Lab A – Introduction to Cryptography

Overview

The notion of cryptography consists of hiding secret information from non-trusted peers by mangling messages into unintelligible text that only trusted peers can rearrange. In this lab, we will use and compare three different techniques commonly employed to hide or encrypt information: secret key cryptography (DES), and public key cryptography (RSA).

1. DES encryption/decryption

In this part of the lab, we will be coding a program to encrypt and decrypt files using DES. Before you working on this part, please check out the following example:

http://www.mkyong.com/java/jce-encryption-data-encryption-standard-des-tutorial/

The above example does the encryption/decryption for a string text. In this assignment, you will extend this code to take an arbitrarily sized input file and encrypt/decrypt it. Your output file should be named as “test.des”

2. RSA encryption/decryption

In this part of the lab, we will be coding a program to encrypt and decrypt files using DES. Before you working on this part, please check out the following example:

http://javadigest.wordpress.com/2012/08/26/rsa-encryption-example/

The above example does the encryption/decryption for a string text. In this assignment, you will extend this code to take an arbitrarily sized input file and encrypt/decrypt it. Your output file should be named as “test.rsa”

3. Performance measures for DES, and RSA

The final part of this lab consist on measuring the time DES, and RSA take to process files of different sizes.

a. Generate text files with the following sizes:
   - For DES (in bytes): 8, 64, 512, 4096, 32768
   - For SHA-1 (in bytes): 8, 64, 512, 4096, 32768

b. Encrypt and decrypt all these files using the DES function that you wrote in part 1. Measure the time it takes to encrypt and decrypt each of the files. To do this, you might want to refer to http://www.mkyong.com/java/how-do-calculate-elapsed-execute-timein-java/. Add these timing functions to your implementation of part 2.

c. Measure the time for RSA encryption and decryption for the file sizes listed in part a using the program you wrote in part 2.

Deliverables

- All students, regardless of whether they are working alone or with someone else, must submit their solutions via Canvas.
- For this particular assignment, please follow these specific instructions:
  - You need to submit the two **java program** you wrote.
  - Word document
    - Tables showing: (i) DES encryption / decryption times; (ii) RSA encryption times; (iii) RSA decryption times for different size files.
    - Answer the following questions
      - Compare DES encryption and RSA encryption. Explain your observations.
      - Compare RSA encryption and decryption times. Can you explain your observations?

How to use Eclipse

- If you don't know how to use Eclipse for Java Programming, below are some good references for you:
  - Eclipse IDE Tutorial: http://www.vogella.com/tutorials/Eclipse/article.html
  - Youtube: **Start from 4:40**

    https://www.youtube.com/watch?v=mMu-JlBrYXo