Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Lab 2

Nhat Nam Nguyen
nhatnamcse@gmail.com

29/02/2016

Part 1. RSA DEMONSTRATION

Install CrypTool 1 (version: 1.4.31 Beta 06 - English) by going to
https://www.cryptool.org/en/ct1-downloads
Get familiar with the options of the program and its On-Line Help.

Please go through all steps of the RSA Demonstration (available under Indiv. Procedures => RSA Cryptosystem => RSA Demonstration...).

Perform this procedure for at least the following sizes of the RSA keys (understood as the size of N in bits):

- 16 bits (CrypTool default)
- 256 bits
- 2048 bits

Assume the equal sizes of P and Q.
For each case, record values of:

- All components of a public key

- All components of a private key
- Message
- Ciphertext

Question 1: Try to encrypt 1, 10, N-1, and N-10 and see if the results match your expectations. Record and discuss your findings.

Hint: *In order to do that you will need to set your Input as numbers (as opposed to text). Please see the corresponding setting of CrypTool in the RSA Demonstration window.*

Question 2: The RSA encryption algorithm works with numbers. As your task is to encrypt some textual messages, we obviously need a method for coding of a message into numbers. The method is used in Lab is b-adic (where b is the number of plaintext elements). **Let perform the RSA encryption of *your name* with the block length of 2 and 27-adic coding**.

Part 2. FACTORING

Using the beginning of the RSA Demonstration generate values of N for at least the following initial sizes:

- 50 bits
- 100 bits
- 150 bits.

For each size of N, double click on N, and then copy the entire value of N to the Input field in the window Factorization of a Number, obtained by choosing Indiv. Procedures => RSA Cryptosystem => Factorization of a Number...

For each case, include in the report:

- Value of N
- Values of P and Q obtained after factoring N
- Sizes of N, P, and Q in decimal digits
- Factoring time
- Method used for factoring (listed after clicking on "Details", and then choosing "Save list into main window")

Find experimentally the size of N for which the factoring time is consistently greater than

- One minute (required)
- Five minutes (bonus).

Then, generate the same size number(s) randomly (e.g., by typing arbitrary digits until the required size is reached). Factor these random numbers and record the same information as in case of N obtained using RSA Key Generation.

Hint: *Please keep clicking on "Continue" until the number is fully factored. Have you noticed any changes in the execution time or method(s) used?*

HOMEWORK

Part 3. Implementation and Analysis of RSA in CrypTool 2

Install CrypTool 2.0 (Beta 12 - RC2 - Build 6121.1) by going to
https://www.cryptool.org/en/ct2-downloads

Using visual programming available in CrypTool 2, prepare a demonstration of the operation of a hybrid system based on the use of RSA and AES.

AES should be used for the secret-key encryption of messages, and RSA for the exchange of AES session keys.

The demonstration should visualize all major operations performed on the sender's side and the receiver's side, and should allow exchange of medium size messages in English. The users are assumed to know each other's public keys.

As a part of your solution, please submit your CrypTool 2 project in an electronic form, and write a short report including screenshots illustrating your project operation on the sender's side and on the receiver's side.

THE END