CSCS 378 1.5 Computer Security - 2025

Assignment 1

Instructions:

- This is an **open book in-class practical** examination.
- You should use **OpenSSL** cryptographic library to complete these tasks.
- You are **NOT allowed** to use other students' codes.
- Prepare **a report** and upload it and **other files (As a single ZIP)** to the LMS on or before the deadline.
  - Include **all your commands** and **outputs** you obtained in your report.
  - **Upload all your files** relevant to your work (store them under the **relevant Task folders**).

Task 1:

- Create a text file and name it using your index number (**AS202xxxx.txt**).
- Include your name and the index number in the text file.
- Encrypt the file using AES encryption and your index number (password) and name it as **[AS202xxxx]_AES_enc.txt**
- Decrypt the file and name it as **[AS202xxxx]_AES_dec.txt**

Task 2:

- Generate 2048-bit AES key and store it in a file named [**AS202xxxx.txt**]**_AESkey.txt**.
- Encrypt your created [**AS202xxxx.txt**] file using AES encryption and the generated key and name it as **[AS202xxxx]_AES_key_enc.txt**
- Decrypt the file and name it as **[AS202xxxx]_AES_key_dec.txt**

Task 3:

- Generate RAS key pair and save your private key as [**AS202xxxx_RSA_Private.txt**] and public key as [**AS202xxxx_RSA_Pulic.txt**].

Task 4:

- Obtain the **SHA1** has of your [**AS202xxxx.txt**] file and store it in a file named [**AS202xxxx**]**_SHA1hash.txt**.
- Sign your has file using your RAS key and save it as [**AS202xxxx**]**_SHA1RSAsigned.txt** .
- Verify the integrity of your signed file and show both positive and negative cases.