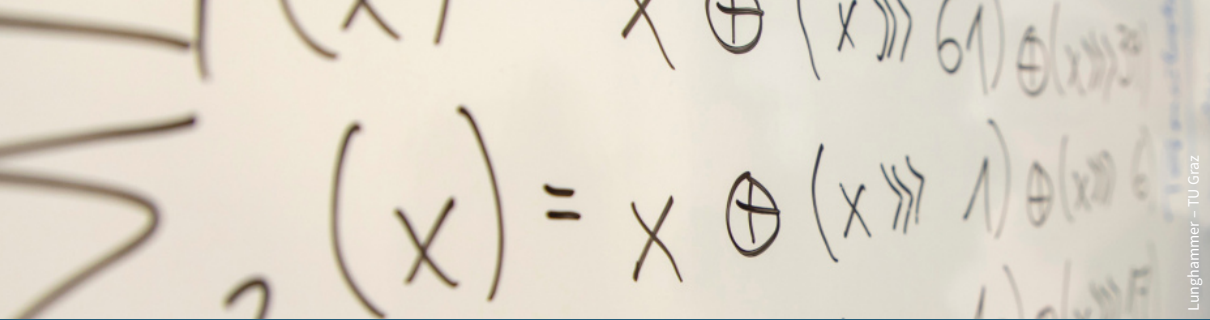


Welcome to “Information Security”

VO: Maria Eichlseder Daniel Gruss Jakob Heher
KU: Marcel Nageler Lukas Lamster Jonas Juffinger

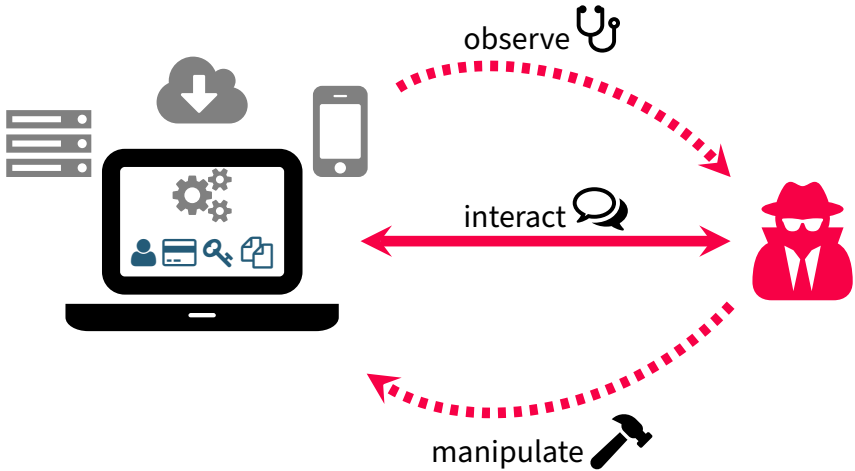
Winter Term 2023/24

Outline

Today: Introducing…

- The Team
- This Course
- Information Security
- Cryptography

Information Security



Information Security – Topics

Cryptography

- How to exchange information securely while everyone's watching?
- The mathematical perspective

System Security

- How to perform computations securely while sharing a processor?
- The system perspective

Network Security

- How to establish secure internet connections?
- The application perspective

The Team

Who are we?

System Security

Cryptology & Privacy

Formal Methods

Secure **Applications**

Team for the Lecture

Maria Eichlseder

Cryptography
Administration

- Assistant Professor
- Cryptology & Privacy

Daniel Gruss

System Security

- Associate Professor
- System Security

Jakob Heher

Network Security

- Lecturer
- Secure Applications

Team for the Exercises

Marcel Nageler

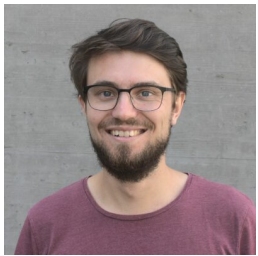
Cryptography
Administration

- PhD Student
- Cryptology & Privacy

Lukas Lamster

System Security

- PhD Student
- System Security

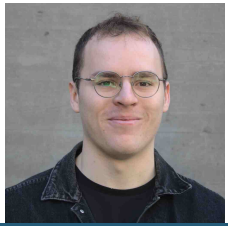


Jonas Juffinger

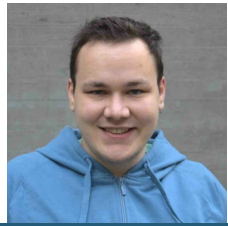
Network Security

- PhD Student
- System Security

Teaching Assistants for the Exercises



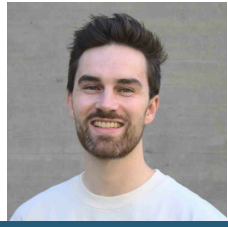
Alexander Friessnig



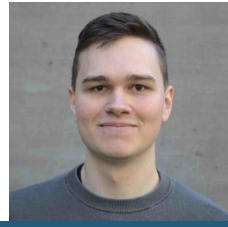
Sebastian Gollob

Benjamin Jost

Oliver Popa



Dominik Prodinger



Markus Schiffermüller

This Course

Administrative Information

When?

- 9:30–12:00 Lecture
  - actually around 9:35–11:50
  - 60 min lecture + 15 min break + 60 min lecture
- 12:00–13:30
- 13:30–15:00 Practicals
  - starts around 13:35
  - sometimes virtual – check schedule!
  - presentation of assignments, tutorials, question time

Friday	VO 9:30–12:00	KU 13:30–15:00	Midnight
06. 10. 2023	Introduction	–	
13. 10. 2023	Cryptography 1	P1 Kick-off	
20. 10. 2023	Cryptography 2	P1 Q&A	
27. 10. 2023	Cryptography 3	P1 Tutorial	
03. 11. 2023	Cryptography 4	P1 Q&A	
10. 11. 2023	System Security 1	P2 Kick-off	P1 Deadline
17. 11. 2023	System Security 2	P2 Tutorial	
24. 11. 2023	System Security 3	P2 Tutorial	
01. 12. 2023	System Security 4	P2 Q&A	
15. 12. 2023	Network Security 1	P3 Kick-off	P2 Deadline
❄ ❄ ❄			
12. 01. 2024	Network Security 2	P3 Q&A	
19. 01. 2024	Network Security 3		P3 Deadline
26. 01. 2024	Exam	–	

Why? – Course Goals

- Understand which security properties crypto algorithms offer
- Be able to choose & properly apply suitable crypto algorithms

- Know potential risks when processing data, detect certain vulnerabilities
- Know isolation techniques and protection mechanisms

- Understand attacks and defenses for network protocols & web technologies
- Understand security aspects on all abstraction layers of secure internet communication

Prerequisites

This course will be a lot easier if you remember stuff from

- **C**omputer **O**rganisation and **N**etworks
- **S**ystem-**L**evel **P**rogramming
- **D**iscrete **M**athematics
- **P**robability **T**heory & **S**tatistics
- Various programming practicals
  Useful for the KU: `C/C++`, `gdb`, Assembler, `Python`,…

How do I get a grade?

Practicals (KU):

- Team programming exercises – register a **team of 2** until next week
- 3 Assignments – more details next week!

Lecture (VO):

- Final written exam
  - 60 minutes, closed-book, pen-and-paper
  - Questions in English
  - Answers in English or German
- First exam date: 26 Jan 2024

Links

- Course website, slides & links: https://www.iaik.tugraz.at/infosec
- Discord for support: https://discord.gg/ypDW5fKHSC
  - Channel `#infosec` for general and VO questions
  - Forum `#infosec-p1` for questions on KU assignment 1
  - Channel `#infosec-groupsearch` to find team members for the KU
- TeachCenter for team registration: https://tc.tugraz.at/main/course/view.php?id=3985

Contact & Finding Help

If you need help, try (in this order):

- Discuss on Discord
- Contact the responsible teaching assistant (KU)
- Contact infosec@iaik.tugraz.at or the responsible lecturer (VO)

This lecture is not based on a particular book, but there are many nice books on information security – ask us if you need recommendations or try

- van Oorschot: Computer Security and the Internet – Tools and Jewels. Springer 2020. https://people.scs.carleton.ca/~paulv/toolsjewels.html

Information Security

A Brief Introduction


“Sicherheit”?
(1.) Safety
Adversary / Attacker
(2.) Security

Security

=

se(d) (without) + cura (care, anxiety)

freedom from anxiety

What are we anxious about?

Asset

An **asset** is anything (e.g., an information, a service, a device…)
that has value to an entity (e.g., an organization or a person).

Examples of assets on your computer:

Human secrets:  **State** secrets:  **Crypto** secrets: 

What should YOU do about it?

- Identifying assets (precisely) is the first step of any security analysis.
- Security mechanisms often shift the problem of protecting one asset to protecting another (e.g., password)

When do we consider it “protected” or “secure”?

Security Property

A **security property** defines something that makes the asset valuable.

Main security properties:

- **C**onfidentiality
- **I**ntegrity and Authenticity
- **A**vailability

Some other security properties:

- Anonymity and Privacy
- Non-repudiation of origin & delivery
- Commitment
- Time-stamping
- …

What could possibly go wrong?

Threat

A **threat** describes a potential violation of security.

The sum of all threats describes everything that can lead to a violation of a security property of the asset.

What should YOU do about it?

- Add protection mechanisms to minimize the threats and attack surface
- Repeat that until the risks of the remaining threats are acceptable

Houston, we have a problem…

Vulnerability

A **vulnerability** is a concrete flaw or weakness in a system that can be exploited by one or more threats

What should YOU do about it?

- Use established standardized security mechanisms and use them correctly
- Test and verify security features

Enter: The Adversary

Attack

An **attack** is a concrete attempt to violate one of the security properties of an asset.

What should YOU do about it?

- Prepare for the fact that things can go wrong: Update mechanisms, logging
- Provide patches and information

Information Security: Break the Chain

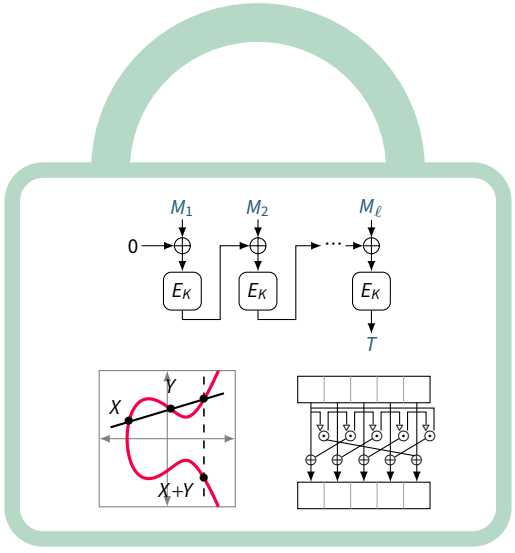
Asset + Security Properties ⛓ Threat ⛓ Vulnerability ⛓ Attack

Cryptography

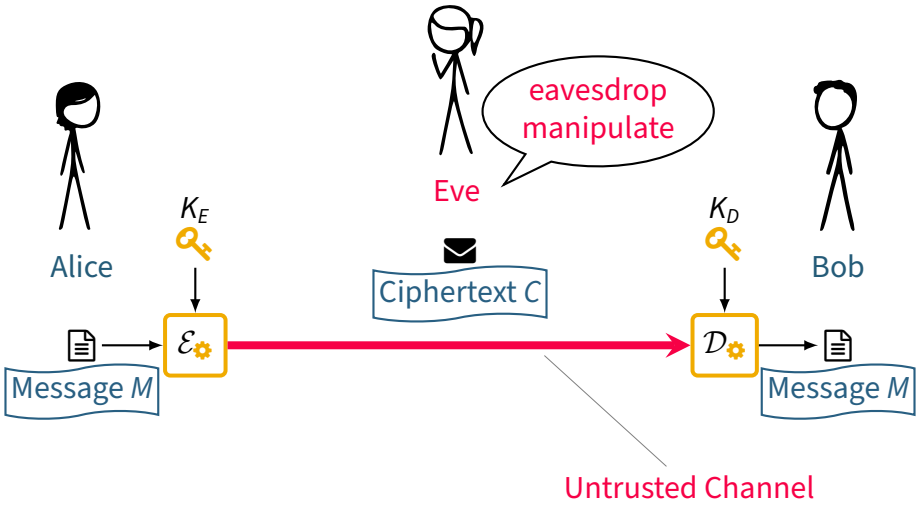
A Brief Introduction

Cryptography – The mathematical backbone of information security

Cryptography – What's inside the padlock?



~~In~~Secure Communication



Basic terminology

- Entities / parties: Alice and Bob
- Adversary: Eve

- Plaintext / message: M
- Ciphertext: C
- Keys: K_E, K_D

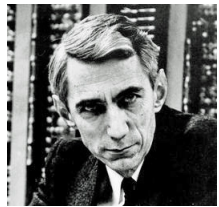
- Cryptographic scheme (algorithm, cipher): for example $\mathcal{E}$(ncrypt),$\mathcal{D}$(ecrypt)
- Cryptographic protocol: How to use the scheme?

Kerckhoffs' Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

- aka Shannon's Maxim: "The enemy knows the system"
- Opposite of "Security by obscurity"

Auguste Kerckhoffs



Claude Shannon

Historical examples

Scytale cipher (Sparta)

Caesar cipher (Rome)

Vigenère cipher (16th century Italy)

Enigma machine (1920s–1940s, Nazi Germany)

In the 1970s: The dawn of modern cryptography

- Before 1970s, cryptography is the domain of military & intelligence agencies
- In the 1970s, commercial applications for everyone emerge

- Triggers many innovations in open cryptographic research
  - Open-source symmetric crypto to protect everyone's communication
  - Asymmetric crypto to establish new communication channels

- Cryptography research is moving on, but 1970s crypto is still everywhere!
  - `DES/3DES` block cipher, `MD` hashing, `DH` key exchange, `RSA` signatures, …

Modern crypto algorithm: two families

Symmetric (secret-key) cryptography

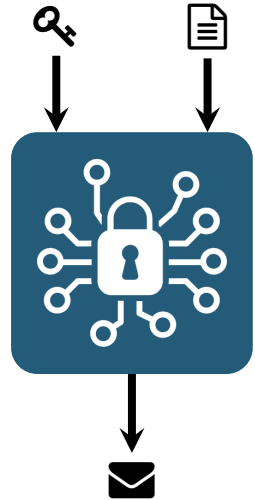
- the secret key is shared and known by Bob and Alice alone
- sender and receiver can be interchanged (insider/outsider view)

Asymmetric (public-key) cryptography

- Bob and Alice use different keys
- public keys and private keys (known only by owner – user-centric view)
- enables advanced protocols

Cryptographic primitives

- Somehow, we need to turn a bunch of simple CPU instructions into a magic box with “unpredictable” behaviour that provides a defined **security level**
- The cryptographic primitive is where this magic happens
- Not meaningful to use by itself, needs a scheme
- Examples:
  `AES` block cipher, `RSA` trapdoor one-way function



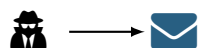
Threats – What does the Adversary want?

- Confidentiality break:

  Read secret messages?

- Authenticity break:

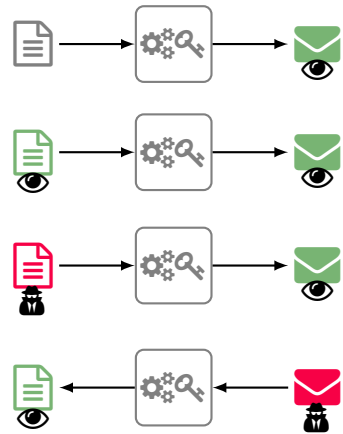
  Forge a ciphertext or signature?



- Full break: Recover the key?

Threats – What are the Adversary's abilities?

- Ciphertext-only attack?
- Known-plaintext attack?
- Chosen-plaintext attack?
- Chosen-ciphertext attack?



Terminology: The Adversary asks "Queries" to the "Oracle"

Threats – What can the Adversary exploit?

- Generic black-box attack:

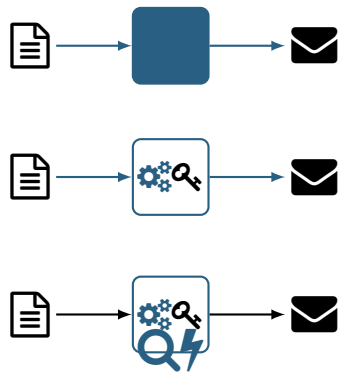
  Exploit only the interface?

- Dedicated black-box attack:

  Exploit the specification of the algorithm?

- Gray-box attack:

  Cheat with side-channels, faults, …?



Conclusion

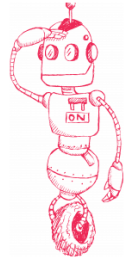
- Information security protects assets against adversaries
  - Break the chain:
    Security Property ⚯ Threat ⚯ Vulnerability ⚯ Attack

- Cryptography is the mathematical foundation of secure communication
  - Algorithms to transform data so it can be sent over untrusted channels
  - Creates a new asset: the key

Lecture Outlook – October

Crypto 1	Crypto 2	Crypto 3	Crypto 4
Symmetric Authentication	Symmetric Encryption	Asymmetric Cryptography	Protocols and Applications
Integrity	Confidentiality	Establishing communication	Theory meets Practice
Hash functions	AEAD (Auth. Encryption)	Key exchange	Protocols
MACs (Message Authentication)	Symmetric primitives	Signatures	Applications
		Asymmetric primitives	

BACHELOR'S **THESIS**



You want to do your bachelor's thesis with us? Great!

You'll agree on a topic with your advisor. Below, we list some open topics that we are currently interested in. If you have your own idea for a potential topic, get in touch with any advisor to see whether they want to supervise your thesis.

OPEN **TOPICS**

System Security

Analyzing Address Leakage	Samuel Weiser
Address Leakage Visualization	Samuel Weiser
Infosec needs you!	LosFuzzys
Spying on Hobbits - or how secure constant-time really is	Peter Pessl
Memory Encryption and Authentication	Mario Werner
Fault Attacks against MORUS/AEGIS	Robert Primas

Cryptology & Privacy

Attacks on AES with a Single Secret S-Box	Lorenzo Grassi
A Zoo of Lightweight Ciphers	Maria Eichlseder
Peer-to-Peer Contact Discovery on Smartphones	Daniel Kales
Case Study: Nonces in Practice	Maria Eichlseder
Evaluation of Cryptographic Functions against Fault Attacks	Robert Primas, Maria Eichlseder
Experimental Evaluation of Fault Attacks	Maria Eichlseder, Robert

ISW + Bachelor **Topics** + Student **Research Awards**

Friday 13 Oct 2023, 12:00–13:30

IAIK, Inffeldgasse 16a, ground floor

www.iaik.tugraz.at/bachelor

IAIK