Applied Cryptography

thgoebel@ethz.ch

ETH Zürich, FS 2021

This documents is a **short** summary for the course *Applied Cryptography* at ETH Zurich. It is intended as a document for quick lookup, e.g. during revision, and as such does not replace reading the slides or a proper book.

We do not guarantee correctness or completeness, nor is this document endorsed by the lecturers. Feel free to point out any erratas.

Contents

1 Symmetric Cryptography

1.1 Block Ciphers

1.2 Symmetric Encryption

1.3 Hash Functions

1.4 Message Authentication Codes MACs

1.5 Authenticated Encryption