

Worksheet 2 – Symmetric Cryptography
Symmetric Algorithms @.NET

Covered topics:

- Confidentiality: symmetric encryption
- Encoding UTF8 and BASE64
- The key exchange problem

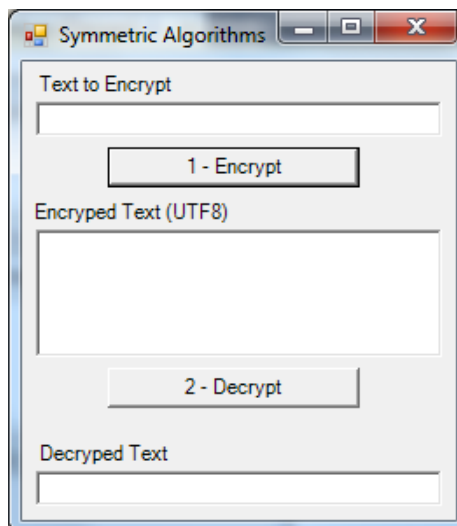
©2015: {rui.ferreira, nuno.costa,vitor.fernandes}@ipleiria.pt

1. Symmetric Encryption

The following exercises are intended to show how we can use symmetric algorithms, implemented in .NET, to ensure data confidentiality.

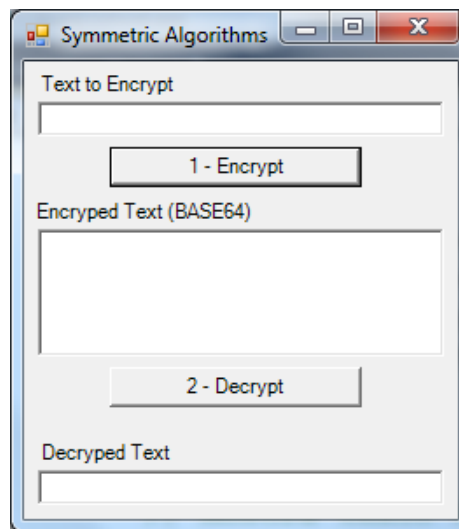
Exercises

1. Build an application, *Windows Forms Application*, and implement the following form, to:



- a) Encrypt the data in the first textbox and write the result in the second textbox;
- b) Decrypt the data previously encrypted, and write the result in the third textbox.

2. Modify the last project to:



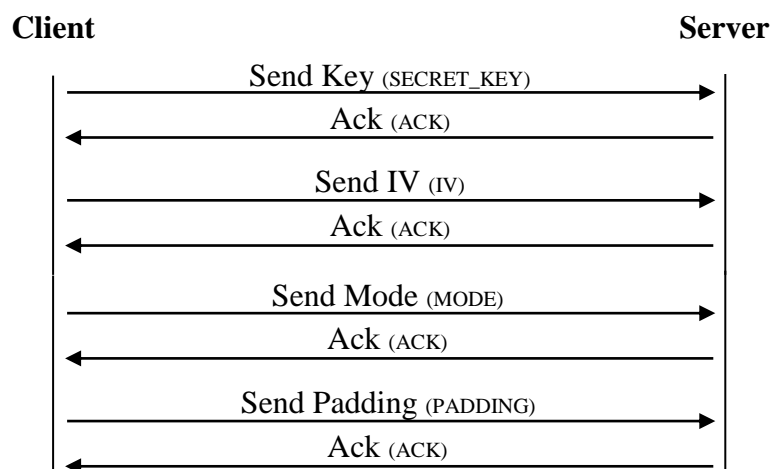
- Encrypt the data in the first textbox and write the result in the second textbox, but with the BASE64 encoding;
- Decrypt the data previously encrypted, and write the result in the third textbox.

2. Key Exchange

Next is presented an exercise where only the exchange of symmetric key is required, and some data needs to be transferred. The goal is to confirm that the generated key was properly transmitted through the network, to another entity.

Exercise

- Use the base project "ei.si_01_Start_4Encryption.zip" to implement the concept of symmetric key exchange. The protocol to adopt is the following:



Notes:

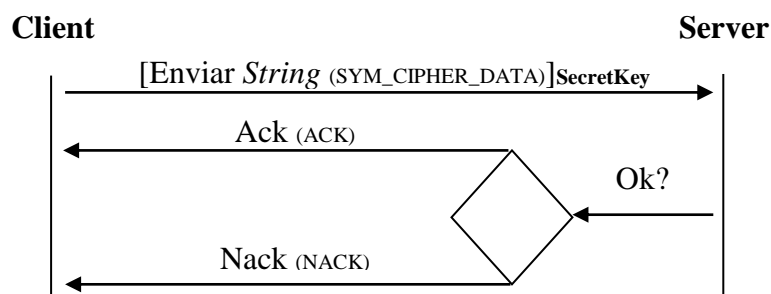
- a) Should not be exchanged any data;
- b) Must be only confirmed the information involved in the key exchange;
- c) It is not supposed that key exchange is done.

3. Confidentiality

Now that the key exchange was implemented (although in a non-secure way), it is possible to ensure that data can be securely transmitted through the network.

Exercise

1. Using the project of exercise 2.1, implement confidentiality in the exchange of data, regarding the following protocol:



Notes:

- a) Choose the algorithm / mode / padding to be used;
- b) String must be sent properly encrypted;
- c) An ACK must be returned to confirm the correct reception of the message, or a NACK otherwise;
- d) Remember that secret key is not yet exchanged in a secure way.