Worksheet 4 – Asymmetric Cryptography

Asymmetric Algorithms @.NET

Covered topics:

- Concept of private and public key
- Asymmetric encryption (RSA): key exchange problem

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

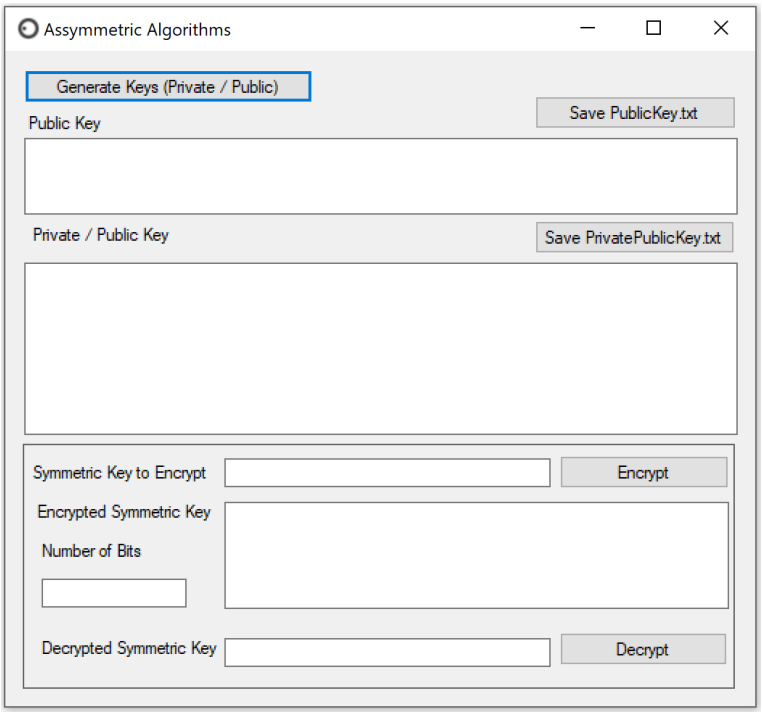
1. Asymmetric Encryption

The aim of the next exercise is to show how to use asymmetric algorithms, implemented in .NET, to achieve the asymmetric encryption.

Note: **The asymmetric encryption should not be used to encrypt data**. The following exercise is just to understand how it's made the asymmetric encryption and decryption in .NET.

Exercise

1. Download the project "ei.si-worksheet4-ex1.1" and use the existing form components to:



Note: Asymmetric encryption **should not** be used to encrypt data.

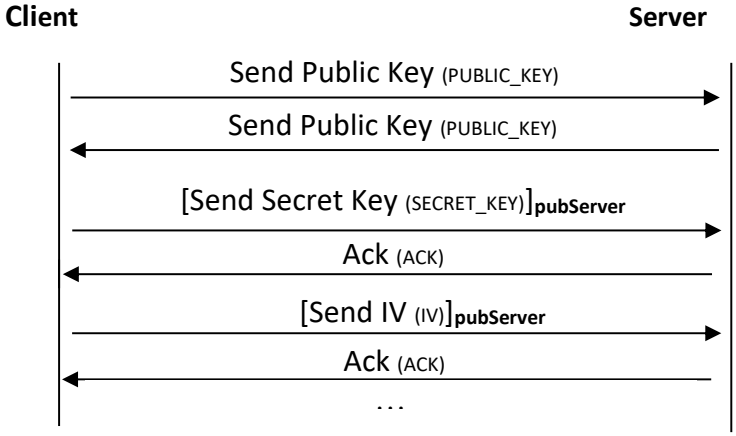
1) Generate a key pair (private / public).
2) Save the public key into a file.
3) Save the private / public key into a file.
4) Encrypt the content of the textbox "Symmetric Secret Key to Encrypt" using the public key stored previously. Place the result in the textbox "Encrypted Symmetric Secret Key" and show its length.
5) Decrypt the data in the textbox "Encrypted Symmetric Secret Key" using the private key stored previously and show the result in the textbox "Decrypted Symmetric Secret Key".

2. Key Exchange

Below, two exercises are presented, and they propose to solve the symmetric key exchange problem, since that is already guaranteed the confidentiality in data exchange. The goal is to ensure confidentially in the key exchange when this is transmitted to another entity through network.

Exercises

1. Use the "ei.si-worksheet4-ex2.1" as base project to implement security in the symmetric key exchange. The protocol adopted to change what's currently implemented is presented below:



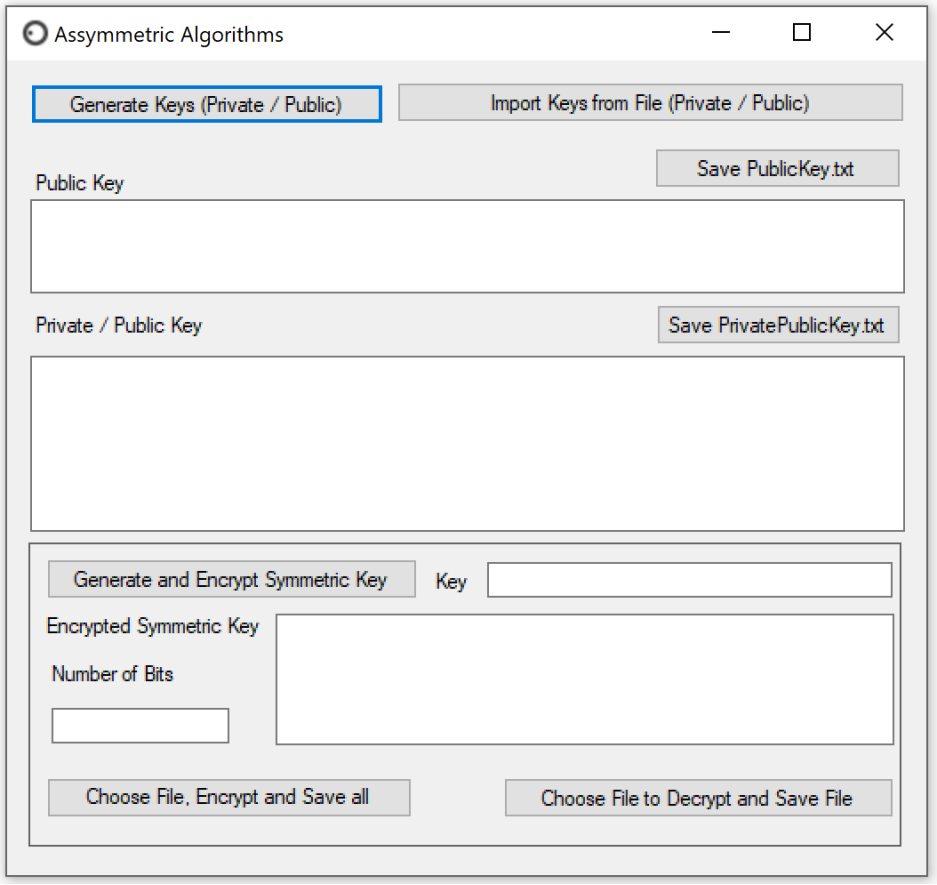
Note: must be generated a new key pair on each execution.

2. Using the projects of exercise 2.1, implement the following functionality:
    1) Every time each application runs the same key pair must be used.

3. Extra Class

Exercises

1. Download the project “ei.si-worksheet4-ex3.1” and use the existing form components, to achieve the following objectives:



1) The elements present in the project of the exercise 1.1 must maintain the same behavior.
2) The "Import Keys ..." button should allow importing public/private keys from a file.
3) The "Generate and Encrypt Symmetric Key" button should generate all the necessary components for the operation of a symmetric algorithm and encrypt the relevant ones using the previously defined asymmetric algorithm.
4) The "Choose File, Encrypt and Save all Resources" button should encrypt the chosen file, using a symmetric algorithm, and should record all the necessary resources to reverse the encryption (symmetric encrypted key, other symmetric algorithm elements, public keys / private).
5) The "Choose File to Decrypt and Save File" button should provide all the resources needed to decrypt the file, decrypt it and save it to the same directory with the extension ".data".

2. In groups of two, use the 2.2 exercise project to communicate safely.

   Note: When connected to the school's wireless network, use port 80, first ensuring that there are no services running on that port (use the "netstat -a" command to perform a search for used ports).