$(10+5i)x = 15$

$x = \frac{15}{10+5i} \cdot \left(\frac{10-5i}{10-5i}\right) = \frac{15 \cdot 10 - 15 \cdot 5i}{100 - 50i + 50i - 25i^2}$

$= \frac{150-75i}{100-25(-1)} = \frac{150-75i}{100+25}$ $\quad i^2 = \left(\sqrt{-1}\right)^2 = -1$

$= \frac{150-75i}{125}$

$= 1.2 - 0.6i$