INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Introduction to Cryptography

Projects *May 29, 2024*

To develop the solutions to the following problems you must not use classical cryptography. However you can use a programming language (C, C++, C#, Java or Python) and any cryptographic library.

1. Description

Digital office

Number of students required: 3

The CEO of a small company is trying to digitalize several processes. In particular they are trying to generate the following documents automatically:

Minute is an official written statement of the motions and resolutions taken in a meeting. It is brief but a complete record of all discussions held among the members of the meeting. Memorandum is a note, document or other communication that helps the memory by recording events or observations on a topic such as may be used in a business office.

Confidential memorandum is the same as a memorandum, but this must be kept in secret. This kind of document must be seen only by the sender and the receiver.

Any minute requires to be signed by every participating member in the meeting. Memorandums require the signature of the person who write the memorandum. Confidential memos, require the signature of the person who writes the memorandum and also that only those persons authorized to see its content can read it.

Whenever a person open a signed document, he or she must be able to verify the signature of the document.

Design and implement an application using cryptography to solve this problem.

Secure grading system

Number of students required: 3

In a small school, the principal is trying to digitalize the process to register the grades of every student. In this small school they have 12 groups of 20 students. There are 6 teachers, a supervisor of teachers and the principal of the school. During a semester, every teacher must register the grades for her/his groups in a report card grades, after the teacher registered the grades of every student in the group, she or he must signed the report card grades. This document is delivered to the supervisor. Also every teacher must write a report, including his name, and identifier of the group, and comments and recommendations for every student in the group. This report is signed by the teacher and must be confidential, i.e. only the supervisor and the principal must be able to read it. The supervisor checks this document and if everything is ok, he also signed the document. Finally, the supervisor delivers the report card grades to the principal, who also signs every report card grades. The supervisor makes a report containing certain information about each report card grades: the full name of the teacher, the date and hour that he received the report card grades, the number of students that passed the course, and the average grade. He also add comments about the teacher's performance. This report must be confidential, i.e. only the principal must have access to it. The supervisor also signs this document. Everytime that someone reads a signed document, he or she must be able to verify the signature.

Design and implement a software to do the process previously described using cryptography.

Delicious recipes as a service

Number of students required: 2 or 3

In a small restaurant, a famous chef has a collection of secret recipes. She wants to store her recipes in the cloud, but not in clear, because she does not trust in the cloud provider. Also she wants that only her closest collaborators have access to them. Every collaborator, must sign a confidentiality agreement to guarantee that he or she will not reveal any recipe, before she shares any recipe. The chef shares only one recipe at a time, and she wants to share the recipe in a secure way with a collaborator. She wants to do the whole process paperless. Imagine that the chef hires your team to design and implement a solution in software using cryptography, to help her.

Secure condo management

Number of students required: 3

A condo manager owns a building with ten appartments. He has information about each tenant in the building, e.g .full name, maintenance fees payed for every tenant every month, and also information about the payments done to service providers. He wants to store this information in a secure way in his computer. He also must print payment coupons for every tenant once a month. This payment coupons must be signed by the condo manager. Also, once a month he must prepare a status certificate for every tenant, this status certificate include personal information about the tenant, and information about the payments that the tenant has made. Finally the condo manager must prepare a financial report, which includes information about the total payments he received and the amount of money spent in services. This report must be signed by the condo management. All this information can be audited by a third party, i.e. an audit must be able to check that the information has not been illegaly modified and must be able to verify the signature in every document. Design and implement a solution in software to help the condo managener, using cryptography.

2. Products

You must present advances of your project, as follows

1. **May 29**: Choose a team and send an email to sdiazsa@ipn.mx, indicating the full name of every member in the team, and name of the project you have chosen.
2. **June 7**: identification of the security services that the problem requires and the cryptographic primitives (block cipher, key exchange, hash function, public key encryption algorithm) that you will use and arquitecture of your solution.
3. **June 14**: Implementation advances of the cryptographic algorithms involved in your proposed solution
4. **June 21**: Final implementation.
5. **June 24-28**: Final Oral Presentation