NTNU | Norwegian University of Science and Technology

COURSE INTRODUCTION

TTM4205 – Lecture 1

Tjerand Silde

18.08.2025

Overview

Course Staff

Motivation

Course Description

Fall 2023 and 2024

Fall 2025

Background Knowledge

Contents

Tjerand Silde

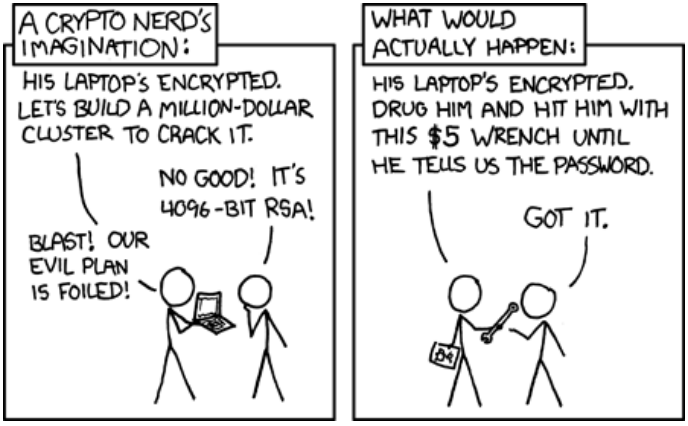
- Associate Professor in Cryptology at IIK
- Research Group Leader at the NTNU Applied Cryptology Lab (NaCl)
- PhD in privacy and crypto from IMF
- Work as Security and Cryptography Expert at startup Pone Biometrics
- Have earlier taught Linear Algebra (M3) and Discrete Mathematics at NTNU

Caroline Sandsbråten

- Lab/Teaching Assistant in TTM4205
- PhD Candidate in Cryptology at IIK
- Researching lattice-based crypto
- Master thesis on breaking ECDSA
- TA/guest lecturer in TTM4138
- Volunteer at Samfundet (ITK)

Contents

Mathematical Security vs. Real-World Security



Mathematical Security vs. Real-World Security

It is somewhere in between the above, and we need to protect against:

- correctness errors and lack of parameter checks
- side-channel and fault injection attacks
- weak or faulty randomness generation
- mismatch when composing protocols
- lack of integrity checks and bad padding

Context

- IIK created a new MTKOM profile: Cryptographic Engineering
- We wanted a new practical engineering course in cryptography
- There is a high demand from academia, industry, and government
- Very few people know cryptographic engineering in Norway...

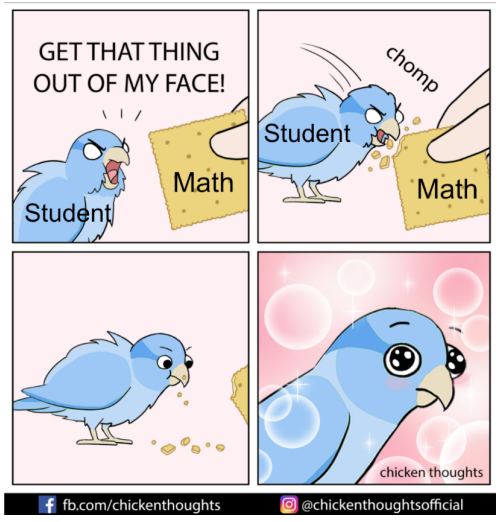
Context

Personal Reasons

I wanted to create a fun and exciting course that I wish I could have taken as a student, and acquire new knowledge that I can use for my own research.

I have included topics I hope you will find interesting and the industry will appreciate that you are familiar with. I want the course to be practical, project- and group-based, with oral presentation and reports instead of a final exam.

Goal


GET THAT THING OUT OF MY FACE!
Student
Math
chomp
Student
Math
chicken thoughts
fb.com/chickenthoughts
@chickenthoughtsofficial

Contents

Course Content

The course covers how to implement, analyse, attack, protect and securely compose cryptographic algorithms in practice. It goes in depth on how to

- implement computer arithmetic
- attack implementations using side-channel attacks and fault injection
- exploit padding oracles and low-entropy randomness
- utilise techniques to defend against these attacks
- securely design misuse-resistant APIs

Learning Outcome

Knowledge

Advanced knowledge about the mathematical building blocks underlying modern cryptography, properties of and applications of cryptographic primitives, challenges and common mistakes when implementing cryptography, side-channel attacks and countermeasures, and high level design principles for secure use of cryptography in practice.

Learning Outcome

Skills

Able to implement the underlying mathematics and high-level protocols used in symmetric key and public key cryptosystems, perform simple side-channel attacks and implement countermeasures, analyse side-channel countermeasures and design misuse resistant APIs for cryptography.

Learning Outcome

General competence

Experience on how to organise projects in small groups, conduct experiments, and write academic reports.

Learning Methods and Activities

Lectures, individual assignments, group projects, and laboratory exercises.

Further on Evaluation

Portfolio assessment is the basis for the grade in this course. The portfolio consists of one or more projects covering implementation, analysis, attacks and protection of cryptographic primitives, including a final practical assignment given at the end of the semester. This will be announced at the beginning of the term.

Further on Evaluation

The work on all tasks composes 100 % of the final grade. The results for the projects are given in points and in %-scores. The entire portfolio is assigned a letter grade. All assignments will be given in English only and reports must be submitted in English.

Further on Evaluation

If a student has the final grade F/failed, the student must repeat the entire course. Also in the case a student wants to improve their grade, they must repeat the entire course.

Recommended Previous Knowledge

The following or equivalent courses are recommended:

- TMA4140 Discrete Mathematics
- TDT4100 Object-Oriented Programming
- TDT4120 Algorithms and Data Structures
- TTM4135 Applied Cryptography and Network Security

It is also recommended to take TTM4138 Wireless Network Security, TTM4195 Blockchain Technologies and Cryptocurrencies, and/or TMA4160 Cryptography at the same time as this course.

Course Materials

To be announced at the beginning of the term.

The main course material will be given in the form of slides, notes, manuals, research papers, books and recordings.

Useful course material:

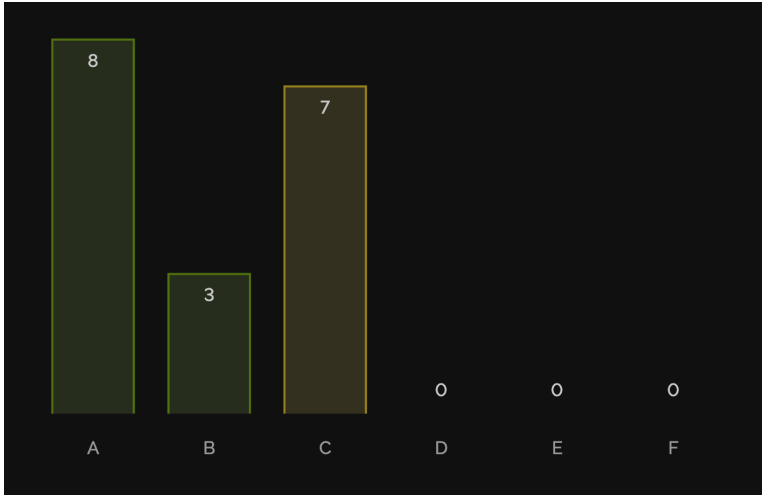
- ChipWhisperer: `https://www.newae.com/chipwhisperer`
- *Serious Cryptography* by Jean-Philippe Aumasson
- *Real World Cryptography* by David Wong
- *The Hardware Hacking Handbook* by van Woudenberg and O'Flynn

Contents

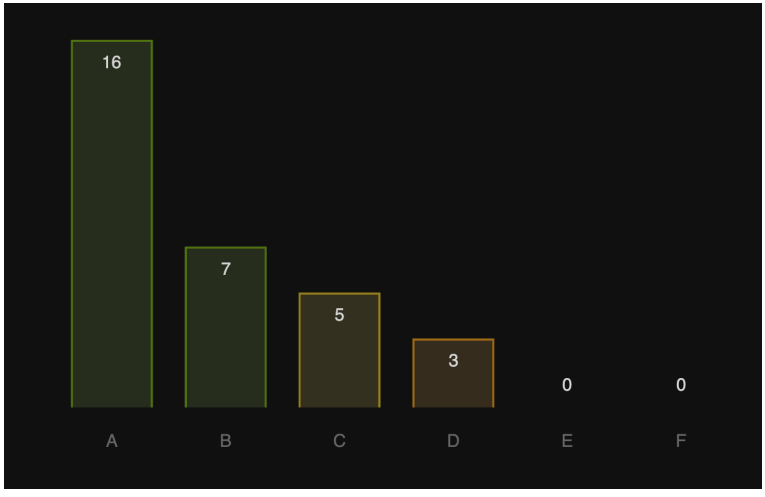
Course Information

The course material, grade distributions, and student evaluations from fall 2023 and 2024 are available on the current course website. The content is similar this year, but we have made some improvements based on the student feedback and experience from the lectures and grading.

Grade Distribution 2023



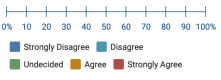
Grade Distribution 2024



Learning Activities

Learning Activities

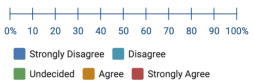
Svar	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Diagram
There were many good learning activities that required me to work actively (rather than just listen).				1	8	
The learning activities have been well prepared and clearly structured.				3	6	
The learning activities have been engaging and motivating.			1	4	4	
The course required that I prepared for the classes.		2	4	1	2	
There has been a good correspondence between the learning goals and what was asked for in the exam and/or assignments.			1	5	3	



Course Information

Teachers and Learning Assistants

Svar	Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree	Diagram
Teachers have made an effort to make the subject interesting.					9	
Teachers have been very good at explaining things.				3	6	
Teachers have also tried to understand the challenges one may have with the course and listened to feedback.				2	7	
The learning assistants have given me the type and amount of help I can expect.			1	3	5	



Contents

Course Information

This is the third time this course has ever been organized. We have planned well, but some things might go differently, and your feedback is essential.

We will make adjustments during the semester and provide help to everyone.

All course material will be made available at `http://ttm4205.iik.ntnu.no`.

Lecture Plan

This course consist of lectures and lab/exercise sessions, but note that the format varies based on the topic of the week. Watch the lecture plan carefully at the course website. Some sessions are already canceled on October 31st.

Sessions fall 2025: Mondays at 15:15-17:00 (lecture) and Fridays at 12:15-14:00 (lecture OR lab) and 14:15-16:00 (exercise OR lab) in lecture room R73.

Lecture Plan

Week	Date	Format	Responsible	Topic	Resources
34	18/8	Lecture	Tjerand	Course Introduction	
34	22/8	Lecture	Tjerand	Randomness 1: Entropy	
34	22/8	Exercises	Caroline	Exercise Class	
35	25/8	Lecture	Caroline	Randomness 2: Breaking ECDSA	
35	29/8	Lecture	Tjerand	Randomness 3: Randomization	
35	29/8	Exercises	Caroline	Exercise Class	
36	1/9	Lecture	Tjerand	Legacy Crypto 1: Crypto Wars	
36	5/9	Lecture	Tjerand	Legacy Crypto 2: Attacks on TLS	
36	5/9	Exercises	Caroline	Exercise Class	
37	8/9	Lecture	Tjerand	Padding Oracles 1: CBC and SHA	
37	12/9	Lecture	Tjerand	Padding Oracles 2: RSA Encryption	
37	12/9	Exercises	Caroline	Excercise Class	
38	15/9	Lecture	Tjerand	Quantum-Safe Encryption	
38	19/9	Lecture	Tjerand	Quantum-Safe Signatures	
38	19/9	Lab	Caroline	Exercise Class	
39	22/9	Lecture	Tjerand	Side-Channel Attack (SCA): Intro	
39	26/9	Lab	Caroline	SCA Setup Tutorial	
39	26/9	Lab	Caroline	SCA Lab 1 (2h)	

Ed Forum

We have created an Ed Forum for you to ask questions and discuss course content at https://edstem.org/eu/courses/2376.

We encourage all of you to both ask and answer questions related to the course. The staff will pay attention and follow up when appropriate.

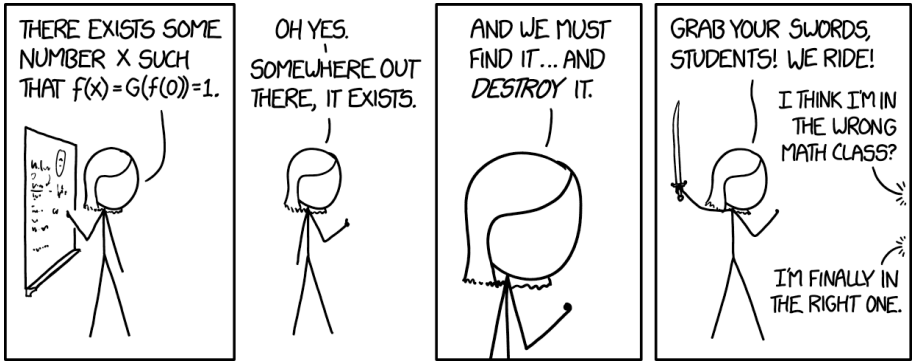
Portfolio Assignments

The course evaluation will consist of three assignments of 100 points total.

You must pass all assignments to pass the course; at least 40% on each.

We will use the official NTNU grading scale to assign combined grades: https://i.ntnu.no/wiki/-/wiki/English/Grading+scale+using+percentage+points.

Weekly Problems



Weekly Problems

This assignment is worth 40 points total. You can make up for mistakes by solving bonus problems. It contains the following kind of problems:

- Mathematics problems
- Coding problems
- CryptoHack problems

Solutions written in LaTeX. The submission deadline is December 7th at 23:59.

ChipWhisperer Lab

ChipWhisperer Lab

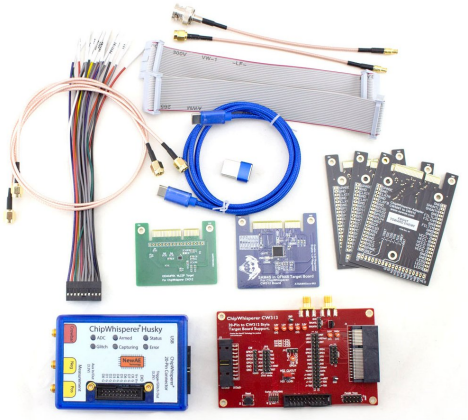


Figure: ChipWhisperer Husky

ChipWhisperer Lab

This assignment is worth 20 points total. It contains the following activities:

- Side-channel attacks (measure time and voltage during computation)
- Fault injections (make things go wrong or skip instructions)
- Analyse captured data (mean, average, difference, graphs)

Lab will be published soon. The submission deadline is December 7th at 23:59.

Technical Essay

Technical Essay

This assignment is worth 40 points total. You will write a technical essay and present about either a topic not covered by the lectures, or to cover a topic from the lectures more in-depth. You can choose the topic yourself.

Technical Essay

Most important guidelines:

- Groups of 2 or 3 students each
- Essays of roughly 8 to 10 pages
- Essays written in LaTeX
- Short oral presentations

Technical Essay

Deadlines:

- Topic/scope/group approval: **October 31st**
- Short oral presentations: **November 17th** or **21nd**
- Draft submission for feedback: **November 21nd**
- Receive feedback on draft: **December 5st**
- Final submission: December 19th at 23:59

We provide LaTeX-templates for the essay and the presentation.

Course Material

- We will make all the slides available on the course website
- You do not need to buy any books but we give recommendations
- You can make an account for free at `https://cryptohack.org`
- We provide ChipWhisperer equipment for the lab assignments

Reference Group

We highly value constructive feedback and encourage you to join the reference group. This is especially important since it is a new course, and you will have more impact than in any other reference group.

Send me an email to join. We plan three meetings during the semester.

Contents

Encryption Security

We have two common notions for encryption security:

- IND-CPA: indistinguishability under chosen-plaintext attack
- IND-CCA: indistinguishability under chosen-ciphertext attack

The difference lie in what kind of power we give to the adversary.

RSA or ElGamal encryption is only IND-CPA secure by default.

Finite Fields

- A finite set of elements
- Two operations (addition and multiplication)
- All elements except zero has inverses
- Every finite field has order p^k for prime p
- We will usually work with $\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, \ldots p-1\}$

Elliptic Curves

Let $E_{a,b} : y^2 = x^3 + a \cdot x + b$ be an elliptic curve over a finite field $\mathbb{F}_p$ of prime order p where $a, b \in \mathbb{F}_p$ and the elliptic curve group $E_{a,b}(\mathbb{F}_p)$ consists of the point at infinity $\mathcal{O}$ and all pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ that satisfy the curve equation of $E_{a,b}$. Denote the number of points in $E_{a,b}(\mathbb{F}_p)$ by $\eta_{a,b}$ and note that $\eta_{a,b}$ does not necessarily have to be a prime number.

The curve $E_{a,b}$ is a group, which means that we can compute addition $P + Q$ of points on the curve as well as scalar multiplication $[k]P = P + \cdots + P$ (k times).

Elliptic Curves

Given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ in $E_{a,b}(\mathbb{F}_p)$, then we compute the sum $P + Q$ in the following way:

1. If $P = \mathcal{O}$, output Q. If $Q = \mathcal{O}$, output P.
2. If $x_1 = x_2$ and $y_2 = -y_1$, then output $\mathcal{O}$.
3. Otherwise, let $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = -y_1 - \lambda \cdot (x_3 - x_1)$, where

$$\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \\ \frac{y_1 - y_2}{x_1 - x_2} & \text{otherwise,} \end{cases}$$

and output $R = (x_3, y_3)$.

Chinese Remainder Theorem

Let $m = m_1 \cdot m_2 \cdots m_k$, where m_i are pairwise coprime. In addition to m_i, we are also given a system of congruences

$$\begin{cases} a & \equiv & a_1 \pmod{m_1} \\ a & \equiv & a_2 \pmod{m_2} \\ & \vdots & \\ a & \equiv & a_k \pmod{m_k} \end{cases}$$

where a_i are some given constants. The original form of CRT then states that the given system of congruences always has *one and exactly one* solution modulo m.

Questions?