Cryptography & Blockchain – 5IF, INSA Lyon

RSA

Attempt the following exercises. Describe your analysis results in a report. Upload your report and source code to the course's Moodle website.

1. Implement the RSA key pair generation, encryption and decryption functions. You may use any programming language e.g. Python, C++, Java.

2. Generate a pair of 1024 bit keys. Use your implementation of RSA to encrypt several plaintext messages. Decrypt the ciphertext to verify the correctness of the cryptosystem.

3. Publish your public key on the course's Moodle website. Ask a class colleague to send you encrypted messages. Decrypt the ciphertext to verify the correctness of the cryptosystem.

4. Digitally sign as well as encrypt a message and send it to a class colleague. Ask them to verify the integrity of the message.

5. If not done so already, enhance your implementation of RSA so that it can handle the encryption and decryption of messages larger than the key size.

6. Analyze the performance of your RSA implementation for 1024 bit keys and varying message sizes. Observe performance in terms of the processing time required for encryption as well as the size of the ciphertext. You may use the following plaintext message sizes: 2^{10} B, 2^{11} B, 2^{12} B, …, 2^{22} B.

7. Compare the performance of your RSA implementation with the performance of your DES implementation for varying message sizes. Observe performance in terms of the processing time required for encryption as well as the size of the ciphertext. Analyze the results.

Additional exercises:

8. Use an existing library implementation of RSA to encrypt, decrypt, and sign messages. In Python, an implementation of RSA is available in the 'cryptography' library.

9. Cryptanalyze RSA in order to determine the private key from a given public key. Use the brute force attack or the attack based on solving the factoring problem. Perform the cryptanalysis for the following key sizes: 2^2 b, 2^3 b, 2^4 b, 2^5 b, … or until the cryptanalysis becomes too time-consuming. Analyze the results.