Cryptographic Hash Functions
Welcome to the Problem Sessions!

Summer 2019

Chair of Media Security Prof. Stefan Lucks
Nathalie Dittrich, Eik List
<firstname>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

April 4, 2019

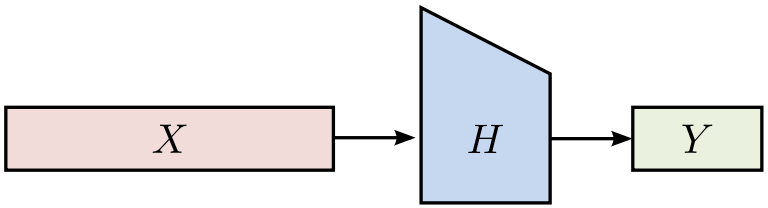
Welcome!

Welcome to the problem session of **Cryptographic Hash Functions**!

Hash functions?

Working horses of cryptography:

- Map variable-length inputs to fixed-length outputs $H : \{0,1\}^* \to \{0,1\}^n$



Basic purpose:

- Fingerprinting (unkeyed)
- Data Authenticity (keyed)

Usage in higher-level schemes:

- Hash-then-Sign in signature schemes
- Hash-then-PRF in MACs
- Primitive for password hashing/key derivation

Problem Sets

- You will most likely learn little without working on the problem sets
- Learning groups of two (or three) persons are encouraged

Admission to the Exam:

- Solve all n problem sets with $\geq 25\%$ **or**
- Solve $n-1$ problem sets with $\geq 25\%$ and ≥ 2 with $\geq 50\%$

Submission Guides for Problem Sets:

- All group members have to be mentioned in the documentation
- Deadline: before the problem sessions (by e-mail 11:00 AM or by print-out)

Final Grade Bonus

1/3 Final-Grade Bonus:

- n problem sets with $\geq 25\%$ of the points **and** ≥ 3 problem sets with $\geq 50\%$ of the points

2/3 Final-Grade Bonus:

- n problem sets with $\geq 25\%$ of the points **and** $\geq n-1$ problem sets with $\geq 50\%$ of the points

First Problem Set and Next Meeting

- Considers the basics of cryptographic hash functions
- Due: 18 April
- Online on the website of the problem session:
  `https://www.uni-weimar.de/de/medien/professuren/medieninformatik/mediensicherheit/teaching/ss-2019/cryptographic-hash-functions-problem-session/`

Next Meeting:

- 18 April, same time (11:00 AM), same place

Topics

- General Information on Hash Functions
- Iterated Cryptographic Hash Functions
- Generic Attacks
- Block-cipher-based Compression Functions
- Dedicated Compression Functions
- Tree Hashing and Hash Trees
- The SHA-3 Competition
- Password-Hashing Basics
- Catena
- The Password-Hash Competition

We Will Consider

- Theory
  - Basic security notions
  - Basic proof techniques
  - Algorithms to find collisions
  - Foundations of number theory for universality
- Design
  - Merkle-Damgård, Haifa, SHA-2, SHA-3
- Usage
- Analysis
  - Scheme level: Block-cipher-based compression functions
  - Primitive level: Why is MD4 broken?
  - Rebound + zero-sum attacks
- Implementations in Python/C

Questions?