INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Selected Topics in Cryptography

Session 07: RSA schoolbook *November 6, 2024*

1. Project task

Do a calendar activities for each member of the project. You must describe the activities that you must complete each week. Your calendar must start on November 4th and end on December 20.

2. Programming exercises

You can use C/C++, Java or Python to develop your source code, but please use only one of these languages to develop all the exercises. You can use a cryptographic library but only for specific purposes described in each exercise. Also you can use a library to do arithmetic with big integers.

1. Design and implement a function to generate the pair of keys for RSA. Please consider the following requirements:
   - You must use a cryptographic pseudorandom function.
   - Each prime number must have 512 bits. You can use a function on a cryptographic library to generate each prime.
   - You can use a function in a library to compute a multiplicative inverse and/or calculate the greatest common divisor.
   - Your function must store the private key in base 64 in a text file. The public key must be stored, also in base 64 in a different text file.
2. Design a function to encipher a message with RSA. Your function must receive a public key and the message. The output will be the ciphertext in base64.
3. Design a function to decipher a ciphertext with RSA. Your function must receive a private key and a ciphertext. The output will be the plaintext.
4. Use the previous functions to generate a key pair for RSA. Then encipher/decipher a password of at least eight characters. **Please avoid to edit your source code to change any parameter**.

3. Products

Every student must write her/his own report including the following information:

1. Your personal information, date of the lab session and the topic that we are studying in this lab session.
2. Your own calendar of activities for the project.
3. The source code used to implement the points of Section 2. Please include a brief paragraph explaining each function.
4. Screenshots of your programs running.

4. Evaluation

- Advances in class: 2 points
- Source code: 3 points
- Program running: 3 points
- Report: 2 points

Deadline : November 12, 2024.