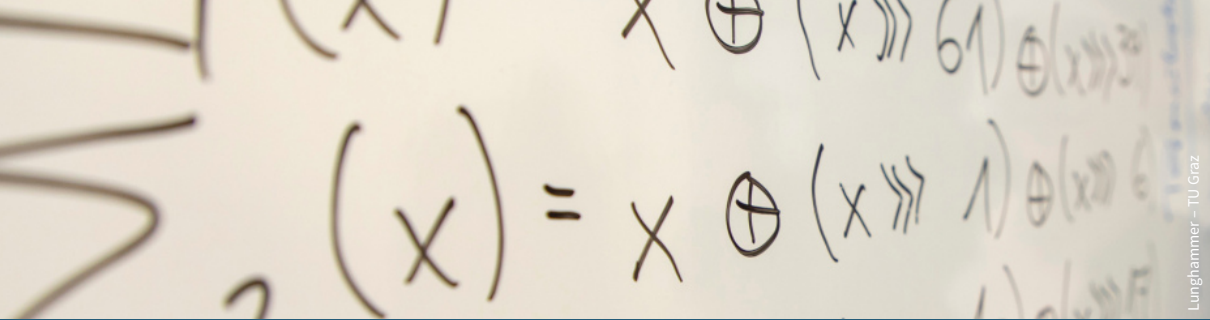


Welcome to "Information Security"

Maria Eichlseder Johannes Feichtner
Daniel Kales Peter Pessl Michael Schwarz

Winter Term 2019/20

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Introduction & Kick-Off P1

Daniel Kales

Information Security – WT 2019/20

Outline

Today: Introducing…

The Team

This Course

Kick-off for P1: Crypto-Misuse

The Team

Who are we?

Team for the Lecture

Maria Eichlseder

Cryptography
Administration

- Assistant Professor
- Cryptology & Privacy

Michael Schwarz

System Security

- PhD Candidate
- System Security

Johannes Feichtner

Network Security

- PhD Candidate
- Secure Applications

Team for the Exercises

Daniel Kales

Administration

- PhD Student
- Cryptology & Privacy

Peter Pessl

- Postdoc
- System Security

Johannes Feichtner

- PhD Candidate
- System Security

Teaching Assistants for the Exercises

Lena Heimberger

Martin Haubenwallner

Lukas Lamster

Michael Ehrenreich

Alexander Prutsch

This Course

Administrative Information

Is this “Introduction to Information Security KU”?

- Old curricula 15U, 16U: “Introduction to Information Security” aka IIS, EIS
  no longer offered – you can still do the VO exam on ...
- New curricula 19U: “Information Security” aka InfoSec
  this course is **new** and replaces IIS
- IAIK equivalence list: `https://teaching.iaik.tugraz.at/equivalences`

New (CS, ICE, SEM)				Old (SEM)				Old (CS, ICE)			
InfoSec	VO	2.5 SSt	4 ECTS	IIS	VO	2 SSt	3 ECTS	IIS	VO	2 SSt	3 ECTS
InfoSec	KU	2.5 SSt	3 ECTS	IIS	KU	1 SSt	1.5 ECTS	IIS	KU	1 SSt	1.5 ECTS
								RKN	KU	1 SSt	1.5 ECTS

- Questions? Contact your student representation or your Dean of Studies

Structure of the Practicals

3 main assignments:

Cryptography	System Security	Network Security
P1: 16 points	P2: 16 points	P3: 16 points

Work is done in groups of 2 students

- Group is fixed for the whole semester

Forming Groups

- Newsgroup for finding partners:
  - tu-graz.lv.infosec.groupsearch
- Alternative way: Meet today after lecture in front of i13

Registering Groups

- Go to https://stics.iaik.tugraz.at:
  - Create an account
    - Need to be registered for the practicals in TuG online
  - One member creates group
  - Other student joins group with the shared password
  - A detailed how-to can be found at https://teaching.iaik.tugraz.at/infosec/stics
  - Deadline for group registration: 10.10.2019 (Thursday!)
- After registration, you will be assigned a teaching assistant

Kick-Off Tutorials & Question Tutorials

- Kick-Off Tutorials
  - One per topic
  - Explanation of tasks and some hints on where to start
  - First one (P1): in a few minutes
- Question Tutorials
  - One per topic
  - We answer your questions
  - Some more helpful hints
  - First one (P1): in two weeks

Deliverables

- Deadlines
  - P1: 04.11.2019, 23:59 (Monday!)
  - P2: 06.12.2019, 23:59 (Friday)
  - P3: 24.01.2020, 23:59 (Friday)
- Hand-in via git
  - access to your repository after group-registration deadline
- Interviews
  - one interview per assignment
  - during the week following the deadline
  - 10 minutes per group, with your teaching assistant

Grading

- 3 tasks with 16 points each
  - maximum of 48 points
- You will “get a grade” if you hand in P1
  - No submission for P1 $\rightarrow$ unregistered, no grade
  - If you still want to do P2 & P3 anyway, hand in empty P1!
- Every group member gets the same grade
  - Exception: students that left the group
  - Individual point deductions at the exercise interviews

Points	Grade
≥ 42	1
≥ 36	2
≥ 30	3
≥ 24	4
< 24	5

Date	Lecture Fri 9:30–12:00	Practicals Fri 13:30–15:00
04. 10. 2019	Cryptography 1 – Introduction	P1 Kick-off Tutorial
11. 10. 2019	Cryptography 2 – Symmetric Authentication	
18. 10. 2019	Cryptography 3 – Symmetric Encryption	P1 Tutorial
25. 10. 2019	Cryptography 4 – Asymmetric Cryptography	
04. 11. 2019		P1 Deadline (Monday!)
08. 11. 2019	System Security 1	P2 Kick-off Tutorial
15. 11. 2019	System Security 2	
22. 11. 2019	System Security 3	P2 Tutorial
29. 11. 2019	System Security 4	
06. 12. 2019	Nikolaus Special	P2 Deadline
13. 12. 2019	Network Security 1	P3 Kick-off Tutorial
❄ ❄ ❄		
10. 01. 2020	Network Security 2	P3 Tutorial
17. 01. 2020	Network Security 3	
24. 01. 2020	Network Security 4	P3 Deadline
31. 01. 2020	Exam	

Rules

- Read these slides and rules at https://www.iaik.tugraz.at/infosec
- Previously on course website:
  - You needed to confirm that your read them...
  - by sending a signed email
- Due to problems with DigiCert certificate service...
  - this email is not mandatory, you do not have to send it!
- You are still encouraged to try and set up S/MIME signing for your email
  - https://teaching.iaik.tugraz.at/infosec/signature_setup

Links

- Course website:
  - https://www.iaik.tugraz.at/infosec
  - Slides, administrative info, links
- Newsgroup
  - Newsserver news.tugraz.at
  - graz.lv.infosec for questions, news
  - graz.lv.infosec.groupsearch to find partners for the practicals
- STicS:
  - https://stics.iaik.tugraz.at
  - Team registration

Contact & Finding Help

- Course website: https://www.iaik.tugraz.at/infosec
- infosec@iaik.tugraz.at
- If you need help for the exercises, try (in this order):
  - Newsgroup graz.lv.infosec
  - Contact the responsible teaching assistant
  - Contact the responsible lecturer for the practicals

Kick-off for P1: Crypto-Misuse

Crypto $\neq$ Cryptocurrency

“Crypto” is often misused

Recently in a different context...

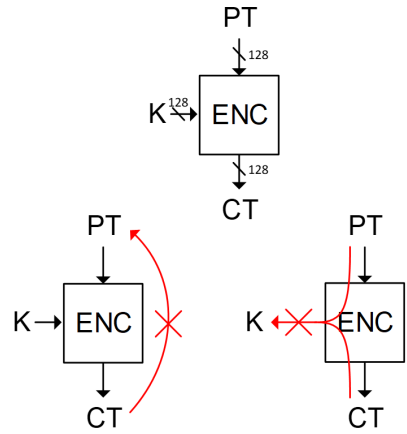
$$\text{CRYPTO} \neq \text{CRYPTOCURRENCY}$$

$$\text{Crypto} = \text{Cryptography}$$

... but there are also many mistakes in the usage of cryptography

Basic Building Block: “Block Cipher”

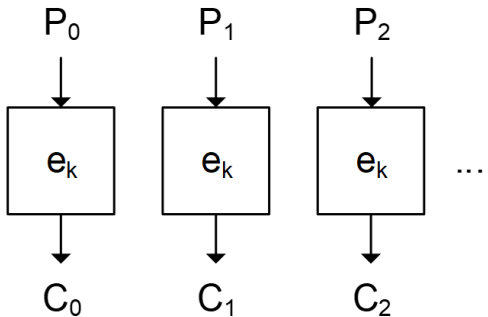
- Encrypt:
  - plaintext (PT) of fixed size (e.g., 128 bits)
  - with a secret key (K)
  - to get a ciphertext (CT) of same size
- Building block is secure!
  - Cannot recover PT from just CT
  - Cannot recover K from PT and CT



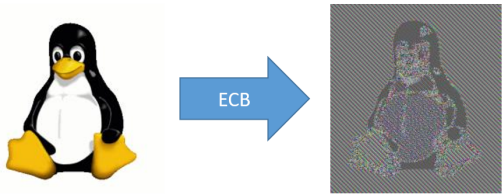
Problem: 128 bits is not much

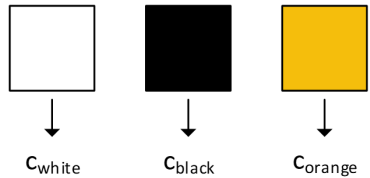
“Solution”: cut PT into blocks (P_0, P_1, ...) and encrypt seperatly

- Electronic Codebook Mode (ECB)



The Problem with ECB

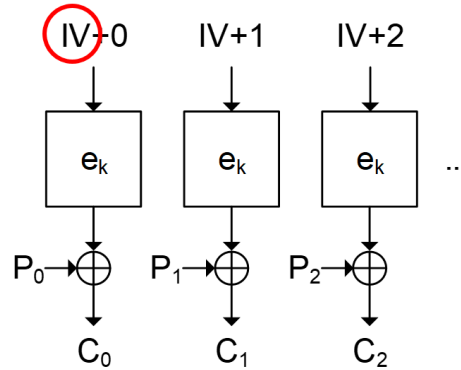




Same input block → same output!

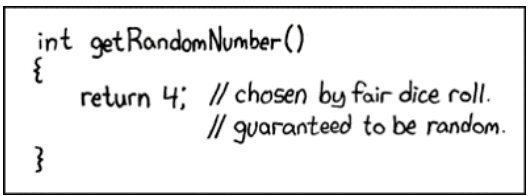
Solution: Other Modes

- Secure alternatives require initialization:
  - initialization vector (IV)
  - nonce: number only used once
  - never repeat! often need to be random!
- Randomness is required for most cryptographic primitives and protocols!



Counter Mode

How to generate random numbers?



xkcd.com/221

But who would do that?

SONY

PLAYSTATION 3

P1: Overview

- Many more mistakes possible
  - Your task is to explore and exploit these mistakes
- Your task: solve 7 challenges
  - based on common mistakes that all happened
  - recent examples are given in the assignment sheet

P1: Challenges

- Challenge model is similar for most tasks:
  - you receive challenge files (e.g., ciphertexts) ...
  - and have to find the solution (e.g., plaintexts)
  - for testing you get challenges + solution
  - for grading: we run your code with new challenges
- Language: Python3
  - 1 folder per challenge, containing 1 or more scripts
  - add your solution in the specified section (`#enter your code here`)
  - automatic comparison with the provided solution to check your implementation

P1: Assignment

- Detailed specification on a seperate assignment sheet
  - Available on course website
  - Read both the assignment sheet and these slides!
- Submission and file-distribution using git
  - repository access after group-registration deadline
  - you can start now: files also available on the website!
- Points will be published online
  - Automated test system with daily tests for each task
  - Links on course website

Questions