



Protecting sensitive information

Team members

Ramírez Fuentes Edgar Alejandro

Rodríguez Melgoza Ivette

Salmerón Contreras María José



Table of contents

Problem to solve	2
Cryptographic services	2
Privacy	2
Integrity	2
Non-repudiation	2
Cryptographic primitives	3
System architecture	3
Introduction to the system	3
Requirements	3
References	3

Problem to solve

The CEO of a certain company is promoting less use of paper. He wishes that sensitive documents be digital. Thus, these documents usually are signed by the board of directors (group of people that take decisions in the company). Also only the board of directors can see the content of these sensitive documents. They do not want to share a unique key, i.e. every member of the board must have her/his own key or keys. Imagine that your team is hired to develop a solution for this company.

Cryptographic services

- Privacy

This service will be useful to hide the information that each sensitive document contains. As mentioned in the problem to solve, only the board of directors will be able to see the content, and privacy is the service that will help us to hide the information from any other user that does not belong to the board of directors.

- Integrity

As mentioned before the documents contain sensitive data that must not be altered in any way. That is why our system must provide integrity and keep the data without any alteration by a third party.

- Non-repudiation

The problem to solve mentions that the documents are usually signed by the board of directors, which means that the system should implement a way to help the users to sign a certain document and prevent them from denying previous commitments or actions.



Cryptographic primitives

System architecture

Introduction to the system

Requirements

References

- C. Paar and J. Pelzl, *Understanding Cryptography*, 1st edition, Springer, 2010