CO 487 Course Notes

Applied Cryptography

Michael Socha

University of Waterloo

Winter 2019

Contents

1 Course Overview **1**

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)