SCIENCE
PASSION
TECHNOLOGY

Introduction

Lukas Helminger

Modern Public-Key Cryptography – SS 2022

Team

Lukas Helminger

Daniel Kales

What this lecture is (not) about

Formalization of "secure"	🟥🟥🟥🟥🟥
Mathematics of cryptography	🟥🟥🟥□□
Proving crypto secure	🟥🟥🟥🟥🟥
Implementing schemes	□□□□□
Discussing concrete security parameters	🟥🟥□□□
Learning "future" crypto	🟥🟥🟥🟥🟥

Course overview

- Standard Public-Key Crypto
  - Basics: Notation, Complexity Theory, Reductions, Hardness Assumptions
  - Public-Key Encryption Scheme
  - Digitial Signatures
  - Provable Security
- Fancy Public-Key Crypto
  - Zero-Knowledge
  - Post-Quantum (Lattices)
  - TBA

Lecture material

- Slides are available
- No printed lecture notes
- Most topics covered by:

📕 Smart
Cryptography: An Introduction.

📕 Jonathan Katz and Yehuda Lindell
Introduction to Modern Cryptographys

Assessment I

- Several exercises
  - ☑ Tick the examples you solved before each exercise class
  - 👥 Solutions are presented (by you!) & discussed in class
  - % You must solve 50% of all examples – bonus points for more:

$\geq 50\,\%$	$+0$ points
$\geq 60\,\%$	$+1$ points
$\geq 70\,\%$	$+2$ points
$\geq 80\,\%$	$+3$ points
$\geq 90\,\%$	$+4$ points

Assessment II

- Examination (32 points)

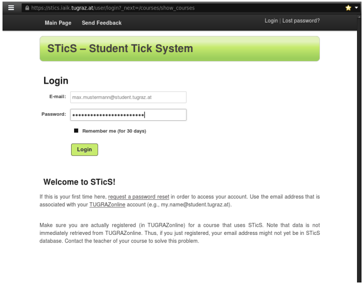
  📅 22. 06. 2021 Exam

Points	Grade
$<$ 16 points	5
$\geq$ 16 points	4
$\geq$ 20 points	3
$\geq$ 24 points	2
$\geq$ 28 points	1

Exercises – STicS

Tick the tasks you solved in the Student Tick System (STicS):

tc.tugraz.at


https://stics.iaik.tugraz.at/user/login?_next=/courses/show_courses
Main Page
Send Feedback
Login | Lost password?

STicS – Student Tick System

Login

E-mail: max.mustermann@student.tugraz.at

Password: •••••••••••••••••••••••

■ Remember me (for 30 days)

Welcome to STicS!

If this is your first time here, request a password reset in order to access your account. Use the email address that is associated with your TUGRAZonline account (e.g., my.name@student.tugraz.at).

Make sure you are actually registered (in TUGRAZonline) for a course that uses STicS. Note that data is not immediately retrieved from TUGRAZonline. Thus, if you just registered, your email address might not yet be in STicS database. Contact the teacher of your course to solve this problem.

Note: Even if you’ve used STicS before, you might have to request a new password.

When and Where?

⌛ 12:00 STicS tick deadline

🕒 14:00–16:00 Lecture/Exercises

Links

- Course website, slides & links:

  https://www.iaik.tugraz.at/course/selected-topics-in-cryptography-and-privacy-modern-public-key-cryptography-705008-sommersemester-2022/

- STicS to tick exercise tasks: https://stics.iaik.tugraz.at

Questions?