My cryptography book

John Doe (February 4, 2023)

Contents

Chapter 1

Basic number theory

Definition 1.0.1. Let $m, n \in \mathbb{Z}$. Then we say that m **divides** n, and we write $m \mid n$, if there is some $x \in \mathbb{Z}$ such that $mx = n$, i.e.,

$$\exists x \in \mathbb{Z} \cdot [mx = n]$$

Proposition 1.0.1. *Let $a \in \mathbb{Z}$.*

(a) Then $1 \mid a$.
(b) If $a \neq 0$, then $a \mid 0$.
(c) (Reflexive) If $a \neq 0$, then $a \mid a$.
(d) If $a \mid b$ and $b \mid a$, then $a = \pm b$.
(d) (Transitive) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Chapter 2

Classical ciphers

2.1 Shift cipher

Definition 2.1.1. The **shift cipher** (E, D) is given by

$$E(k, x) = x + k \pmod{26}$$

and

$$D(k, x) = x - k \pmod{26}$$

Historically the shift cipher with key $k = 3$ was used by Julius Caesar and is called the **Caesar cipher**.

2.2 Affine cipher

2.3 Vigenère cipher

2.4 Substitution cipher

2.5 Permutation cipher

2.6 Hill cipher

2.7 One-time pad cipher

2.8 Linear feedback shift register

Chapter 3

Group theory

3.1 Definitions

The most basic mathematical object is $\mathbb{Z}$. $\mathbb{Z}$ has two opertions: addition and multiplication. We first abstract the study of $\mathbb{Z}$ by focusing on just one operation, the $+$.

Definition 3.1.1. $(G, *, e)$ is a **group** if G is a set and $*$ satisfies

group

(C) If $x, y \in G$, then $x * y \in G$. In other words $* : G \times G \to G$ is a binary operator.

(A) If $x, y, z \in G$, then $(x * y) * z = x * (y * z)$.

(I) If $x \in G$, then there is some $y \in G$ such that $x * y = e = y * x$. y is called an **inverse** of x. Later we will see that the inverse of x is uniquely determined by x.

inverse

(N) If $x \in G$, then $x * e = x = e * x$.

Definition 3.1.2. $(G, *, e)$ is an **abelian group** if $(G, *, e)$ is a group such that if $x, y \in G$, then $x * y = y * x$. In other words, $(G, *, e)$ is an abelian group if $(G, *, e)$ is group and $*$ is a commutative operator.

abelian group

The reason for now including the commutativity condition for groups is because there are many important groups which are not abelian.

Chapter 4

Ring theory

Chapter 5

Field theory

Index

Bibliography

[1] Leslie Lamport, *LaTeX: a document preparation system*, Addison Wesley, Massachusetts, 2nd edition, 1994. (EXAMPLE)