Computer Science and Engineering Department

Group Name&Surname: Mehmet Taha USTA & Burcu ÖZTAŞ

Identity Numbers: 21527472 & 21483435

Course: BBM-465 Information Security Lab.

Experiment: Assignment 1

Subject: Asymmetric Cryptography, Hashing& Digital Signatures

Due Date: 18/11/2019 - 23:59

Advisor: Dr. Ahmet Selman BOZKIR

Problem

At this project,It is required which subject is Asymmetric Cryptography,Md5 and Digital Signatures.Although symmetric ciphers have strong features, the mediator between the two sources is extremely vulnerable to the attacks of the source. Asymmetric encryption provides the solution to this problem.As is stated, in this experiment, we are expected to develop of a licensing framework by utilizing the methods of asymmetric cryptography, MD5 and digital signatures. The following lines state the requirements of out assignment.

Method & Solution of Problem

The program starts from main.java
First, the client creates.
After creating the client, it checks the existence of the license.txt file with the check function.
The check() function returns a boolean value.
Collects credentials if the file exists.
The information is encrypted with the RSA algorithm using the encrypt() function.
The encrypted information is processed by the Md5 hash algorithm with the Md5() function.
With the result from the Md5 hash algorithm, the license file is verified.
Validation is performed with the verification() function.
The verification() function returns a boolean value.
If validation fails, the process() function is called and the license file is rebuilt.
If there is no file, the process() function is called.
The process() function collects credentials.
The collected credentials are encrypted with the Rsa algorithm using the Encrypt function and public key.
The encrypted data is then sent to the Md5 () function for verification.
The result in the Md5() function is stored for later use. The encrypted data is sent to the Licence Manager with the send() function.
The data sent is decrypted with the decrypted() function and the private key in the Licence Manager.

The decoded data is hashed by the Md5 algorithm with the Md5() function.
Encrypted data is processed with the SHA256withRSA algorithm and private key in the sign() function.
The result of the Sign function is sent to the client.
The signature verification() function from the client is validated with hashed Md5 and public key, and the boolean value is returned.
If the Boolean value is True, the signature is written to the file.
If it is False, it gives an error.