

Introduction

Lukas Helminger

Modern Public-Key Cryptography – SS 2021

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
 - Digital 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:

≥ 50 %	+0 points
≥ 60 %	+1 points
≥ 70 %	+2 points
≥ 80 %	+3 points
≥ 90 %	+4 points

Assessment II

- Examination (32 points)



30.06.2021 Exam

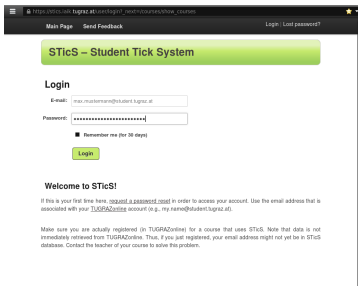
??.??..2021 “Second-chance” Exam

Points	Grade
< 16 points	5
≥ 16 points	4
≥ 20 points	3
≥ 24 points	2
≥ 28 points	1

Exercises – STicS

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


<https://stics.iaik.tugraz.at>



The screenshot shows the login page of the Student Tick System (STicS). At the top, there is a navigation bar with links for 'Main Page' and 'Send Feedback', and a 'Login / Lost password?' link. Below this is a green header with the text 'STicS – Student Tick System'. The main content area is titled 'Login' and contains an 'E-mail:' field with the value 'max.muellers@iaik.tugraz.at', a 'Password:' field with masked characters, and a 'Remember me (for 30 days)' checkbox. A green 'Login' button is positioned below the password field. Underneath the login form, there is a 'Welcome to STicS!' section with a small paragraph of instructions: '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@iaik.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

- actually 14:15–15:45

 MS Teams

Links



Course website, slides & links:

<https://www.iaik.tugraz.at/course/selected-topics-in-cryptography-and-privacy-modern-public-key-cryptography-705008-sommersemester-2021/>



STicS to tick exercise tasks:

<https://stics.iaik.tugraz.at>

Questions?