Introduction to Modern Cryptography

gelesen von Prof. Rösler
an der FAU Erlangen
in LaTeX umgesetzt von Moritz Palm

October 17, 2024

Contents

1 Introduction

1.1 Motivation

1.1.1 Caesars Cipher

1.1.2 Enigma

1.1.3 Cryptology

Cryptology (translated from greek "studying secrets") can be divided into two separate branches: Cryptography, the science of designing constructions and proving their security and Cryptanalysis, the science of breaking constructions or their underlying assumptions

1.1.4 Kerkhoffs Principle

> A cryptographic construction should be secure even if the adversary knows all details about the construction with the exception of the secret key material. In particular, all algorithms should be publicly known.

1.1.5 Provable Security

1. Definition of Security
   a) Goal(s) of adversary (e.g. learning the message m, authenticating as A, ...)
   b) Capabilities of adversary (e.g. observing cybertexts, knowing parts of plaintexts, ...)
   c) Functionality of protocol class (e.g. delivery of payload messages, ...)
2. Specification of construction
3. Specification of computational assumptions
   - Existence of secure components (e.g. hash function, secure[1] randomness generator, ...)
   - of computational problems (e.g. factoring, discrete logarithm, learning with errors, ...)

[1] with regard to its definition

  - Computational resources of users & adversary (e.g. runtime, memory, classical vs. quantum computing, ...)
  - ...

4. Proof of security $\rightsquigarrow$ Reduction

1.2 TLS & Double Ratchet

1.2.1 Transport Layer Security (TLS)

Cryptographic protocol designed to enable secure communication over a network (e.g. HTTPS). Currently standardized in version 1.3. Browser vendors, standardization experts and academic experts were involved in the development. Its security has been proven using both reductions and tool-based approaches.

1.2.2 Double Ratchet Algorithm

- used in Signal, Whatsapp, iMessage, ...
- de facto Standard (but not standardized by a standardization organization)
- Analyses and extensions developed by academia

2 Key Derivation