CO 487 Course Notes

Applied Cryptography

Michael Socha

University of Waterloo

Winter 2019

Contents

1 Course Overview

This course is an applied introduction to modern cryptography. Topics covered include:

- Symmetric-key encryption
- Hash functions
- Authenticated encryption
- Public-key encryption
- Signature schemes
- Key establishment
- Key management
- Examples of deployed cryptography (e.g. SSL, cryptocurrencies, WPA)

2 Introduction - What is Cryptography?

Information security (also known as cybersecurity) deals with protecting information assets from unauthorized acquisition, damage, disclosure, manipulation, loss, or use. Cryptography deals with the mathematical, algorithmic and implementation aspects of information security.

Cybersecurity more broadly includes the study of computer security, network security and software security.

2.1 Goals of Cryptography

In short, cryptography is about securing communications in the face of malicious adversaries. When describing cryptographic scenarios, Alice and Bob are used to indicate two parties who wish to communicate with one another across some channel, while Eve is a malicious adversary. Eve may attempt to read or modify the data being transmitted.

The main goals of cryptography are to provide:

- **Confidentiality:** Keeps data secret from unauthorized entities.
- **Data integrity:** Ensures data has not been altered by unauthorized means.
- **Data origin authentication:** Determines the sender of data.
- **Non-repudiation:** Provides proof of data origin and integrity, which can be used to prevent senders from disputing a previous action.