<div align="center">

In the name of GOD

Applied Data & Network Security

Spring 2025   ## Homework 1

</div>

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 <u>incorrect parts</u> 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. CIA Triangle

For CIA triangle proposed additional principles like "No Repudiation", find them and explain two of them. Give an example for each case.

Question 2. uBlock Origin

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

You can download it for Firefox browser from here or here.

Question 3. Base64

a) What is Base64 encoding? Explain it with example.
b) How is it different from encryption?

Question 4. Hash

Download Windows Firewall Control software from here and save the SHA256 hash of it. Calculate SHA256 for downloaded file and compare with the original SHA256 hash.

Explain the results with screenshot of them.

Question 5. AES Encryption

a) Write small program that get a string like this: "I Love network security" and encrypt it
with AES-128 with key "mySecretKey#2025" in CBC mode. For better display, the output
should be in the Base64 format.
b) Update you program and give a random IV to it.
c) Compare the result of a & b.
d) Use this online tool for decrypt your encrypted text.

Send your code and program with this homework. Put screenshot of the code and results in
your answer.