INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Lab 07. Cryptographic hash functions *June 7, 2024*

Please do the following exercises with your team. Choose ONLY ONE of the following programming languages TO DO ALL THE EXERCISES: C, C++, Python, Java or C#. Also choose a cryptographic library that implements SHA2 family in the programming language previously chosen.

1. Programming exercises

Using the cryptographic library of your choice to do the following exercises

1. Design a program to calculate the message digest of any file (.pdf, .txt, .docx). Please try SHA-224, SHA-256 and SHA-384 to calculate the message digest. Test your program with at least 10 different files and take screenshots of your program running.
2. Use a tool on line to calculate the message digest of any file, using SHA-224, SHA-256 and SHA-384. Compare the message digests that your program gave with the result using the on line tool.
3. Each student must write a small document that contain the following:
   - Include your full name, number and title of the lab session, date.
   - Please specify which cryptographic library you used to implement your programs.
   - Specify which files you test your program.
   - Include screenshots of your program running and also screenshots of the online tool

   Please upload the pdf of this document to Microsoft Teams.

2. Advances of project

Write with your team a document to report the following information about the problem you have chosen as a project.

1. Which cryptographic services (confidentiality, integrity, authentication, non repudiation) you need to provide to solve the problem in your project?
2. For each cryptographic services that you identified, give a cryptographic algorithm (block cipher, mode of operation, MAC, public key encryption algorithm,etc.) that provides that service? Justify your answer.
3. Give a preliminary architecture of your solution. This architecture must emphasize the cryptographic algorithms that you are planning to use, and how they are going to interact. Explain in one or two paragraphs your solution.
4. Every student must upload this report to Microsoft Teams.