IT&C Security Master Program
Secure Application Programming
June 2024

Note: The entire Java solution must be implemented in a single .java file. You can use multiple static methods.

Using the input file ***msg.txt*** implement a Java application that will:

1. (1.35 points) Compute and display a SHA-256 hash value. The value is displayed using hexadecimal symbols.

2. (1.35 points) The file will be **encrypted** using AES in CBC mode with

- An IV vector having the 6th byte (it's position, not the index) from left to right equal with CCh. The IV value is NOT written in the encrypted file because is a known value.
- A password equal with "passwordsecurity" The output file is called ***enc_msg.aes***

3. (1,8 points) To assure the destination that no one is tampering with that value, digitally sign (SHA-256) the previous encrypted binary file with your private key. Store the signature in another binary file. Using keytool generate a RSA pair. Export the public key in a X509 .cer file (**the key date must be the exam key. Older keys are not accepted**). Use the private key to sign the previous file, ***enc_msg.aes***.

Upload

- your java solution
- your binary file with the signature
- your public certificate.

To get the points, the digital signature must be validated for the previous file with your public key