Information Systems Security

Assignment #1

Due date: (28/05/2022)

(No more than 4 students in each group)

In this assignment, you can create a group of maximum 4 students to work together. Each student is fully responsible for discussing his/her group's project in details; each student must be able to describe/run/test and defend his/her group's project.

Introduction

Perhaps the most versatile cryptographic algorithm is the cryptographic hash function. It is used in a wide variety of security applications and Internet protocols. To better understand some of the requirements and security implications for cryptographic hash functions, it is useful to look at the range of applications in which it is employed. In this assignment, you are asked to research the topic of cryptography hash function.

description

in this assignment you are requested to write a report and to prepare a presentation covering at least 5 topics of the following:

- Summarize the applications of cryptographic hash functions.
- Explain why a hash function used for message authentication needs to be secured.
- the differences among preimage resistant, second preimage resistant, and collision resistant properties.
- Present an overview of the basic structure of cryptographic hash functions.
- Describe how cipher block chaining can be used to construct a hash function.
- the operation of SHA-512.
- present the birthday paradox and present an overview of the birthday attack

The report

Your report should consist of the following:

a. A title page (faculty, department, project name, date)
b. A table of content with page numbers
c. An introduction summarizes what you have presented in the report.

d. Divide your report into a set of main section and subsections. Number the main section as (1. Main section), and the subsections (1.1 subsections)
e. The font type is times
f. The font size (16 for main sections, 14 sub sections, and 12 for body text)
g. Use appropriate references for every single source you use. Moreover, list all of them in a reference section.

The presentation

Prepare a PowerPoint presentation for the report. Each group will be given no more than 10 minutes to present their work.

What should the group submit?

A) A report up to 15 pages.
B) A presentation up to 15 slides.
Both must be submitted on Moodle.

Due date: (28/05/2022)

Grade distribution

Report completeness and quality	**30%**
Presentation quality	**30%**
Discussion of the project	**40%**

Important notes

1- Late submissions are **NOT** acceptable under any circumstances.
2- Each student must contribute to the assignment work and must be able to discuss everything in details.
3- Make sure that your group members' names are written clearly.
4- Submissions start on 25/05/2022. Earlier submissions are not acceptable.

------Good luck-------