I. Motivation and topics

Cryptography scientific study of techniques for securing digital information, transactions, and distributed computations.

Main goals

- confidentiality
- privacy
- integrity
- authenticity
- non-repudiation

while maintaining avalability

Course concentrates on authenticity, non-repudiation, and privacy (a little bit).

Scenario

wants to listen
change
impersonate

Scenario can be more complex

- more participants
- different roles of participants
- more complex tasks

Scenario

wants to listen
change
impersonate

Goals & methods

- data integrity - hash functions, message authentication codes
- entity/data authentication - message authentication codes, digital signatures, identification protocols,
- non-repudiation - digital signatures

Goals and methods

authentication

- message authentication codes
- digital signatures
- identification protocols

non-repudiation

- digital signatures, identification protocols

privacy

- multi-party computations
- oblivious transfer

Authentication

data origin authentication

- connected to messages

entity authentication

- access control

Basic principles

0. **Principle (Kerckhoff)** The cryptographic scheme must not be required to be secret and must be able to fall into the hands of the adversary without inconvenience.

1. **Principle** One must formulate a rigorous and precise definition of security for a given cryptographic problem.

2. **Principle** If the security of a cryptographic construction relies on an unproven assumption, this must be stated precisely.

3. **Principle** Cryptographic constructions require rigorous proofs of security with respect to the security definition and the underlying assumptions.

Assumptions

1. **Concrete assumptions** „The following mathematical/ computational problem is hard to solve.“

➔ factoring, discrete logarithms

2. **General assumptions** „Computationally hard problems of the following type exist.“

➔ languages in NP\P exist, one-way functions exist.

mostly follow 2. ➔ foundations of cryptography

Organization

Information about this course

http://cs.uni-paderborn.de/cuk/lehre/veranstaltungen/ss-2016/cryptographic-protocols/

Here you find

- **handouts**
- **slides**
- **literature**
- **announcements**

Prerequisites

- elementary probability theory
- algorithm theory
- basic complexity theory
- very basic number theory