An introduction to the lab

TTM4135 Applied Cryptography and Network Security

Spring 2022

Quick overview

- Three weeks, three parts, one report
- Group work
- Technical support available
- Counts as 20% of your course grade

- Lab assignment (and these slides) are available in Blackboard.

Part I: PGP and GPG

Goals:

- Make a public and private key
- Sign and encrypt emails
- Verify signatures, decrypt private mails

Link to the lectures:

- Apply your knowledge of asymmetric cryptography
- Makes your email life more secure

Part II: Web server + certificate

Goals:

- Install Apache to host websites
- Obtain a certificate from a CA
- Host webpages that can be accessed through HTTPS

Link to the lectures:

- Apply your knowledge of certificates
- Teaches you how the theory is applied on ‘the internet’

Part III: TLS

Goals:

- Generate and analyse TLS traffic
- Analyse different kinds of cipher data
- Reconstruct the pre-master secret and the key

Link to the lectures:

- Demonstrate your knowledge about practical security
- Explaining how different parts of the course come together

What do we expect from you?

Part I + II: Follow the instructions, answer questions.

Part III: More “freedom” in terms of task and report.

What does that mean?

- Points are given for both doing tasks and writing the report.
- The report should answer questions, but also be insightful.
- The parts might not be equally time consuming.

Time schedule

	First week	Second week	Third week	Afterwards
Suggested	Work on part I + II	Start part III	Finish part III Start lab report	Finish report
Binding			**Lab deadline:** March 24th Tasks should be done	**Report deadline:** April 17th

If you need help

Our Teaching Assistants are available:

- Physically or on Zoom during office hours (see next slide)
- Via email (`ttm4135@item.ntnu.no`)
- Via Piazza

Searching online and asking other groups is allowed
(but plagiarism is of course forbidden)

When/where are TAs available?

	Monday	Tuesday	Wednesday	Thursday	Friday
09:00-12:00	Zoom	Sahara	Sahara	Sahara	Zoom
12:00-13:00	Zoom	Sahara	Sahara	Sahara	Sahara
13:00-14:00	Zoom	Sahara	Sahara	Zoom	Sahara
14:00-15:00	Sahara	Zoom	Sahara	Zoom	Zoom
15:00-17:00	Sahara	Zoom	Sahara	Sahara	Zoom

Sahara (F272): https://link.mazemap.com/2IYF9IJX

FAQ

Who do I contact if I have a specific question from my group?
Contact the TA email address `ttm4135@item.ntnu.no`.

Who do I contact if I have a question that other groups might also have?
Ask on Piazza.

I don’t have a group! / My group is missing! / Someone dropped out!
Contact the TA email address asap, we’ll figure something out.

Are there intermediate deadlines?
No, but you will have a bad time if you postpone all work to the end.

What should the report look like?
There is a template available, otherwise you’ll find details in the assignment.