My notes on cryptography

Omid Bodaghi

March 1, 2025

Contents

Part I

Prerequisites

Chapter 1

Introduction to Cryptography

1.1 Historical Background

Definition 1.1. A *cryptosystem* is a pair of algorithms for encryption and decryption.

Example 1.1. The Caesar cipher shifts each letter by a fixed number of positions [Dés86].

1.2 Basic Concepts

Theorem 1.1. *If a cryptosystem is perfectly secure, then the key must be at least as long as the message.*

References

[Dés86] Jacques Désarménien. *TEX for Scientific Documentation: Second European Conference, Strasbourg, France, June 19-21, 1986. Proceedings*. Vol. 236. Springer Science & Business Media, 1986.

Part II

Zero Knowledge Proofs