

# Einführung in die Informationssicherheit

Florian Mendel

**Institute for Applied Information Processing and Communications (IAIK)**

Graz University of Technology  
Inffeldgasse 16a, A-8010 Graz, Austria



<http://www.iaik.tugraz.at/>

# L0 – Organisatorisches

Einführung in die Informationssicherheit

# 705.026 Einführung in die Informationssicherheit

- 1VO + 1KU (1.5 + 1.5 ECTS)
- Pflichtfach für Softwareentwicklung u. Wissensmanagement, Telematik (nur VO) und Informatik
- Empfohlen für das 5. Semester (Telematik + SeW), bzw. 3. Semester Informatik
- Unterrichtssprache: Deutsch

# Ziele der Lehrveranstaltung

- Das Ziel dieser LV ist es, die StudentInnen mit Begriffen und Konzepten der Informationssicherheit vertraut zu machen
- Moderne Informationssicherheit beinhaltet verschiedenste Aspekte:
  - Die LV behandelt einige dieser Aspekte
  - Darüber hinaus gibt die LV einen Überblick über die zugrunde liegenden Konzepte und Lösungsmöglichkeiten für die Problemstellungen

- Florian Mendel
- Studienassistenten:
  - Daniel Brolli
  - Robert Primas
  - Stefan Steinegger

# Inhalte

- Kryptographie
- Elektronische Unterschriften und PKI
- Electronic Commerce (e-Payment)
- Netzwerk-Sicherheit
- Operating System Security
- Implementierungs-Sicherheit
- Privacy
- Bachelor@IAIK

# Unterlagen

- Die aktuellen Folien und ein Skriptum (WS 12/13) findet man auf der Homepage der Vorlesung.
- Es wird empfohlen, nicht nur ausschließlich aus dem Skriptum zu lernen:
  - Die Informationen im Skriptum sind relativ komprimiert.
  - In der Vorlesung werden die Konzepte genauer erklärt und erhellende Beispiele gebracht.
  - Es wird jedoch nicht mehr zur schriftlichen Prüfung verlangt, als im Skriptum behandelt wird.

# Download von Passwort-geschützten Dateien

- Die meisten Dateien auf der EIS-Website sind passwortgeschützt.
- Um das Passwort zu erhalten, müssen Sie folgendes Rätsel lösen:

- Entschlüsseln Sie die folgende Nachricht:

IFXUFXXBTWYKZJWINJATWQJXZSLXIFYJNJSGJXYJMYF  
ZXIJSFSKFSXLXGZHMXYFGJSIJWJWXYJSXJHMXBTJWYJW  
INJXJXXFYEJXUQZXIJWEFMQEBJNYFZXJSIANJWEJMS

- Hinweis: Es wurde eine Cäsar-Chiffre benutzt 😊



# Benotung

- Für die VO ist eine schriftliche Prüfung zu absolvieren, für die KU ist ein Projekt zu bearbeiten.
- Die schriftliche Prüfung ist kurz (1 Stunde) und überprüft, wie genau Sie die Themengebiete studiert haben.
- Es gibt jeweils 10 Punkte zu erreichen, eine positive Note hat man ab 5 Punkten.

# Prüfungen

- Innerhalb des Studienjahres gibt es 6 Möglichkeiten, schriftliche Prüfungen abzulegen
  - Kurz nach Ende der Vorlesung (10.12.2014)
  - Semesterende
  - Ca. alle 2 Monate
- Auf der Homepage finden Sie gegen Ende der VO exemplarische Prüfungsfragen.
- Nach jedem Kapitel im Skriptum sind ebenfalls möglich Fragen aufgelistet!

# Konstruktionsübung

- Für die KU wird vertieft in einem der 7 Themengebiete gearbeitet.
- Es gibt 3 Studienassistenten die die Übung begleiten werden.
- Beachten Sie:
  - SIE machen die Übung, die Studienassistenten sind da um zu helfen, aber nicht, um Ihnen die Arbeit abzunehmen!
- Die möglichen Themen finden Sie auf der Website der LV.

# Konstruktionsübung

- Eine Gruppe besteht immer aus 4 Studenten:
- Verwenden Sie auch die Newsgroup um Gruppen zu bilden:
  - `tu-graz.lv.einfuehrunginformationssicherheit.  
partnersuche`
- Anmeldung erfolgt über das Student Tick System (STicS)
  - `https://stics.iaik.tugraz.at`
- **Deadline** für die Registrierung einer Gruppe ist der **15.10.2014**

# Konstruktionsübung

- Für jedes Themengebiet steht jeweils ein praktisches Projekt bzw. mehrere theoretische Aufgaben zur Auswahl
- Nach der Registrierung
  - Wird Ihrer Gruppe ein Studienassistent zugeordnet
  - Hat Ihre Gruppe ca. 4 Wochen Zeit, um eine Spezifikation für Ihre gewählte Aufgabenstellung (mit Hilfe des Stud.Ass.) zu erarbeiten.
- Die **Deadline** für die Projektspezifikation ist der **12.11.2014**.

# Konstruktionsübung

- Nachdem die Gruppe die Spezifikation abgegeben hat, arbeitet sie an der Aufgabenstellung unter Anleitung des Stud. Ass.
- Die Sprechstunden der Stud. Ass. werden nach Ende der Registrierung bekannt gegeben (20.10.2014)
- Die fertigen Projekte/Überblicksartikel müssen bis **21.01.2015** abgegeben werden (die **Deadline** ist STRENG).
- Danach wird es noch ein **Abgabegespräch** zum Projekt bzw. Überblicksartikel geben.

# Konstruktionsübung – Projekte

P1.1 Kryptografie Challenge

P2.1 Elektronischer Signaturen

P3.1 Electronic Payment Systems

P4.1 Attacken auf TLS

P5.1 Android Permission Framework

P6.1 Seitenkanalattacken auf Smartcards

P7.1 Mix Server / Mix Netz

# Konstruktionsübung – Überblicksartikel

T2.1 Asymmetrische Verschlüsselung

T2.2 Symmetrische Verschlüsselung

T3.1 Electronic Payment Systems

T4.1 Intrusion Detection

T4.2 Internet Protokoll Sicherheit

T5.1 Sicherheit in Linux/Unix/BSD

T5.2 Sicherheit in Android

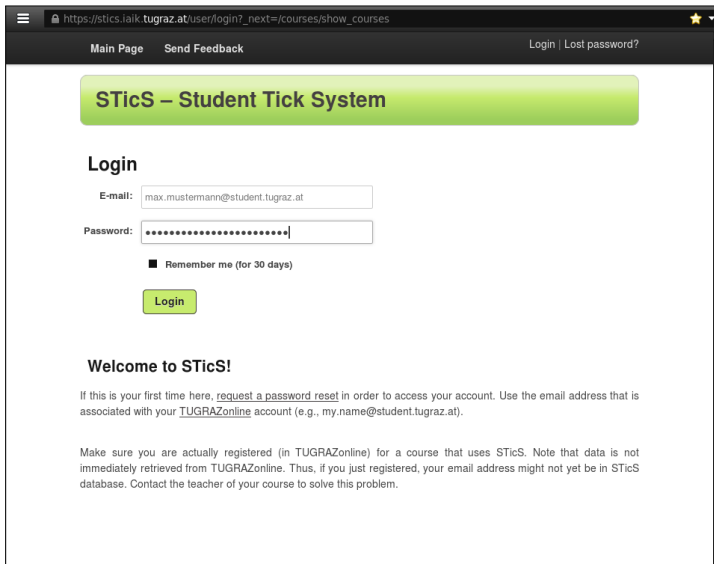
T6.1 Seitenkanalattacken

T6.2 Sicherheit von Programmiersprachen

T7.1 Privacy Enhancing Technologies



# Konstruktionsübung – Anmeldung



The screenshot shows a web browser window with the URL `https://stics.iaik.tugraz.at/user/login?_next=/courses/show_courses`. The page has a dark header with a hamburger menu icon, the URL, and a star icon. Below the header, there are links for "Main Page" and "Send Feedback" on the left, and "Login | Lost password?" on the right. The main content area features a green gradient box with the text "STicS – Student Tick System". Below this is a "Login" section with two input fields: "E-mail:" containing "max.mustermann@student.tugraz.at" and "Password:" containing a series of dots. A checkbox labeled "Remember me (for 30 days)" is positioned below the password field. A green "Login" button is located below the checkbox. Further down, a "Welcome to STicS!" section contains a paragraph of text and a note about registration.

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)

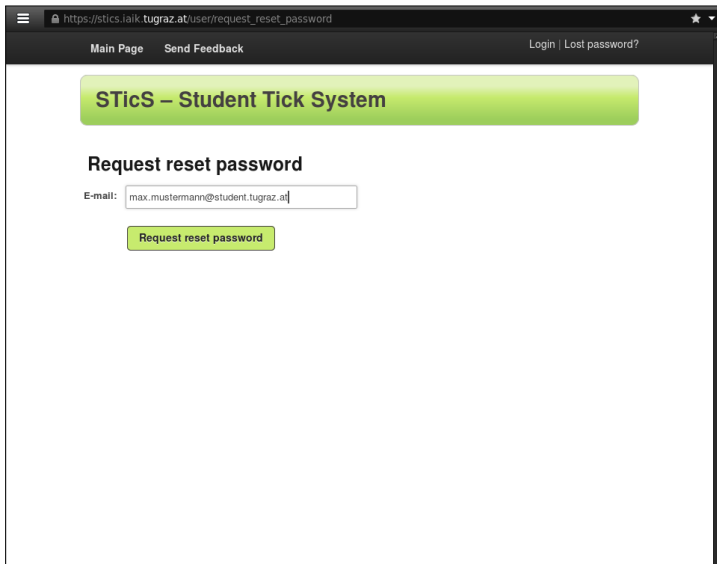
Login

### 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.

# Konstruktionsübung – Anmeldung



The screenshot shows a web browser window with the address bar displaying `https://stics.laik.tugraz.at/user/request_reset_password`. The page has a dark header with a hamburger menu icon, the text "Main Page" and "Send Feedback", and links for "Login" and "Lost password?". Below the header is a green gradient banner with the text "STicS – Student Tick System". The main content area is titled "Request reset password" and contains an "E-mail:" label followed by a text input field containing the email address "max.mustermann@student.tugraz.at". Below the input field is a green button labeled "Request reset password".

https://stics.laik.tugraz.at/user/request\_reset\_password

Main Page Send Feedback Login | Lost password?

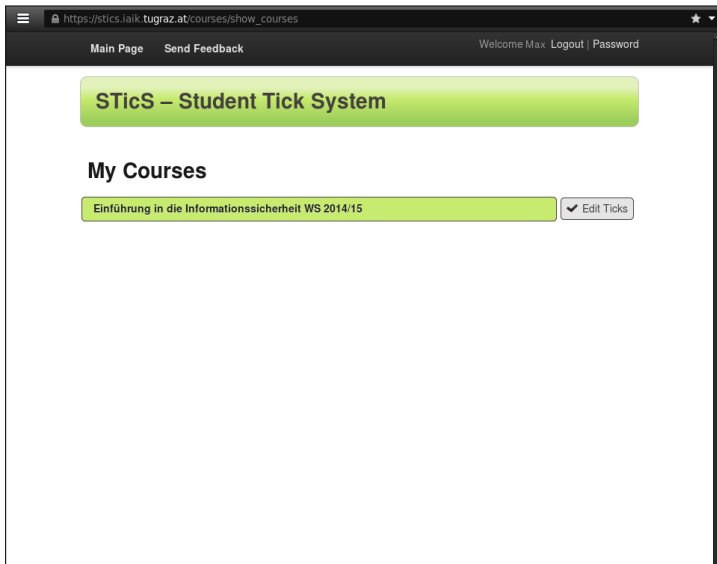
**STicS – Student Tick System**

**Request reset password**

E-mail:

**Request reset password**

# Konstruktionsübung – Anmeldung



# Konstruktionsübung – Neue Gruppe anlegen

The screenshot displays a web browser window with the URL `https://stics.laik.tugraz.at/student_detail/show_stats`. The page has a dark header with a menu icon, navigation links for "Main Page" and "Send Feedback", and a user greeting "Welcome Max" with links for "Logout" and "Password".

The main content area features a green gradient banner with the text "STicS – Student Tick System". Below this is a button labeled "Back to Courses".

The course title "Einführung in die Informationssicherheit WS 2014/15" is prominently displayed. Below the title, the user's details are listed: "Matriculation Nr 1234567", "Name Mustermann, Max", and "Group Standardgruppe".

A section titled "Team" contains two buttons: "Create New Team" (highlighted in green) and "Join Team".

# Konstruktionsübung – Neue Gruppe anlegen

The screenshot shows a web browser window with the URL `https://stics.laik.tugraz.at/teams/create_team`. The page has a dark header with a menu icon, navigation links "Main Page" and "Send Feedback", and user information "Welcome Max Logout | Password". A green banner at the top reads "STicS – Student Tick System". The main content area is titled "Einführung in die Informationssicherheit WS 2014/15: Create New Team". It contains three input fields: "Name" (set to "None"), "Password" (masked with dots), and "Topic" (set to "T7.1 Privacy Enhancing Technologies"). At the bottom are "Submit" and "Cancel" buttons.

https://stics.laik.tugraz.at/teams/create\_team

Main Page Send Feedback Welcome Max Logout | Password

**STicS – Student Tick System**

**Einführung in die Informationssicherheit WS 2014/15:  
Create New Team**

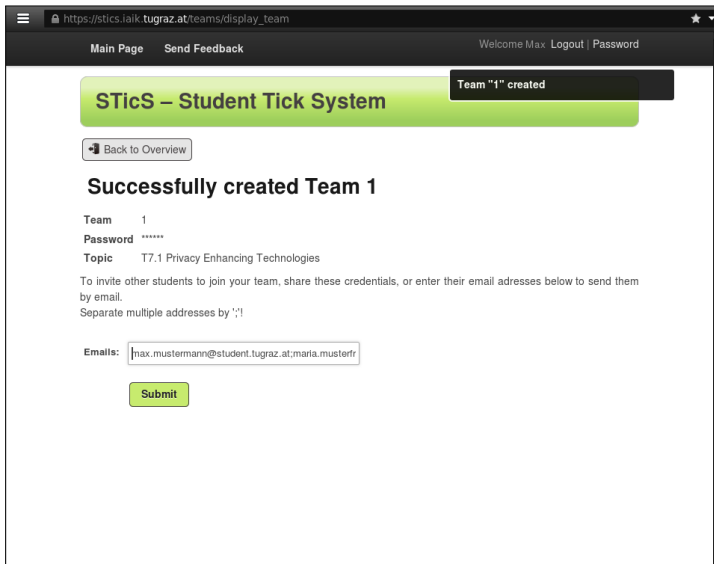
Name: None

Password: .....

Topic: T7.1 Privacy Enhancing Technologies

Submit Cancel

# Konstruktionsübung – Neue Gruppe anlegen





The screenshot shows a web browser window with the URL `https://stics.laik.tugraz.at/teams/display_team`. The page has a dark header with a menu icon, the URL, a star icon, and navigation links: "Main Page", "Send Feedback", "Welcome Max", "Logout", and "Password". A green banner at the top reads "STicS – Student Tick System". A dark notification box in the top right corner says "Team '1' created". Below the banner is a button labeled "Back to Overview". The main heading is "Successfully created Team 1". The form displays the following details:

- Team** 1
- Password** \*\*\*\*\*
- Topic** T7.1 Privacy Enhancing Technologies

Below the details, there is explanatory text: "To invite other students to join your team, share these credentials, or enter their email addresses below to send them by email. Separate multiple addresses by ','!"

The "Emails:" label is followed by a text input field containing the email addresses: `max.mustermann@student.tugraz.at;maria.musterfr`. Below the input field is a green "Submit" button.

# Konstruktionsübung – Gruppe anlegen

 [https://stics.laik.tugraz.at/student\\_detail/show\\_stats](https://stics.laik.tugraz.at/student_detail/show_stats) 

[Main Page](#) [Send Feedback](#) Welcome Max [Logout](#) | [Password](#)

## STiCS – Student Tick System

[Back to Courses](#)

### Einführung in die Informationssicherheit WS 2014/15

**Matriculation Nr** 1234567

**Name** Mustermann, Max

**Group** Standardgruppe

### Team

**Team** 1

**Topic** T7.1 Privacy Enhancing Technologies

**Members** Max Mustermann (max.mustermann@student.tugraz.at)

[Edit team](#) [Leave team](#)

### Submissions

[Upload new submission](#)

Date	Assignment	Submission	Points
2014-11-12 23:59:59	Design Document / Extended Abstract	✖	? / 0
2015-01-21 23:59:59	Final Project / Paper	✖	? / 10

# Konstruktionsübung – Gruppe beitreten

The screenshot shows a web browser window with the URL `https://stics.laik.tugraz.at/student_detail/show_stats`. The page has a dark header with a menu icon, navigation links "Main Page" and "Send Feedback", and a user greeting "Welcome Maria Logout | Password". Below the header is a green gradient banner with the text "STicS – Student Tick System". Underneath the banner is a button labeled "Back to Courses". The main content area features the course title "Einführung in die Informationssicherheit WS 2014/15" in bold. Below the title, the user's matriculation number "1234321" is displayed. A table-like structure shows the user's name as "Musterfrau, Maria" and the group as "Standardgruppe". A section titled "Team" contains two buttons: "Create New Team" and "Join Team".

https://stics.laik.tugraz.at/student\_detail/show\_stats

Main Page Send Feedback Welcome Maria Logout | Password

**STicS – Student Tick System**

Back to Courses

**Einführung in die Informationssicherheit WS 2014/15**

Matriculation Nr 1234321

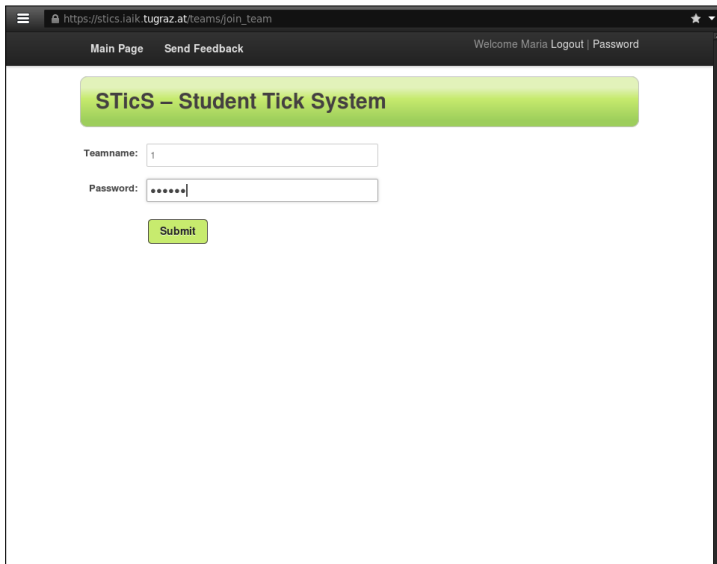
Name	Musterfrau, Maria
Group	Standardgruppe

**Team**

Create New Team Join Team



# Konstruktionsübung – Gruppe beitreten



The screenshot shows a web browser window with the address bar displaying `https://stics.laik.tugraz.at/teams/join_team`. The page has a dark header with a menu icon, navigation links "Main Page" and "Send Feedback", and a user status "Welcome Maria Logout | Password". The main content area features a green gradient box with the title "STicS – Student Tick System". Below this, there are two input fields: "Teamname:" with the value "1" and "Password:" with masked characters ".....". A green "Submit" button is positioned below the password field.

https://stics.laik.tugraz.at/teams/join\_team

Main Page Send Feedback Welcome Maria Logout | Password



## STicS – Student Tick System

Teamname: 1

Password: .....

Submit

# Konstruktionsübung – Abgabesystem

 [https://stics.iaik.tugraz.at/student\\_detail/show\\_stats](https://stics.iaik.tugraz.at/student_detail/show_stats) 

[Main Page](#) [Send Feedback](#) Welcome Maria Logout | Password

**STics – Student Tick System** Joined group!

[Back to Courses](#)

## Einführung in die Informationssicherheit WS 2014/15


**Matriculation Nr** 1234321  
**Name** Musterfrau, Maria  
**Group** Standardgruppe

### Team

**Team** 1  
**Topic** T7.1 Privacy Enhancing Technologies  
**Members** Max Mustermann (max.mustermann@student.tugraz.at)  
Maria Musterfrau (maria.musterfrau@student.tugraz.at)



[Edit team](#) [X Leave team](#)

### Submissions

 Upload new submission

Date	Assignment	Submission	Points
2014-11-12 23:59:59	Design Document / Extended Abstract	✗	? / 0
2015-01-21 23:59:59	Final Project / Paper	✗	? / 10

# Konstruktionsübung – Abgabesystem

 [https://stics.laik.tugraz.at/student\\_detail/edit\\_submissions](https://stics.laik.tugraz.at/student_detail/edit_submissions) 

[Main Page](#) [Send Feedback](#) Welcome Maria [Logout](#) | [Password](#)

## STicS – Student Tick System

[Back to Course Overview](#)

### Submissions

**Note:** Previously uploaded files cannot be deleted, only overwritten.

Assignment	Upload New File	Current File	Points	Deadline
Design Document / Extended Abstract	<a href="#">Browse...</a> No file selected.		0	2014-11-12 23:59:59
Final Project / Paper	<a href="#">Browse...</a> No file selected.		10	2015-01-21 23:59:59

[OK](#) [Cancel](#)



# Wichtige Links

## ■ TUGRAZ online

- `online.tugraz.at/tug_online/lv.detail?clvnr=183387`

## ■ Homepage

- `www.iaik.tugraz.at/content/teaching/bachelor_courses/einfuehrung_in_die_informationssicherheit/`
- `stics.iaik.tugraz.at/`

## ■ Newsgroup

- `news.tugraz.at`
- `tu-graz.lv.einfuehrunginformationssicherheit`

Nächste Woche geht's los!