**Chapter 4: Number Theory and Cryptography**

Table of Contents

[4.1 Divisibility and Modular Arithmetic 2](#_Toc44627441)

[Arithmetic Modulo 5](#_Toc44627442)

[4.2 Integer Representations and Algorithms 6](#_Toc44627443)

[Binary Expansion 6](#_Toc44627444)

[Octal Expansion 6](#_Toc44627445)

[Hexadecimal Expansion 6](#_Toc44627446)

[Base Conversion 7](#_Toc44627447)

[Conversion Between Binary, Octal and Hexadecimal Numbers 7](#_Toc44627448)

[Binary Addition 8](#_Toc44627449)

[Binary Multiplication 8](#_Toc44627450)

[Algorithm for and 9](#_Toc44627451)

[4.6 Cryptography 11](#_Toc44627452)

[Public Key Cryptography 11](#_Toc44627453)

[Block Ciphers 11](#_Toc44627454)

## 4.1 Divisibility and Modular Arithmetic

When an integer is divided by another integer, it gives an integer as a result. Thus, .

Definition 1:

If and are integers and and there is an integer such that , we say “ divides ”. This can also be written as or .

By this definition since is not an integer, but since .

Dividing an integer by another integer may also result in an integer remainder. Thus, and .

Definition 2:

If and are integers and there is an integer such that and an integer such that , then where is the quotient and is the remainder.

Definition 3:

If and are to integers and is a positive integer such that (i.e. ), then (this means ).

This statement is true since , an integer.

Definition 4:

If and are two integers and is a positive integer, then if and only if (i.e. and have the same remainder when divided by )

This statement is true since (i.e. ).

Definition 5:

Given that is a positive integer, and are congruent modulo if and only if there exists an integer such that .

Since , . From definition 3, we know this means .

This statement is true since , where .

Definition 6:

Let be a positive integer. If there exist integers , , and such that

and , then and .

Thus .

Thus .

and

### Arithmetic Modulo

For a set of non-negative integers less than a positive integer , meaning ,

Addition Modulo :

Multiplication Modulo :

These operations are called arithmetic modulo .

## 4.2 Integer Representations and Algorithms

Binary Expansion

For a binary number where , the decimal form is:

Octal Expansion

For an octal number where , the decimal form is:

Hexadecimal Expansion

For a hexadecimal number where , the decimal form is:

Base Conversion

To convert a decimal number to a base number , where ,

while ,

Thus,

Conversion Between Binary, Octal and Hexadecimal Numbers

One octal digit corresponds to three binary digits. One hexadecimal digit corresponds to 4 binary digits.

Thus,

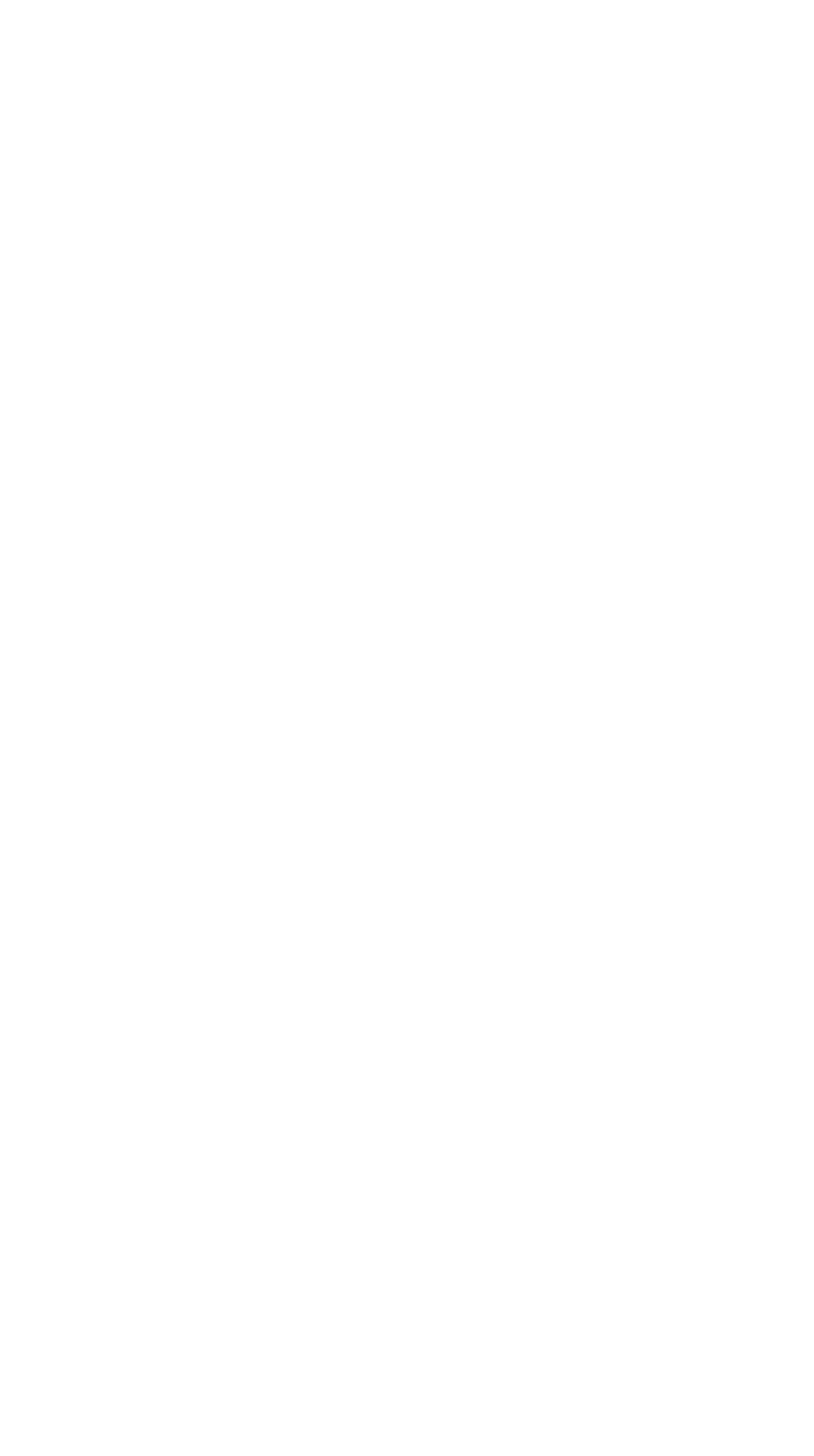
Binary Addition

( signifies binary multiplication)

Binary Multiplication

For two -bit Binary numbers and ,

Thus, if and if . Every time a term is multiplied by , the binary expansion is shifted one place to the left and a is added to the tail of the expansion.



Here,

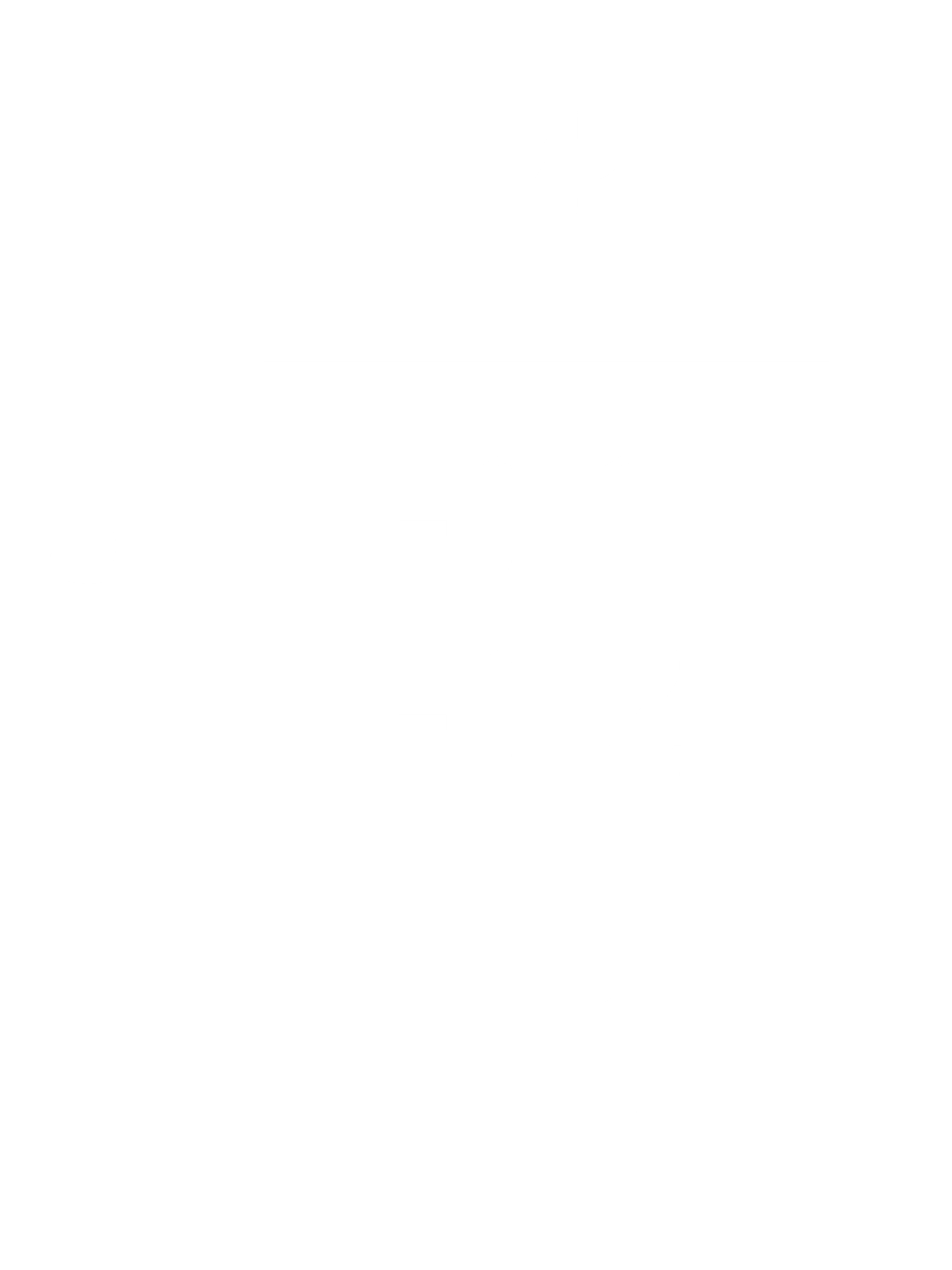
Algorithm for and

Let and be integers, where . To find and ,

while

if and

This algorithm is not normal division. For negative numbers, it follows the logic that the larger negative number is actually less than the smaller negative number, and performs the division accordingly. For example, for ,



Here, initially, and . Following the algorithm, at the end of the while loop, and . Then, since is negative, and .

## 4.6 Cryptography

### Public Key Cryptography

The Caesar’s Cipher is a method of cryptography that takes each character and shifts it forward by values. It considers to have the value , and each alphabet to have the consecutive values until , with a value of . Thus, the word HELLO, with code becomes KHOOR with code . The value is known as the key. To decrypt the message, must be subtracted from the value of each character.

The Caesar’s Cipher specifies that the key value must be . The Public Key Cryptography method is exactly the same, but more general in that the key value is not fixed. For this method,

Encryption:

Decryption:

Both of these methods fall under the category of classical cryptography, specifically, shift ciphers.

### Block Ciphers

Block Ciphers divide the characters into blocks, ignoring spaces. So, for example, with block size , HELLO WORLD is divided into 3 blocks, HELL OWOR LDAC. The actual text ends before the third block is filled however, leaving two spaces left to be filled. These are filled with random characters. Next, the characters are shifted using a key , as with shift ciphers.

An alternative to shifting the characters is a method known as transposition. In it, the characters of each block switch positions. So, the block OWOR could become WROO. A set is first defined with a cardinality equal to the block size. So, for the above example, . Next, the transpositions are defined. Say , , and . This means that the character in the first position must be shifted to the third position, the character in the second position must be shifter to the first position and so on. To decrypt the message, the inverse functions of the transposition must be defined. Thus, , , and .