

**Worksheet 6 – Digital Signatures**

**Digital Signatures @.NET**

**Covered topics:**

- Concept of Digital Signatures
- Digital Signatures in .Net

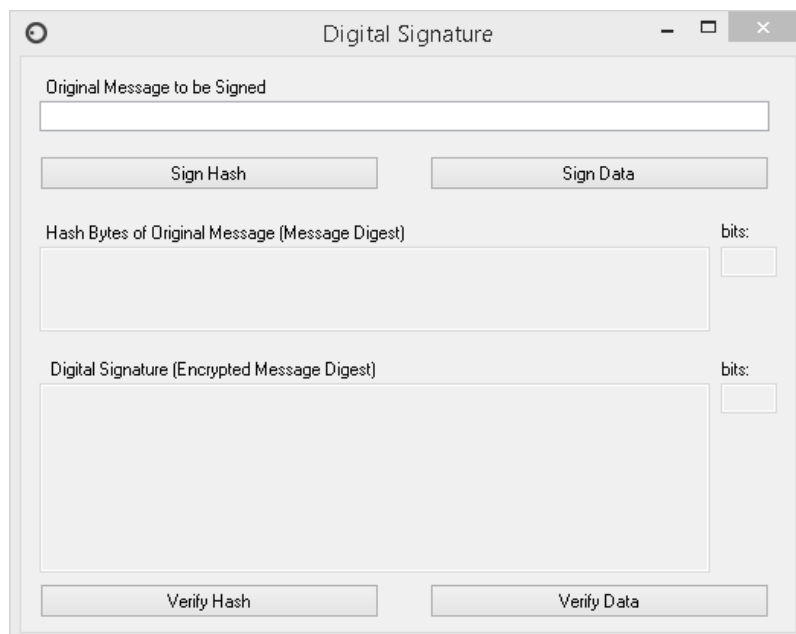
©2021: { rui.ferreira,nuno.costa,vitor.fernandes,ricardo.p.gomes,nuno.reis, marisa.maximiano }@ipleiria.pt

## 1. Digital Signatures

The next exercise shows how to use hash algorithms and asymmetric algorithms, implemented in .NET, to perform digital signatures.

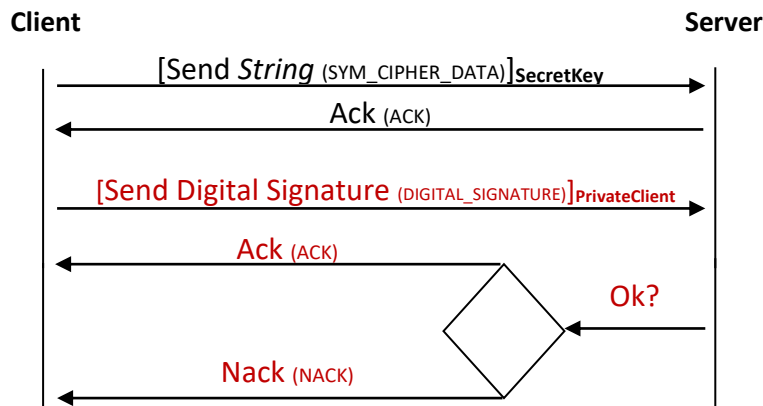
### Exercise

1. Download the project “ei.si-worksheet6-ex1.1” and use the existing form components to:



- a) Calculate the digital signature and verify it, using the methods: SignHash() & VerifyHash().
- b) Calculate the digital signature and verify it, using the methods: SignData() & VerifyData().

2. Download the project “ei.si-worksheet6-ex1.2” and implement the concept of **authentication** and **integrity** in the exchange of information. The new version of the protocol to be implemented is highlighted in red on the following image:



Note 1: the digital signature must be computed using the encrypted data.

Note 2: assume that both entities know each other.

## 2. Extra Class

### Exercises

1. Download the project “ei.si-worksheet6-ex2.1.zip” and verify that the following files exist:
  - a) “data.txt”: file with the original data.
  - b) “signature\_and\_data.dat”: the first 1024 bits are the digital signature computed over the “data.txt” file (using the hash algorithm SHA256) and the remain is the content that was signed.
  - c) “private\_public.txt”: private / public key pair used to sign the previous file.
  - d) “public\_1.txt” ... “public\_5.txt”: 5 public keys, where only one matches the private key that has signed the “data.txt” file.

Using the C# language, create a project that allows you to answer the following questions:

- 1) Who is the author of the digital signature?
- 2) Is the original file still the same as the one which was digital signed?

2. Using the project “ei.si-worksheet4-ex2.1” as a base (*from Worksheet 4*):
- a) Implement a new project to act as a Man-In-The-Middle, changing the existing projects accordingly to support this.
  - b) Verify that the MITM can see and change the data in transit.
  - c) Make the communication channel secure using asymmetric algorithms.
  - d) Verify that the MITM can no longer see or change the data in transit, without being detected.