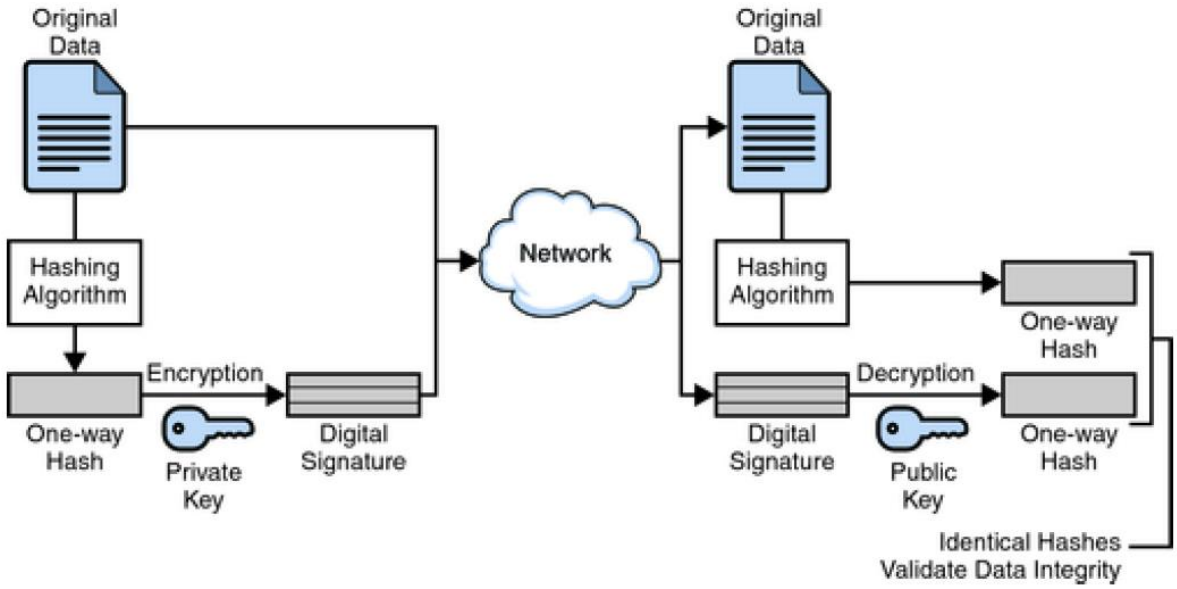
DAT 510: Assignment 3

Submission Deadline 23:59, Tuesday, 3rd November, 2020

PART 1 (80%)

Alice and bob have been trying to send the data using key exchange protocols. Now they are trying to sign and validate the data being transferred by each side. Alice and bob try to communicate and send document. Here is how the Signature scheme looks like:



As shown above, the digital signature scheme has several building blocks:

- A key exchange protocol to share public and private data
- a Hash function
- a per-user public key
- a per-user private key

This assignment requires that
_ you choose one Signature Scheme DSS;
_ you choose a hash function for use in your digital signature scheme, which should work on arbitrary length messages, but you are otherwise free to choose how to implement them.

In the actual signing algorithm, you should spend some time figuring out what sizes the different elements should have. Beware of computational problems when using big integers! The program should take a message from the user as input, sign it and store it. It must then be possible to verify the signature of stored messages. You can use the key exchange system you have built in the previous assignment. Here is a recommended design for the DSS.

- You should be able to sign the given documents
- You can then call a function to send data to other side
- The other party should be able to verify the validity of coming documents with their hashes
- Keep in mind that you can use libraries to implement hashes and key exchange since this assignment is based on the DSS implementation.

PART 2 (20%)

PKI certificates are documents that act as digital passports, assigned to any entity that wants to participate in a PKI-secured conversation. They can include quite a bit of data. the main part of it normally consists of a public key. There are several PKI implementations however the most popular public key infrastructure system is TLS/SSL protocol, which secures just about all encrypted HTTP communication in the whole internet.

1. What are the different types of SSL's and how different they are in aspect of security? Why ?
2. Research about the the Certificate Authority Security concerns and explain.
3. How does browsers identify secure CA's From another CA's and how is it measured ?

Assignment Submission

Deadline: 23:5**9, Tuesday ,** NOV**.** 3**,** 2020 **(**submit your assignment through can**v**as**)** Final submission:

1. **Source Code**

Source code submitted for the assignment should be your own code. If you have usesources from the internet everything should be added to the references. If you used someone's code without reference, that will also be treated as plagarism. Source code should be single, compressed directory in .tar.gz or .zip format.

Directory should contain a le called **README** that describes the contents of the directory and any special instructions needed to run your programs (i.e. if it requires and packages, commands to install the package. describe any command-line arguments with the required parameters).

You may use any reasonable programming language for the assignment. Reasonable languages include: Java, C, C++, Python, Javascript, R, Go and others with permission from Sohrab Chalishhafshejani (s.chalishhafshejani@stud.uis.no) or Dhanya Therese Jose (Email: dhanya.t.jose@uis.no)

You should NOT use available libraries/packages/classes for implementing the core functionality of the assignment.

2. A separate report with PDF format

Texts in the report should be readable by human, and recognizable by machine; Other formats will NOT be opened, read, and will be considered missing; Report should follow the formal report style guide in next page. Each student should write an individual report. Each report will be checked for plagiarism. If it is copied from somewhere else, you will fail the assignment.

3. A presentation on the PowerPoint

Including your voiceover describing the steps and challenges during implementation of each part. This should not be more than 10 minutes and you can include parts of your code and explain what you have done. (**DO NOT** upload videos directly to canvas. Please upload in platforms like OneDrive , Google Drive , . . . and present the link to the video when submitting)

NOTE: If you encounter problem with upload archive le (e.g. *.zip, *.tar) to the website

https://uis.instructure.com/, you should be able to upload after you add extention .txt to your

achieve le (e.g., *.tar) *.tar.txt).

Note: The assignment is individual and can NOT be solved in groups.

Project Title

Abstract

A one-paragraph summary of the entire assignment - your choices of cryptographic primitives and their parameters, procedure, test results, and analysis.

Introduction

A description of the scientific background for your project, including previous work that your project builds on. (Remember to cite your sources!) The final sentence (analogous to the thesis statement in a term paper) is the objective of your experiment.

Design and Implementation

A detailed description (in paragraph format) of the design, procedure, and implementation of your project. This should be the main part of the report.

Test Results

Results of testing the software, as you observed/recorded them. Note that this section is only for observations you make during testing. Your analysis belongs in the Discussion section.

Discussion

Your analysis of what your testing results mean, and your analysis.

Conclusion

A short paragraph that restates the objective from your introduction and relates it to your results and discussion, and describes any future improvements that you would recommend. Works Cited A bibliography of all of the sources you got information from in your report.