In the name of GOD

Applied Data & Network Security

Spring 2025

Homework 2

Important Notes

- Answers to exercises must be submitted in typed form. Submitting a photo of the manuscript is not acceptable.
- Answers to questions should be short and written by you. Avoid writing answers that you are not sure of them. Negative marks will be given for incorrect parts of the answer.
- For each day of delay in submitting, 20% of the exercise grade will be deducted. After 5 days, no grade will be awarded for the exercise.
- If you have any questions about the exercises, you can ask them in the Telegram group.
- If cheating is observed, action will be taken in accordance with educational rules.
- The output of the exercise must be a pdf file, with name *ANS-HW#-Name-STID.pdf* like this one *ACN-HW1-RezaMohammadi-40200123.pdf*. Please name the rest of the items same manner and send it along with pdf file.

Question 1. Salt

What is salt in encryption? Explain it with an example.

Question 2. PGP encryption

Create a PGP key give it to your friend.

Write an email, encrypt it with your friend public key and send it.

Ask your friend to do same.

Report generate and distribute key and encryption and decryption process.

Question 3. Privacy

What is the uBlock Origin browser extension and what does it do?

Question 4. AI

https://gandalf.lakera.ai/baseline

Attack on Gandalf

In this question, we want to test your skill in prompt engineering and using social engineering techniques to attack LLMs. The **Gandalf website** is an excellent platform for practicing these skills. In this website, you are challenged with multiple levels, where Gandalf chooses a password and hides it. Your task is to discover the password using clever prompts. But Gandalf is not so easily fooled — it has been trained to resist prompt injection, and breaking its defenses is a tough task even for experienced users.

Try to pass as many levels as you can and prepare a report. Your report must include:

- The level number,
- The final successful prompt,
- And a brief explanation of your thought process at each step.

If you fail to pass any level, you should still include your failed attempts in the report and explain why they did not work.

Name your file as `gandalf_studentname_name.pdf`.

This question is exploratory in nature. Your grade will be based on your creativity in finding solutions, and your attempts to bypass Gandalf's defenses. Even if you don't get many answers, your report on the different strategies you tried and why they failed will still be evaluated.

This is an individual task and copying from others will result in severe penalties.