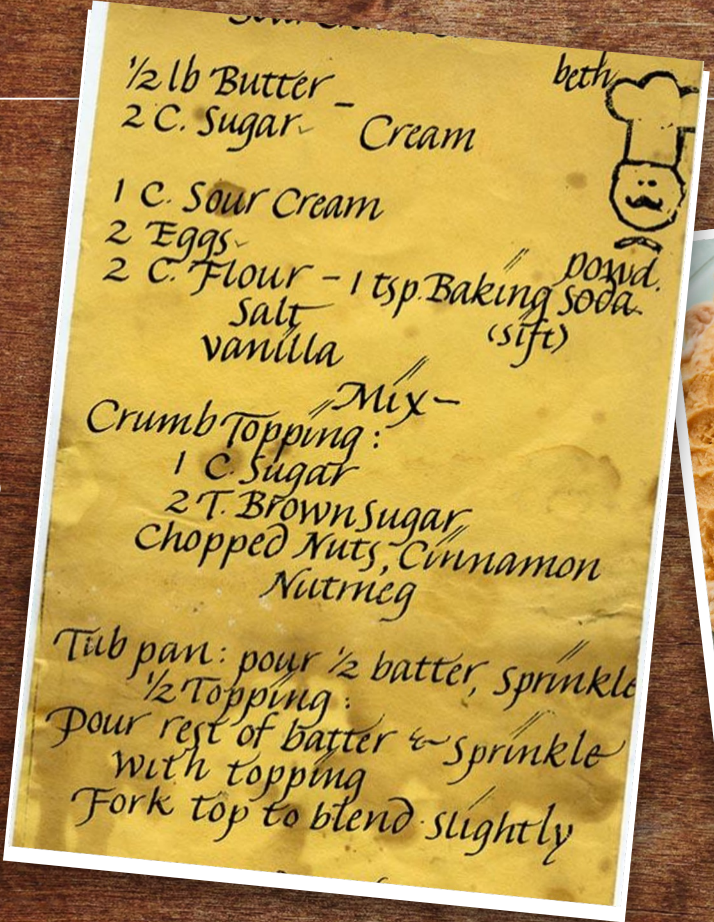
Problem Solving With Algorithms



½ lb Butter –
2 C. Sugar – Cream
beth

1 C. Sour Cream
2 Eggs
2 C. Flour – 1 tsp. Baking powd. soda
Salt (sift)
vanilla
– Mix –
Crumb Topping:
1 C. Sugar
2 T. Brown Sugar
Chopped Nuts, Cinnamon
Nutmeg

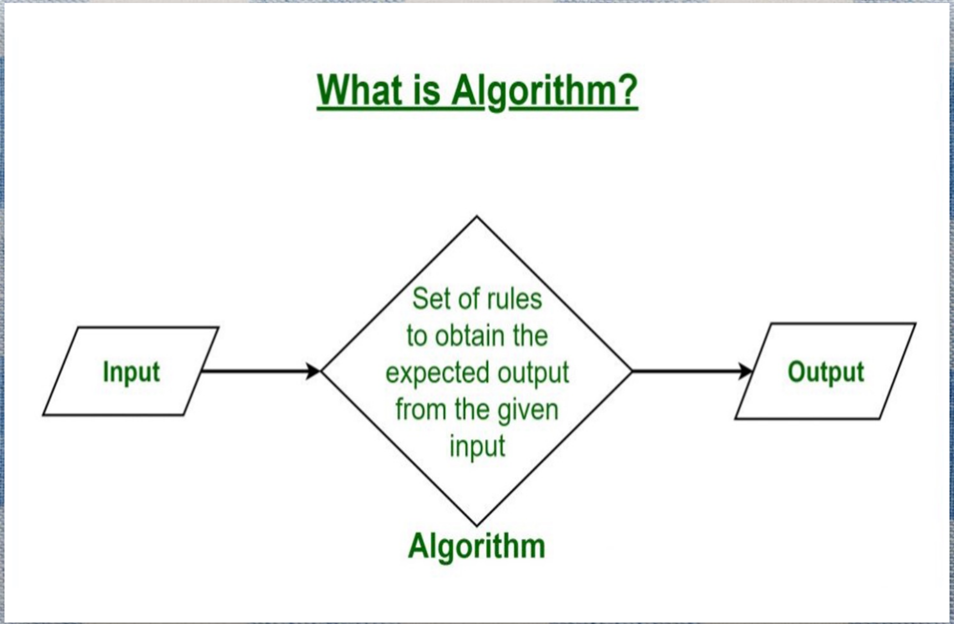
Tub pan: pour ½ batter, sprinkle
½ Topping.
Pour rest of batter & sprinkle
with topping
Fork top to blend slightly

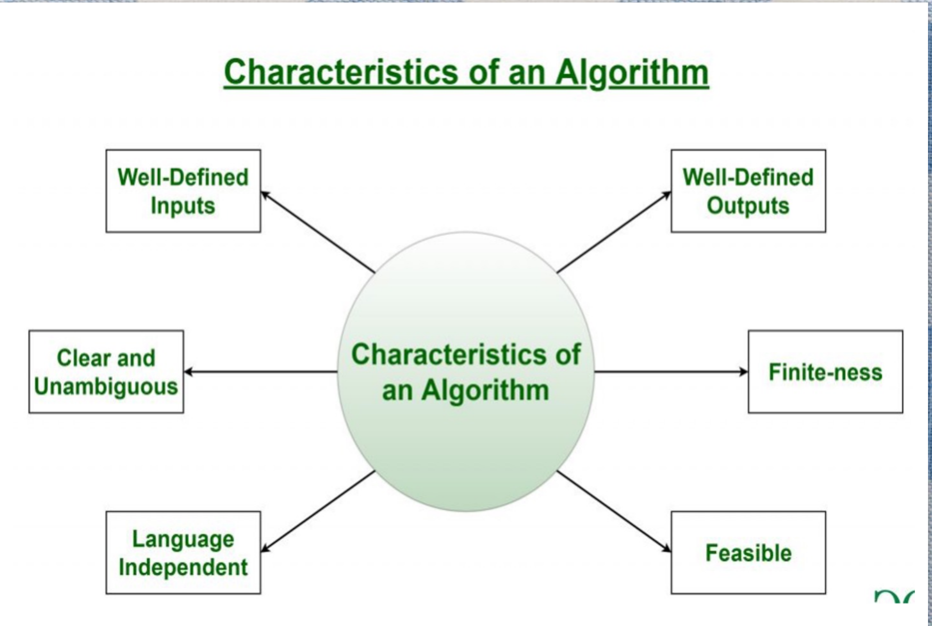
Sarah Meng Li

Math Circles
2022

Table of Contents

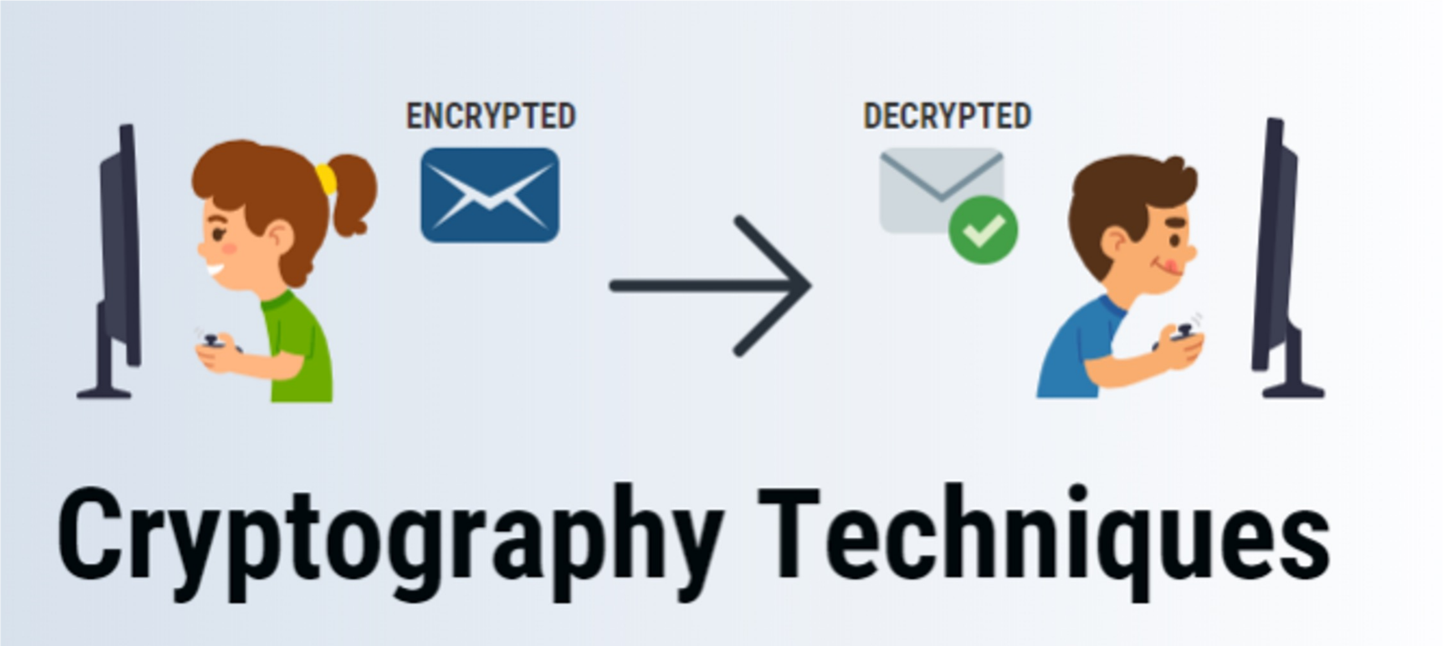
Table of Contents





An algorithm is finite sequence of rigorous instructions to solve a class of specific problems, or to perform computations.

Algorithms help secure communication



Algorithms allows us to search quickly in database

Algorithms enable us to socialize virtually.

Algorithms account for various constraints to schedule transportations.

Algorithms empowers online shopping.


Algorithms coordinate
traffic signals.

GPS


Central Railway
Town Hall Square
Coral Coast avenue
Bridgetown street
Middlegate street
Raspberry Gardens
Yacht Club Marina
Hospital
Western side
Port avenue
H18
Tower Square
South Coast street
Industrial street
Western terminal
N
500 m
Atlantic


Facial Recognition

Steaming Service

Table of Contents

- A **fraction** represents a part of a whole. When spoken in everyday English, a fraction describes how many parts of a certain size there are, for example, one-half, eight-fifths, three-quarters.
- A **fraction** consists of a **numerator**, displayed above a line (or before a slash like ½), and a non-zero **denominator**, displayed below (or after) that line.

- **Exercise 1: Give three examples of fraction, and use them to describe things in daily life.**

- To **simplify a fraction**, divide both the numerator and denominator by the greatest common factor.
- The **greatest common factor (GCF)** between two numbers is the largest factor dividing both of them.
- A fraction is in its simplest form if the GCF of its numerator and denominator is 1.

What is a fraction?
What is a fraction's simplest form?
How to reduce a fraction?

Simplify the fraction.

$$\frac{24}{16} \underset{\div 4}{\overset{\div 4}{=}} \frac{6}{4} \underset{\div 2}{\overset{\div 2}{=}} \frac{3}{2}$$

$$\frac{24}{108} \underset{\div 2}{\overset{\div 2}{=}} \frac{12}{54} \underset{\div 2}{\overset{\div 2}{=}} \frac{6}{27} \overset{\div 3}{=} \frac{2}{9}$$

Exercise 2: Simplify fractions

We use GCF to simplify a fraction!
But it's not easy to find the GCF when the numbers get larger.

1. What are the factors of 12?
2. What are the factors of 16?
3. What are the common factors of 12 and 16?
4. What is the greatest common factor (GCF) of 12 and 16?
5. What are the common factors of 15, 30, and 105?
6. What is the GCF of 15, 30, and 105?
7. What is the GCF of 24 and 108?
8. What are the simplified forms of the following fractions?

   12/16, 15/105, 24/108, 15/30, 30/105

How to find the GCF between two numbers efficiently?

Euclidean Algorithm

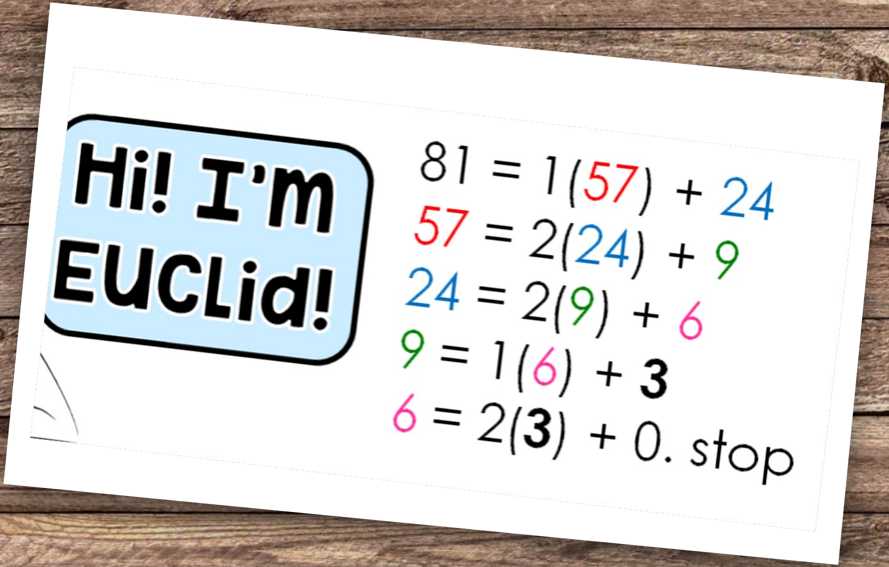
- The **Euclidean algorithm**, or **Euclid's algorithm**, is an efficient method for computing the greatest common factor (GCF) of two integers (numbers), the largest number that divides them both without a remainder. It is named after the ancient Greek mathematician Euclid, who first described it in his *Elements* (c. 300 BC).
- It is an example of an *algorithm*, a step-by-step procedure for performing a calculation according to well-defined rules and is one of the oldest algorithms in common use.
- It can be used to reduce fractions to their simplest form, and is a part of many other number-theoretic and cryptographic calculations.

Blackboard Demo & Activities

Exercise 3: Find GCF(a,b) using Euclidean Algorithm

1. a = 10, b = 75
2. a = 48, b = 360
3. a = 9357, b = 5864
4. a = 12345, b = 67890
5. a = 54321, b = 9876

Why Euclidean Algorithm?



It provides an efficient way to find the GCF of two numbers.

→ You don't have to factor the numbers to find the GCF.

→ By repeatedly performing long division.

→ When the division stops, the remainder will be the GCF.

Factoring a number is hard!

Table of Contents

The Extended Euclidean Algorithm

Example 1: $m = 65, n = 40$

Step 1: The (usual) Euclidean algorithm:

$$\begin{array}{lrl}
(1) & 65 & = 1 \cdot 40 + \boxed{25} \\
(2) & 40 & = 1 \cdot \boxed{25} + 15 \\
(3) & \boxed{25} & = 1 \cdot 15 + 10 \\
(4) & 15 & = 1 \cdot 10 + 5 \\
 & 10 & = 2 \cdot 5
\end{array}$$

Therefore: $\gcd(65, 40) = 5$.

Step 2: Using the method of back-substitution:

$$\begin{aligned}
5 &\overset{(4)}{=} 15 - 10 \\
&\overset{(3)}{=} 15 - (25 - 15) = 2 \cdot 15 - 25 \\
&\overset{(2)}{=} 2(40 - 25) - 25 = 2 \cdot 40 - 3 \cdot 25 \\
&\overset{(1)}{=} 2 \cdot 40 - 3(65 - 40) = 5 \cdot 40 - 3 \cdot 65
\end{aligned}$$

Conclusion: $65(-3) + 40(5) = 5$.

Extend the Euclidean Algorithm

The Extended Euclidean Algorithm

Application: Widely used in cryptography

ax + by = GCF(a,b)

This is a certifying algorithm, because GCF(a,b) is the only number that can simultaneously satisfy this equation and divide a and b. It could be used to derive key-pairs in the RSA public-key encryption method.

Blackboard Demo & Activities

Exercise 4: Express GCF(a,b) in terms of a,b using the Extended Euclidean Algorithm

1. a = 10, b = 75
2. a = 48, b = 360
3. a = 9357, b = 5864
4. a = 12345, b = 67890
5. a = 54321, b = 9876

Table of Contents

PERFECT SQUARES AND THEIR ROOTS

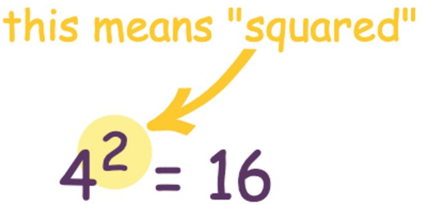
$1^2 = 1$	$11^2 = 121$	$21^2 = 441$
$2^2 = 4$	$12^2 = 144$	$22^2 = 484$
$3^2 = 9$	$13^2 = 169$	$23^2 = 529$
$4^2 = 16$	$14^2 = 196$	$24^2 = 576$
$5^2 = 25$	$15^2 = 225$	$25^2 = 625$
$6^2 = 36$	$16^2 = 256$	$26^2 = 676$
$7^2 = 49$	$17^2 = 289$	$27^2 = 729$
$8^2 = 64$	$18^2 = 324$	$28^2 = 784$
$9^2 = 81$	$19^2 = 361$	$29^2 = 841$
$10^2 = 100$	$20^2 = 400$	$30^2 = 900$

$\sqrt{1} = 1$	$\sqrt{11} = 3.3166$
$\sqrt{2} = 1.4142$	$\sqrt{12} = 3.4641$
$\sqrt{3} = 1.732$	$\sqrt{13} = 3.6055$
$\sqrt{4} = 2$	$\sqrt{14} = 3.7416$
$\sqrt{5} = 2.236$	$\sqrt{15} = 3.8729$
$\sqrt{6} = 2.4494$	$\sqrt{16} = 4$
$\sqrt{7} = 2.6457$	$\sqrt{17} = 4.1231$
$\sqrt{8} = 2.8284$	$\sqrt{18} = 4.2426$
$\sqrt{9} = 3$	$\sqrt{19} = 4.3588$
$\sqrt{10} = 3.1622$	$\sqrt{20} = 4.4721$

What is a square root of a number?
What is a perfect square?
Is every number a perfect square?

How to square a number?

- Squaring a number means multiplying that number by itself.



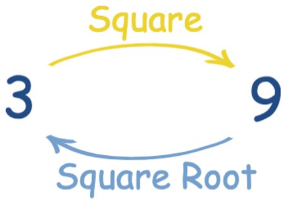
This says ***"4 Squared equals 16"***

(the little 2 says the number appears twice in multiplying)

How to find the square roots of a number a?

What can we multiply by itself to get a?

- A square root of a number is a value that can be **multiplied by itself** to give the original number.
- A square root goes the other way.



3 squared is 9, so a **square root of 9 is 3**

$\sqrt{1} = 1$	$\sqrt{11} = 3.3166$
$\sqrt{2} = 1.4142$	$\sqrt{12} = 3.4641$
$\sqrt{3} = 1.732$	$\sqrt{13} = 3.6055$
$\sqrt{4} = 2$	$\sqrt{14} = 3.7416$
$\sqrt{5} = 2.236$	$\sqrt{15} = 3.8729$
$\sqrt{6} = 2.4494$	$\sqrt{16} = 4$
$\sqrt{7} = 2.6457$	$\sqrt{17} = 4.1231$
$\sqrt{8} = 2.8284$	$\sqrt{18} = 4.2426$
$\sqrt{9} = 3$	$\sqrt{19} = 4.3588$
$\sqrt{10} = 3.1622$	$\sqrt{20} = 4.4721$

What is a perfect square?

- The **Perfect Squares** (also called "Square Numbers") are the squares of the integers.
- Not all integers are perfect square.

Exercise 5: What are the non perfect squares between 1 and 20?

How to approximate a real number?

Continued Fraction

- **Rational number** is a number that can be represented as the quotient p/q of two integers such that $q \neq 0$.
    - In addition to all the fractions, the set of rational numbers includes all the integers, each of which can be written as a quotient with the integer as the numerator and 1 as the denominator.
    - In decimal form, rational numbers are either terminating or repeating decimals. For example, $^1/_7 = 0.\overline{142857}$, where the bar over 142857 indicates a pattern that repeats forever.
- **Irrational number** is a real number that cannot be expressed as a quotient of two integers.

Exercise 6: Examples of rational & irrational number?

What is continued fraction?

- An expression obtained through an **iterative process** of representing a number as the sum of its integer part and the reciprocal of another number, then writing this other number as the sum of its integer part and another reciprocal, and so on.

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

a_0 non-negative,
$a_1, \ldots, a_n$ positive integers

Exercise 7

What is the continued fraction expression of 75/33?

$$75 = 2 \cdot 33 + 9 \qquad \frac{75}{33} = 2 + \frac{9}{33}$$

$$33 = 3 \cdot 9 + 6 \qquad \frac{75}{33} = 2 + \frac{9}{3 \cdot 9 + 6} = 2 + \cfrac{1}{3 + \cfrac{6}{9}}$$

$$9 = 1 \cdot 6 + 3 \qquad \frac{75}{33} = 2 + \cfrac{1}{3 + \cfrac{6}{1 \cdot 6 + 3}} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{3}{6}}}$$

$$6 = 2 \cdot 3 \qquad \frac{75}{33} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{3}{2 \cdot 3}}} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

Blackboard Demo & Activities

Exercise 6: Find the continued fraction of $\sqrt{5}$ using the algorithm on the right.

To find the CF of x:

1) Let $x_0 = x$, $a_0 = \lfloor x_0 \rfloor$.
2) Let $x_1 = 1/(x_0 - a_0)$, $a_1 = \lfloor x_1 \rfloor$.
3) Let $x_2 = 1/(x_1 - a_1)$, $a_2 = \lfloor x_2 \rfloor$.
4) Continue until a pattern is spotted.

Then $x = [a_0; a_1, \ldots, a_n]$

Continued Fraction (CF) for Real Numbers

Finite continued fraction represent rational numbers

- Finding CF exactly parallels the Euclidean algorithm applied to the numerator and denominator of the number.
- It must terminate and produce a finite continued fraction representation of the number.
- The sequence of integers that occur in this representation is the sequence of successive quotients computed by the Euclidean algorithm.
- By construction, every rational number has a unique CF representation.

$$\frac{181}{101} = 1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{4}}}}}.$$

Infinite continued fraction represent irrational numbers

- Finding CF continues indefinitely.
- This produces a sequence of approximations, all of which are rational numbers, and these converge to the starting number as a limit.
- The real numbers whose CF eventually repeats are precisely quadratic irrationals.
- The square roots of all positive integers that are not perfect squares are quadratic irrationals, and hence has unique periodic continued fractions.

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}$$

Why Continued Fraction?

Better Ways to Approximate

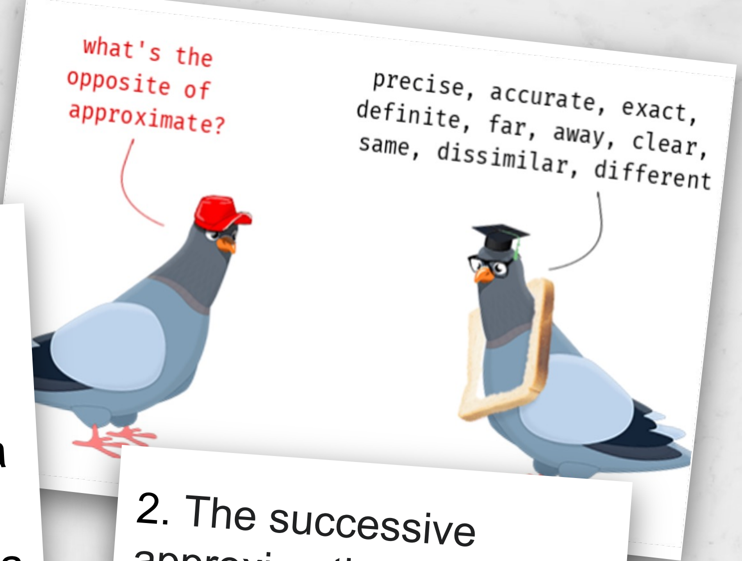
$\pi = 3.14159265358...$

$\frac{22}{7} = 3.1428...$

$\frac{355}{113} = 3.14159292...$

$\frac{104{,}348}{33{,}215} = 3.14159265392...$

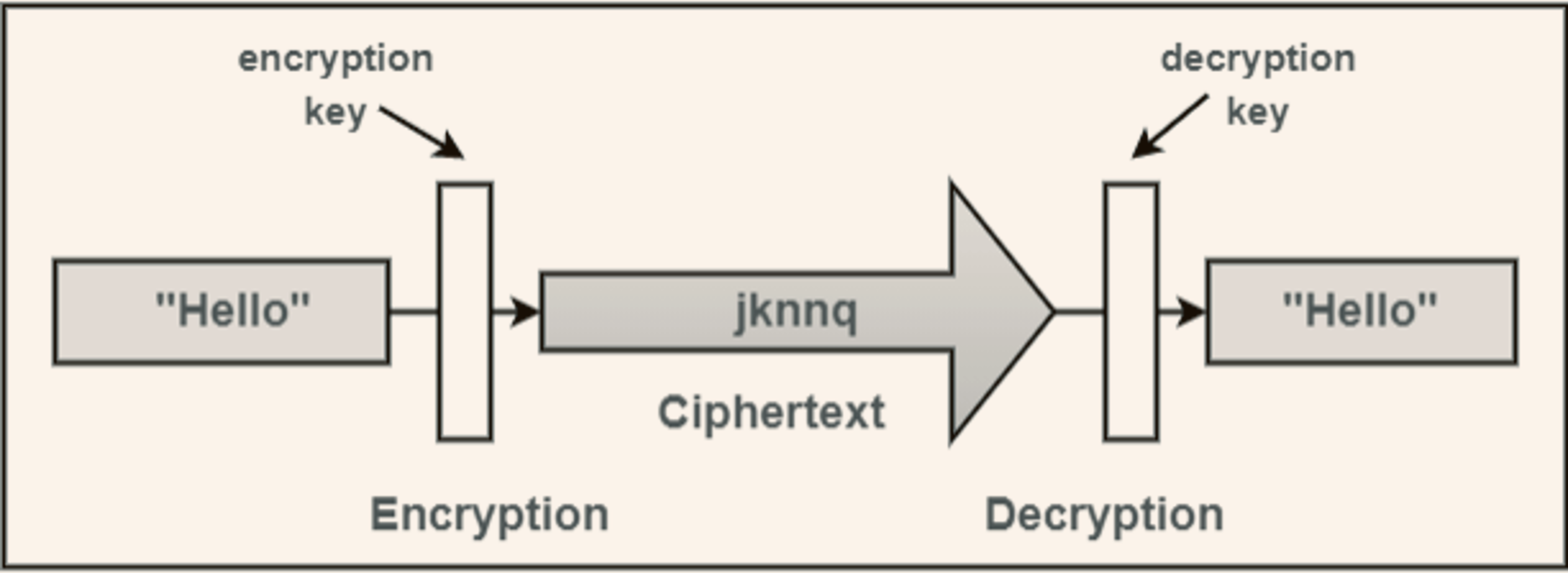
1. More natural representation of a real number than other ways such as decimal representations.



2. The successive approximations generated in finding the continued fraction representation of a number, that is, by truncating the continued fraction representation, are considered as the "best possible" approximation.

Table of Contents

What is cryptography?



Cryptography

A method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

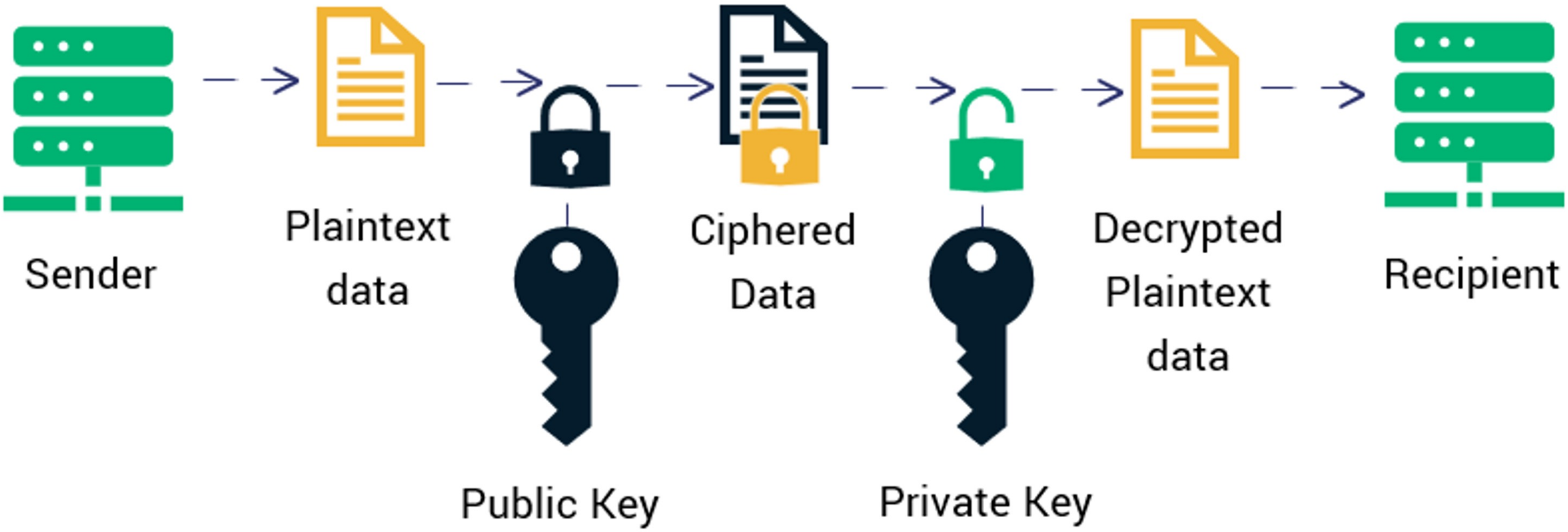
RSA Cryptosystem, publicly described in 1977

RSA (Rivest–Shamir–Adleman) is a **public-key cryptosystem** that is widely used for secure data transmission. It is also one of the oldest.

It applied the Extended Euclidean Algorithm.

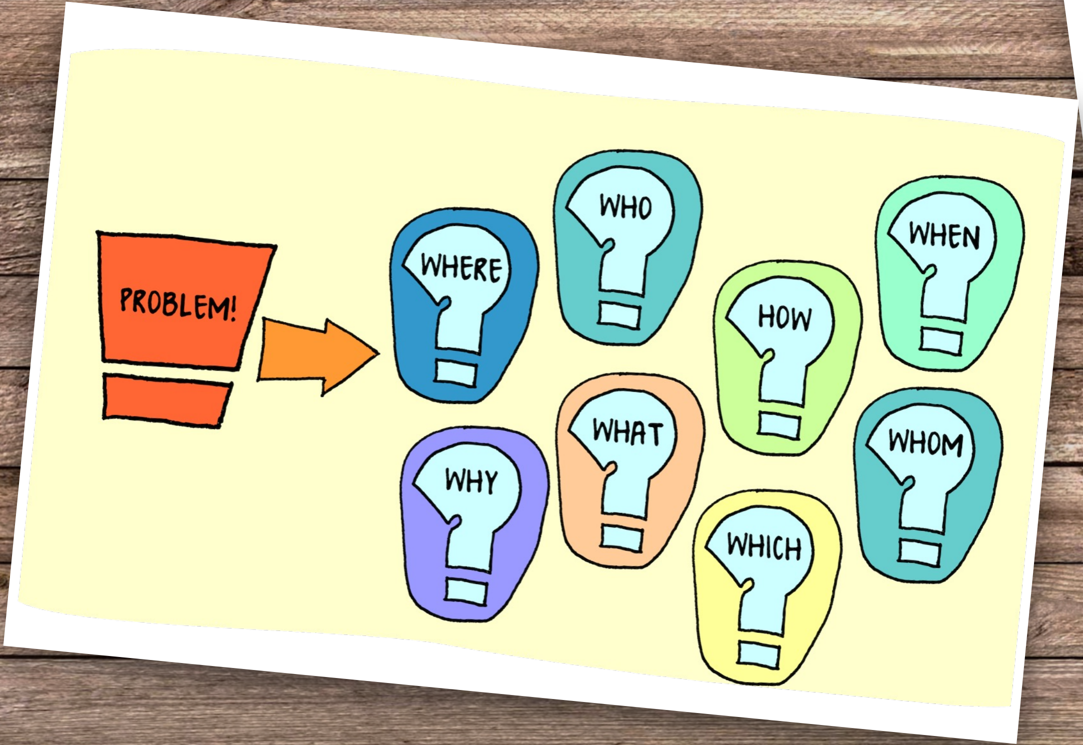
In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

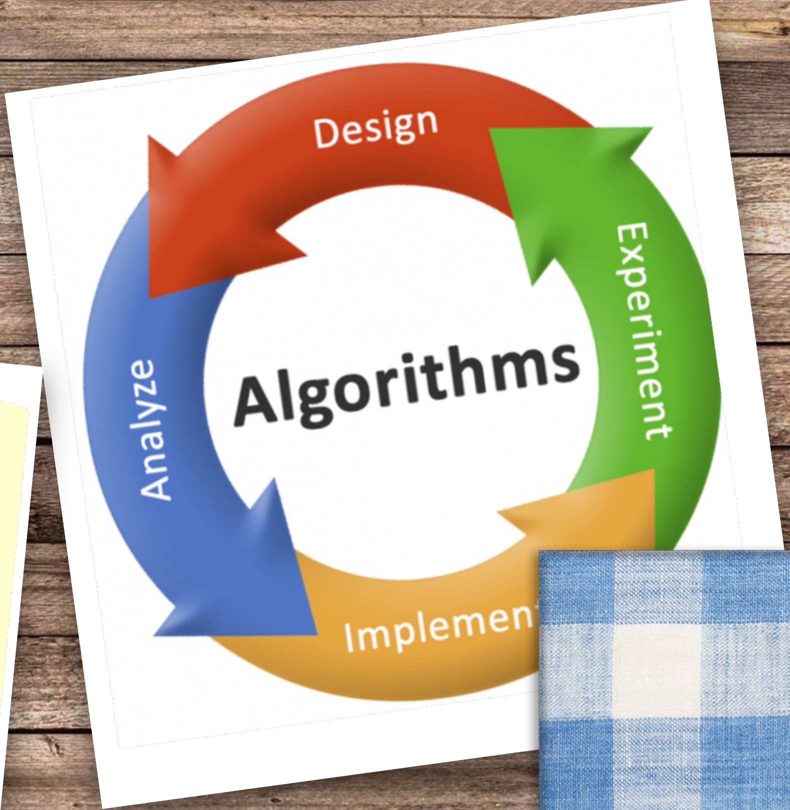
How RSA Encryption Works



Blackboard Demo & The Last Activity

Table of Contents


PROBLEM!
WHERE
WHO
HOW
WHEN
WHY
WHAT
WHICH
WHOM


Design
Experiment
Algorithms
Analyze
Implement