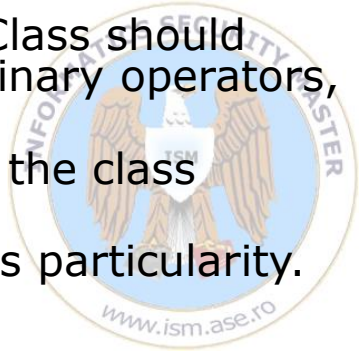
Secure Application Programming Homework

Deadline: **20 December 2017**
Evaluation: **10% in the final mark**

Requirements. Provide one single source code file considering the below requirements:

1. Define a class having the following components and features:
    1.1 Extensions (fields) to heap memory segment. All fields are private.
    1.2 Constructors.
    1.3 Destructor.
    1.4 Getter and setter methods.
    1.5 Operator overload methods as class members. Class should contain overloads for =, cast operator, other 2 unary and 3 binary operators, at least.
    1.6 Two operator overload functions defined outside the class (external functions) using the class objects.
    1.7 All other needed methods depending on the class particularity.



Secure Application Programming Homework

Requirements (cont.):

2. Define the class Cipher being able to:

2.1 Compute the SHA-256 message digest for a given input.

2.2 Encrypt and decrypt an input according to DES. The DES key is generated by a different method defined within the class Cipher.

3. Define the main function with following features:

3.1 Instantiates the defined class by using all defined constructors at 1.2).

3.2 Calls all overloaded operators by the class, including the external function overloads (1.5 and 1.6).

3.3 Calls all methods defined by the class Cipher. The digest and encryption operations are validated against the initial input (clear input message).

Important notes:

1. The source code file must be uploaded on SAKAI assignment.

2. All identical source code files will be eliminated from the evaluation.