SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with ‘A’ Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

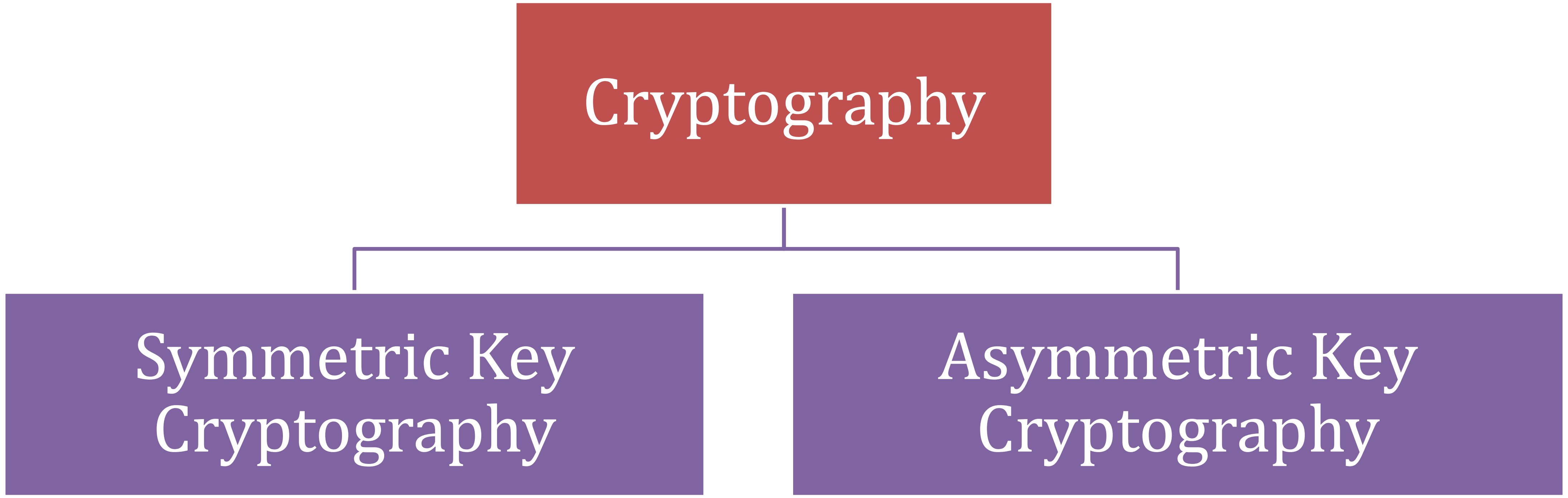
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Course Code and Name : 19CS503– CRYPTOGRAPHY AND NETWORK SECURITY

Unit 3: Public Key Cryptography

Topic : Factorization

CLASSIFICATION OF CRYPTOGRAPHY

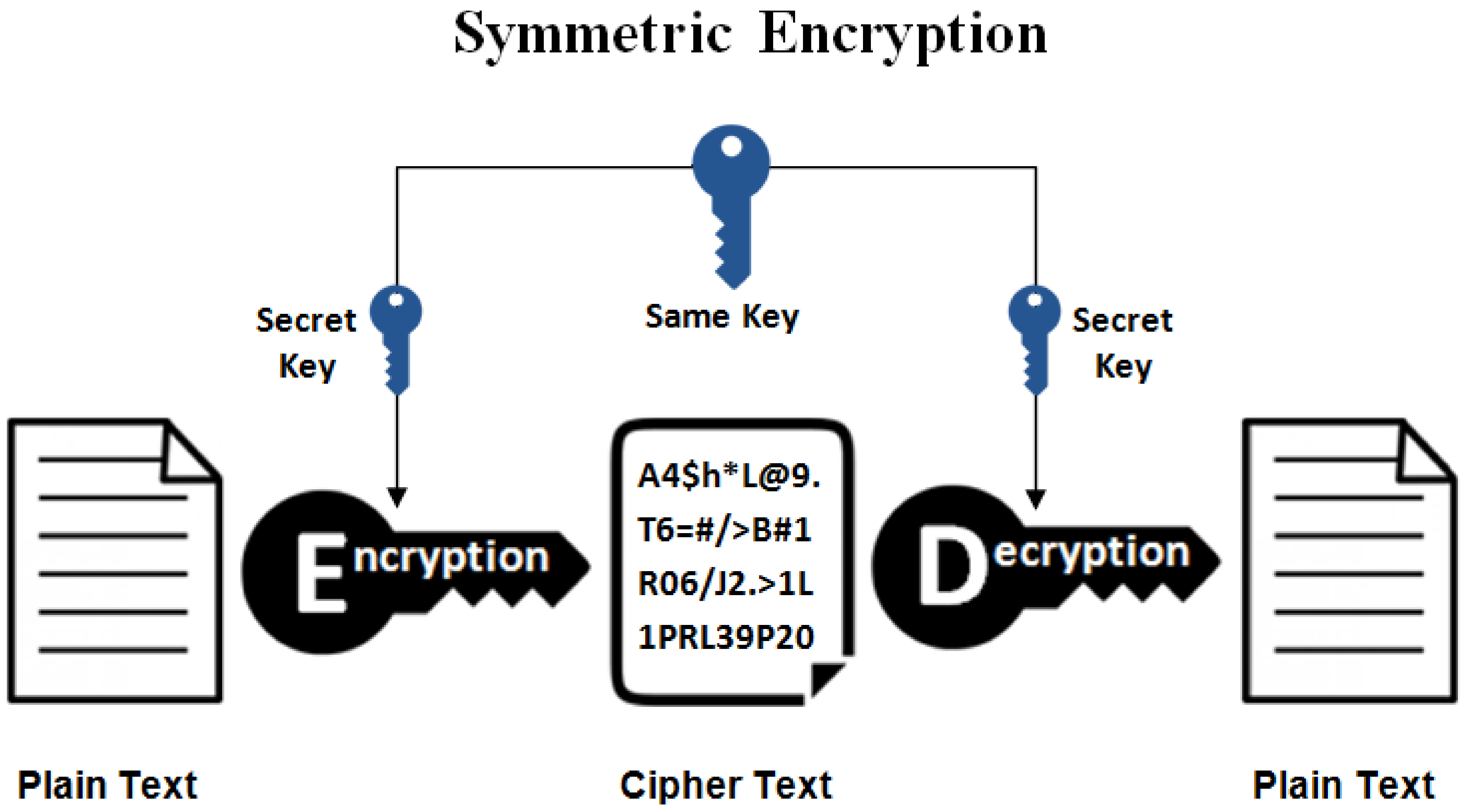


Cryptography

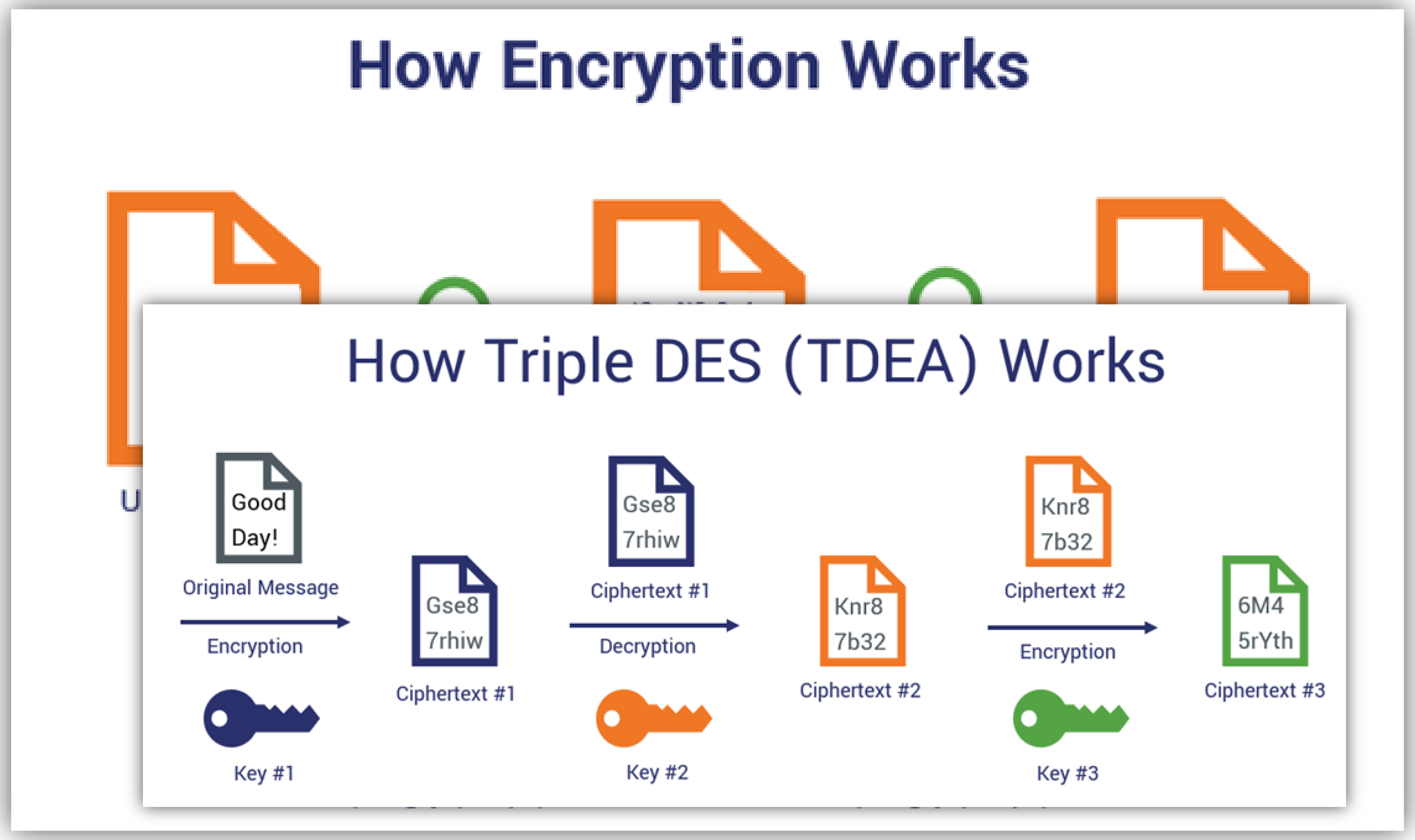
Symmetric Key Cryptography

Asymmetric Key Cryptography

CLASSIFICATION OF CRYPTOGRAPHY

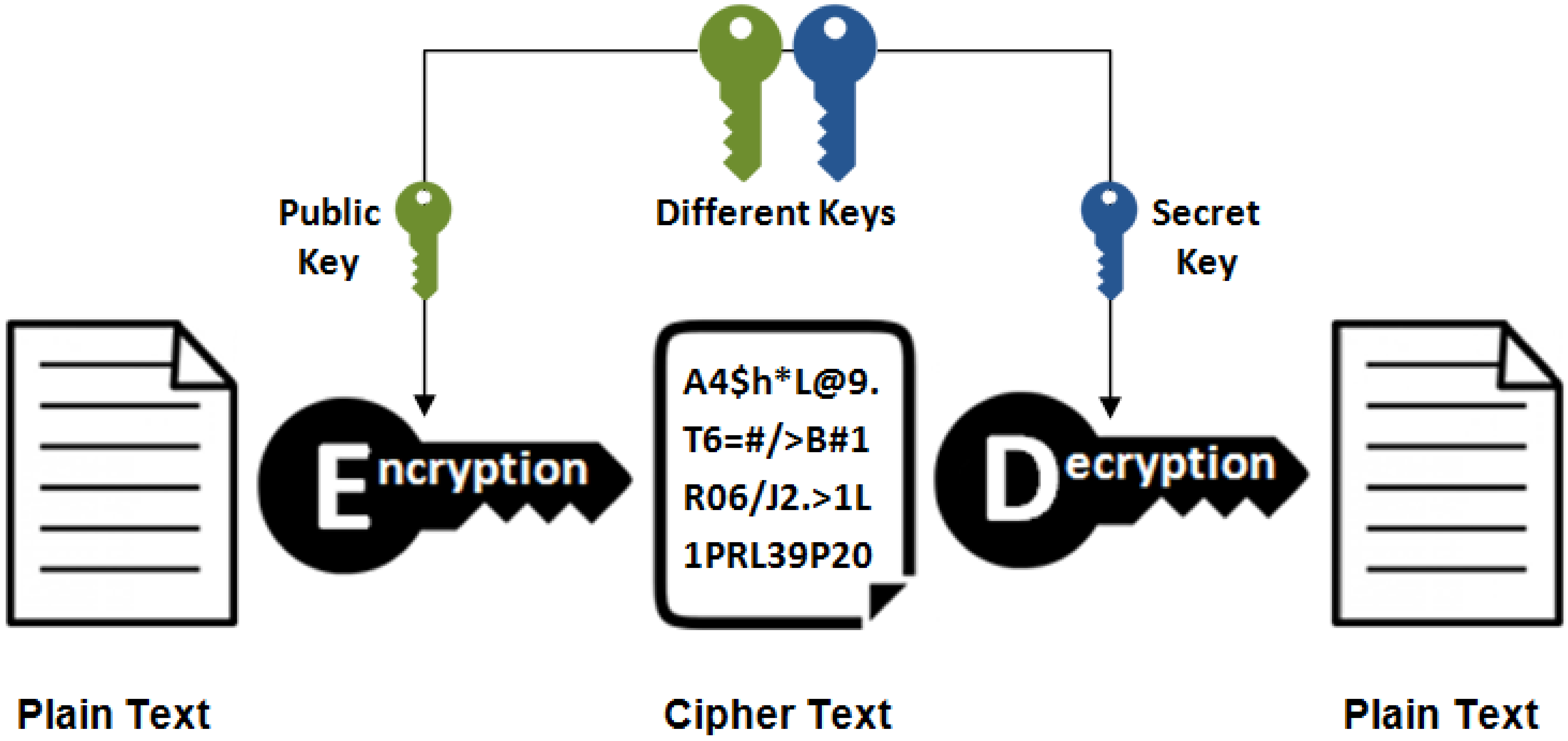


CLASSIFICATION OF CRYPTOGRAPHY

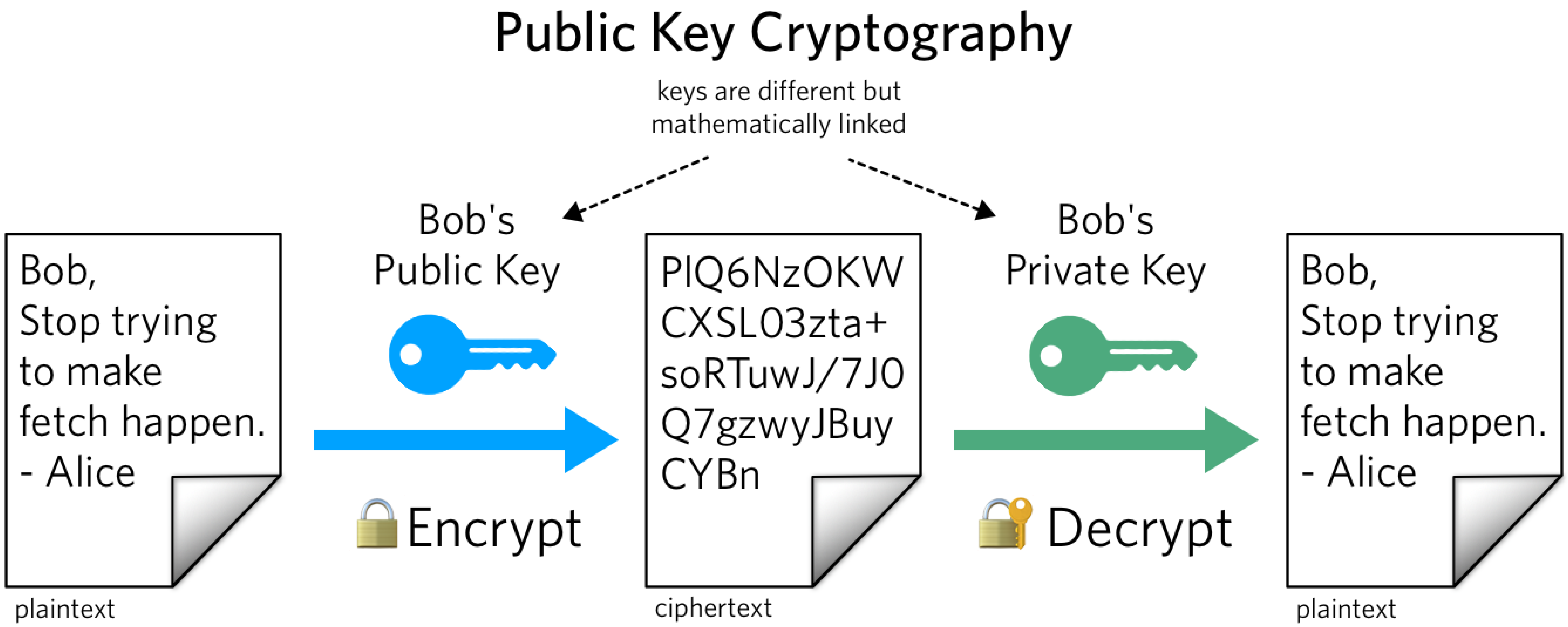


CLASSIFICATION OF CRYPTOGRAPHY

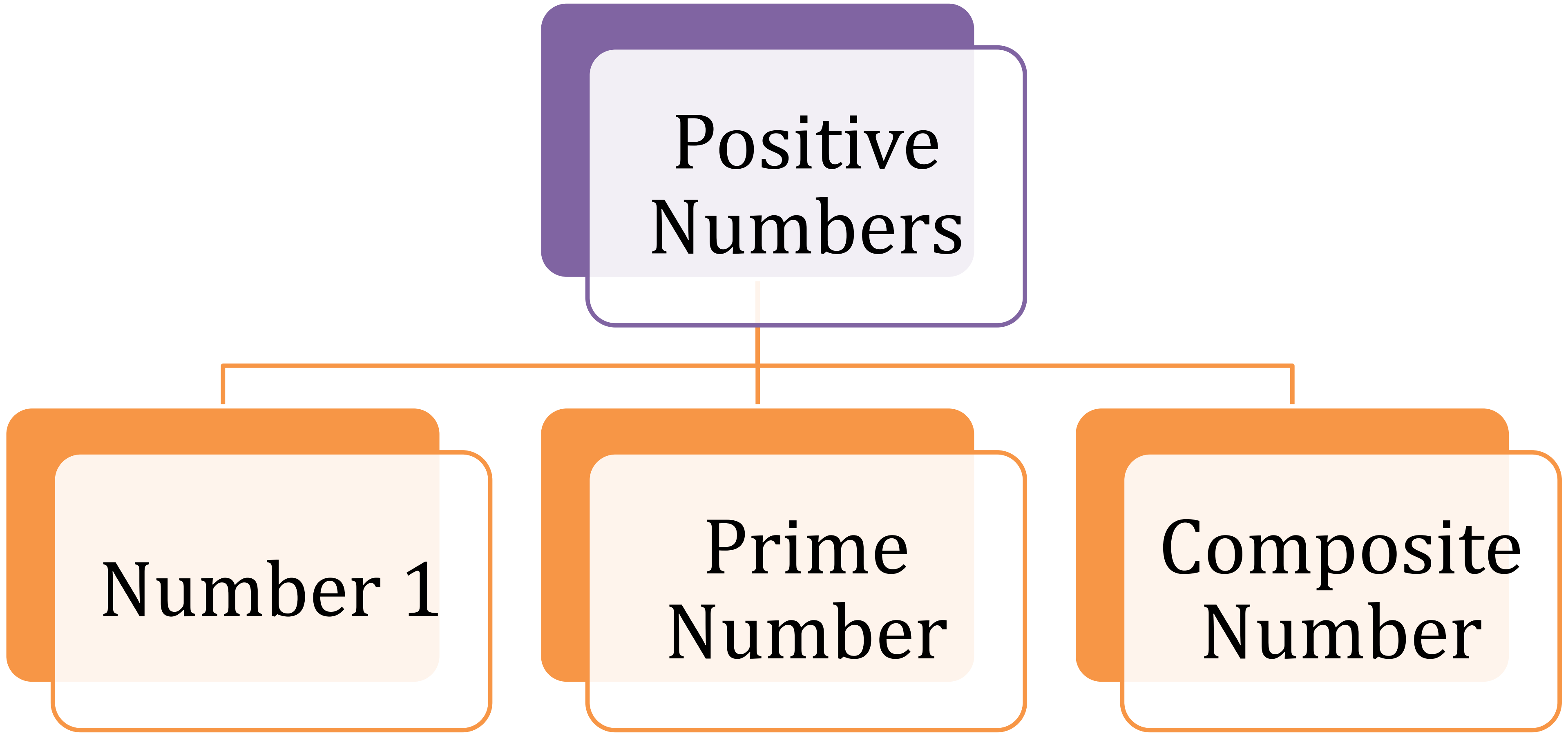
Asymmetric Encryption



CLASSIFICATION OF CRYPTOGRAPHY


Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

GROUPS OF NUMBERS



Positive Numbers

Number 1

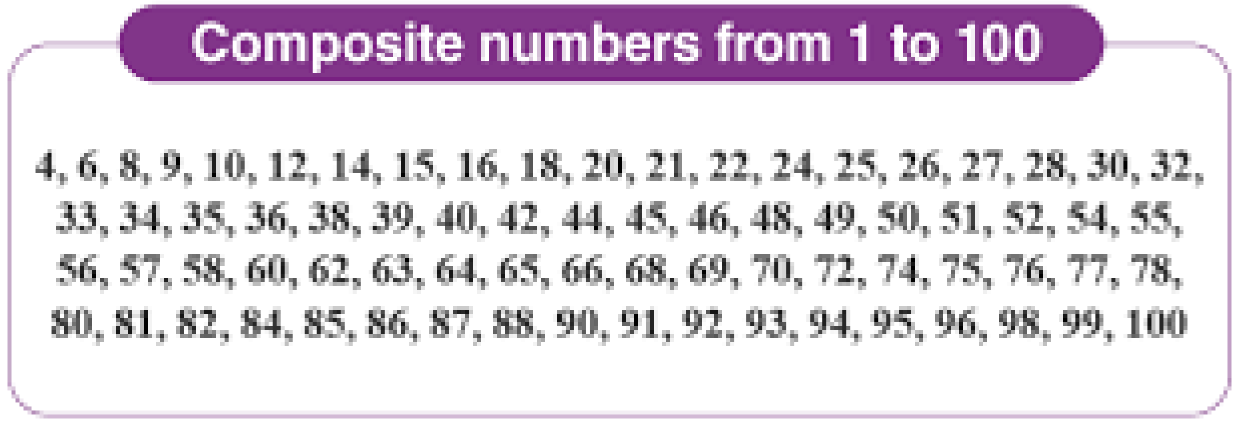
Prime Number

Composite Number

Exactly One Divisor

Exactly Two Divisors

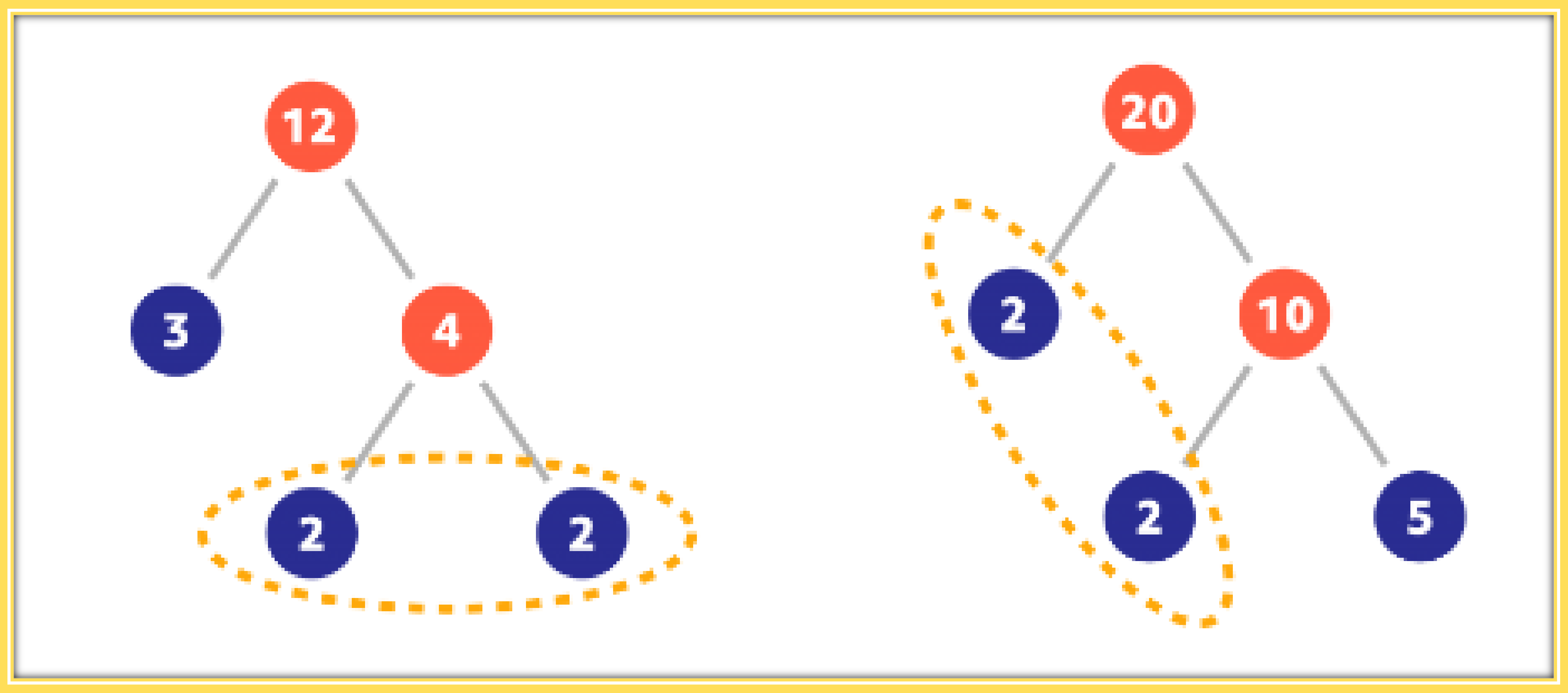
More than Two Divisors

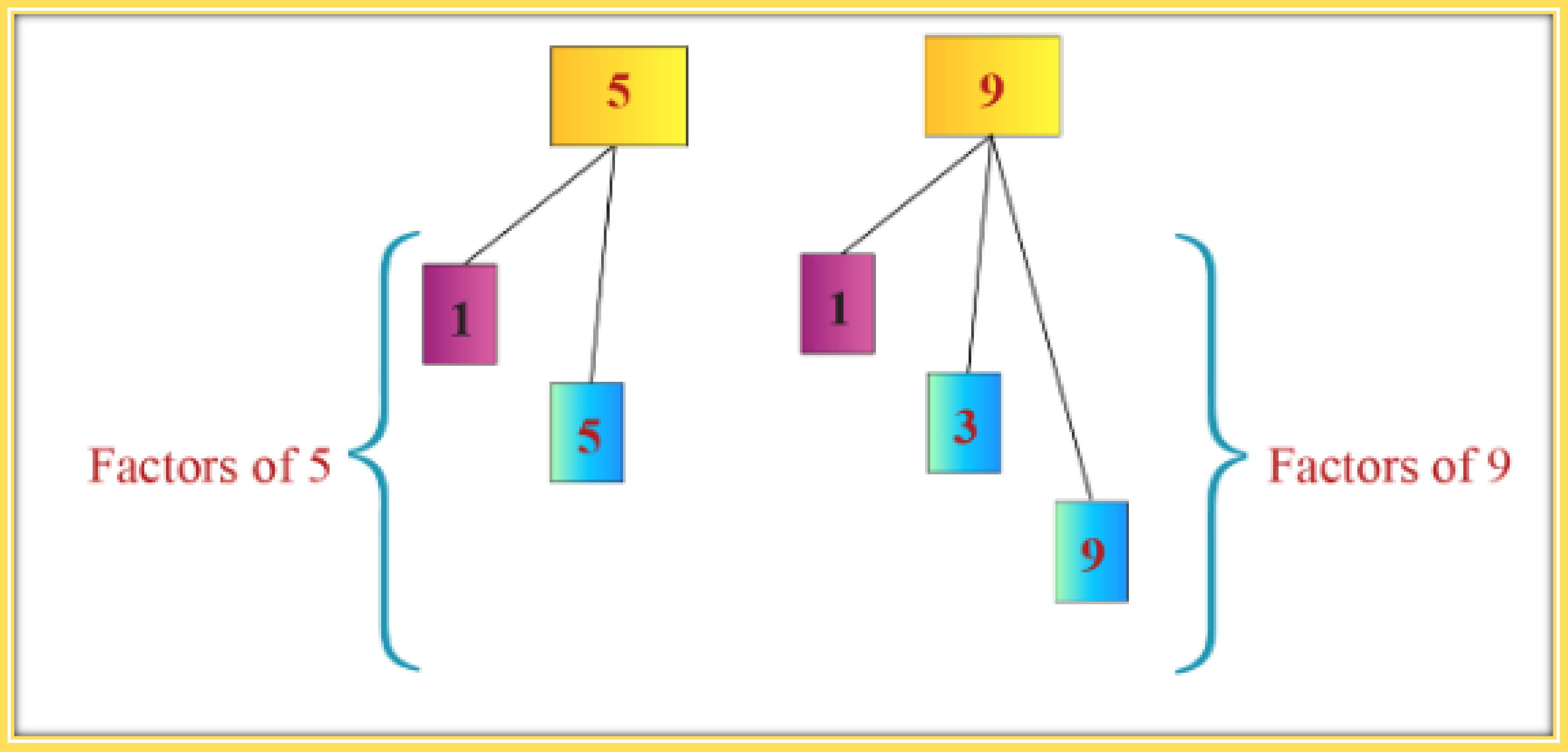


Composite numbers from 1 to 100

4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 62, 63, 64, 65, 66, 68, 69, 70, 72, 74, 75, 76, 77, 78, 80, 81, 82, 84, 85, 86, 87, 88, 90, 91, 92, 93, 94, 95, 96, 98, 99, 100

PRIME FACTORIZATION AND CO-PRIMES





Relatively Prime

Find Whether the following are Co-Primes or Not

- {6,10}
- {7,15}

Prime Factorization

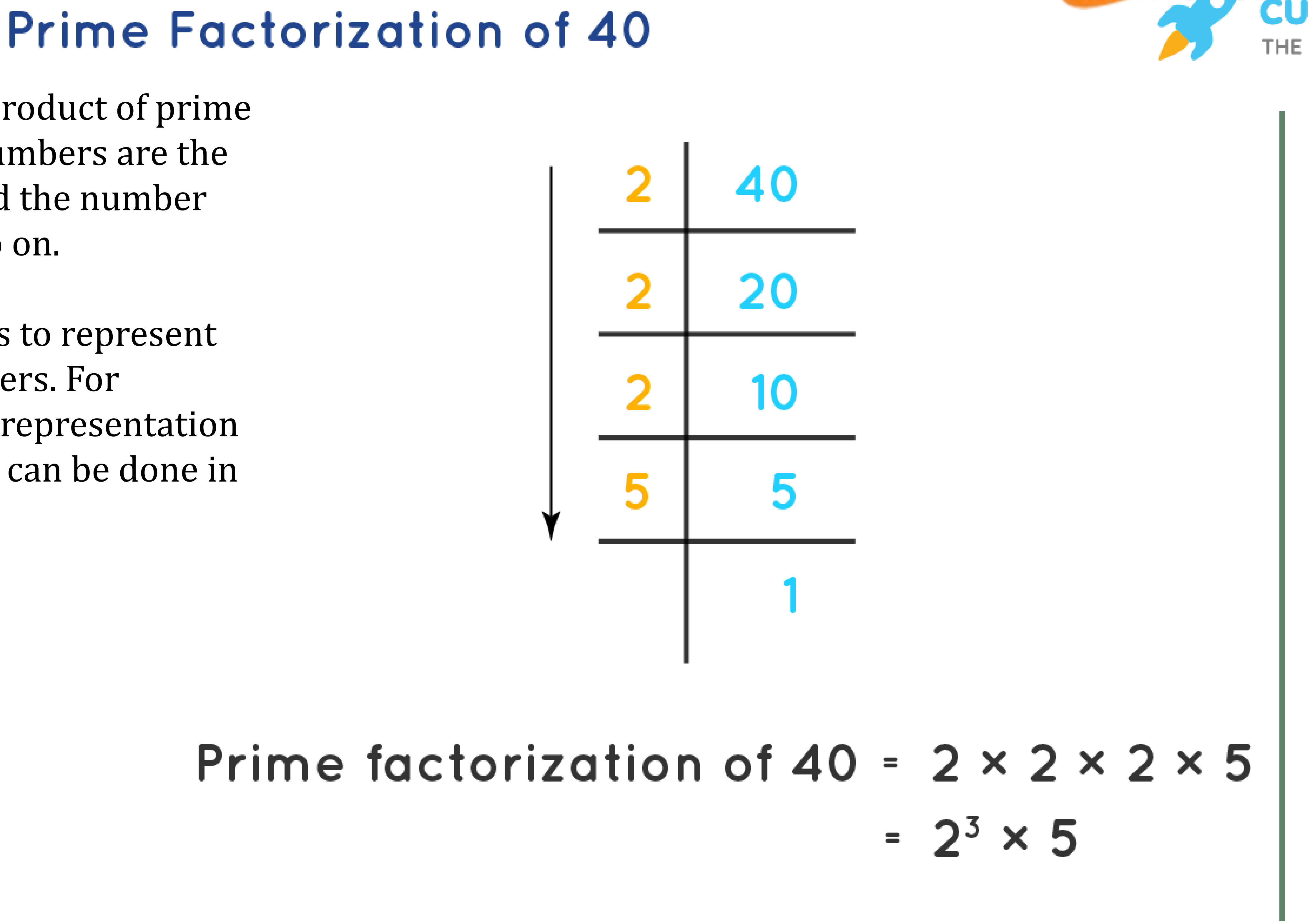
- ✓ Prime factorization is a way of expressing a number as a product of its prime factors. A prime number is a number that has exactly two factors, 1 and the number itself.

- ✓ Let's take an example of the number 30. We know that 30 is 5 × 6, but 6 is not a prime number. The number 6 is expressed as 2 × 3 since 3 and 2 are prime numbers. Therefore, the prime factorization of 30 is 2 × 3 × 5.

What is Prime Factorization?

- ✓ The process of writing a number as the product of prime numbers is prime factorization. Prime numbers are the numbers that have only two factors 1 and the number itself like 2, 3, 5, 7, 11, 13, 17, 120, and so on.

- ✓ Prime factorization of any number means to represent that number as a product of prime numbers. For example, prime factorization of 40 is the representation of 40 as a product of prime numbers and can be done in the following way:



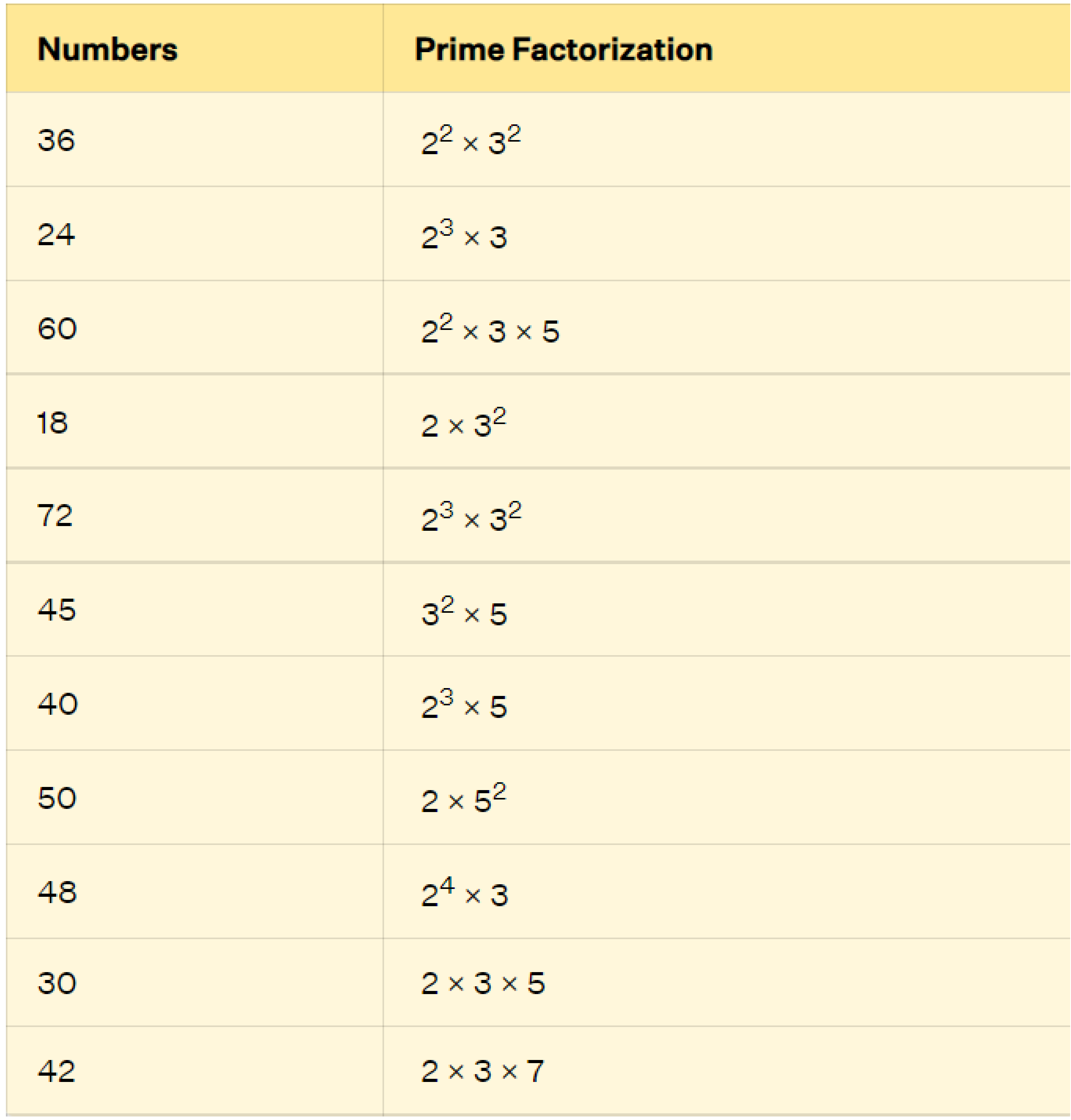
Prime Factorization of 40

2	40
2	20
2	10
5	5
	1

Prime factorization of 40 = $2 \times 2 \times 2 \times 5$

= $2^3 \times 5$

Prime Factorization of a Number



Numbers	Prime Factorization
36	$2^2 \times 3^2$
24	$2^3 \times 3$
60	$2^2 \times 3 \times 5$
18	2×3^2
72	$2^3 \times 3^2$
45	$3^2 \times 5$
40	$2^3 \times 5$
50	2×5^2
48	$2^4 \times 3$
30	$2 \times 3 \times 5$
42	$2 \times 3 \times 7$

What are Factors and Prime Factors?

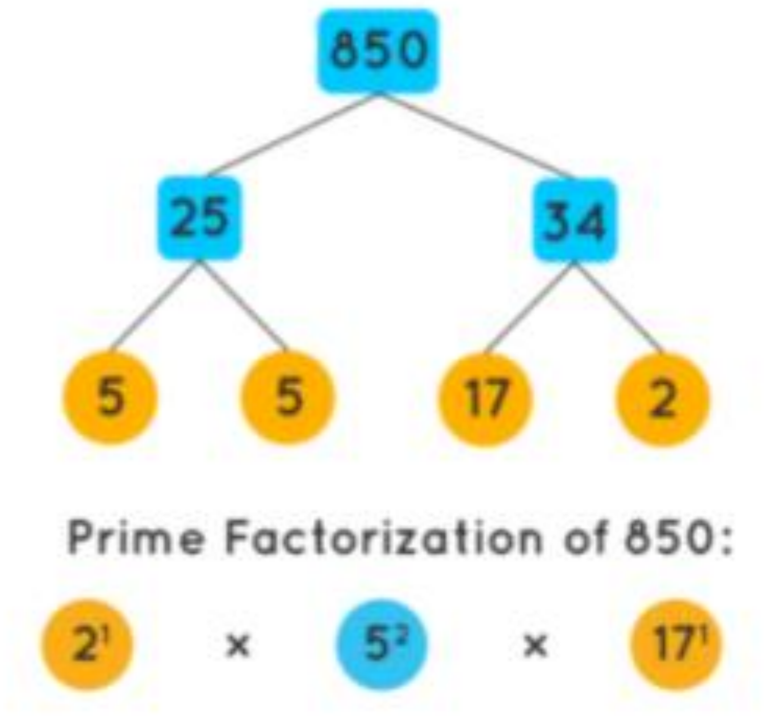
- ✓ Prime factorization is similar to factoring a number and considering only the prime numbers (2, 3, 5, 7, 11, 13, 17, 120, and so on) among all the factors. The factors are the numbers that divide the original number completely and can't be split into more factors are known as the prime factors.

- ✓ Factors of a number are the numbers that are multiplied to get the original number. For example; 4 and 5 are the factors of 20, i.e. 4 × 5 = 20, whereas prime factors of a number are the prime numbers that are multiplied to get the original number. For example: 2, 2, and 5 are the prime factors of 20, i.e. 2 × 2 × 5 = 20.

Prime factorization using factor tree method
Division method of prime factorization

Prime Factorization using Factor Tree Method

- ✓ Step 1: Consider the number as the root of the tree that is at the top of the factor tree.
- ✓ Step 2: Then write down the corresponding pair of factors as the branches of the tree.
- ✓ Step 3: Factorize the composite factors that are found in step 2, and write down the pair of factors as the next branches of the tree.
- ✓ Step 4: Repeat step 3, until we get the prime factors of all the composite factors.



Prime Factorization using Factor Tree Method

- ✓ Step 1: Divide the number by the smallest prime number such that the smallest prime number should divide the number completely.
- ✓ Step 2: Again, divide the quotient of step 1 by the smallest prime number.
- ✓ Step 3: Repeat step 2, until the quotient becomes 1.
- ✓ Step 4: Finally, multiply all the prime factors that are the divisors of the division.

Definition 01

The integer factorization problem is the following: given a positive integer N, compute its decomposition into prime numbers N = Q p ei i (unique up to reordering).

Definition 02

An integer is B-smooth if all its prime factors are smaller than B.

Definition 03

The sub exponential function is

$$LN\ (\alpha, c) = \exp\ c(\log N)\ \alpha\ (\log \log N)\ 1-\alpha$$

Definition 04

The smoothness test problem is as follows:

Given a number N and a bound B, decide whether N is B-smooth

Assessment

Can you help Charlize to express 1080 as the product of prime factors? Also, can you tell if this factorization is unique?

REFERENCES

William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

THANK YOU