Assignments - Information Security 2019

Nguyen Minh Huong, ICT Lab, USTH

October 3, 2019

Exercise 1

Based on the provided description of the A5/1 cipher, write a program in Matlab or using C++ to implement the A5/1 Key generation algorithm. List n the keystream bits, suppose that the values of registers are provided X_0 , Y_0 , Z_0

Test the program with following values: $X = (x_0, x_1, ..., x_{18}) = (1111101010101010101)$ $Y = (y_0, y_1, ..., y_{21}) = (110011001100110011)$ $Z = (z_0, z_1, ..., z_{22}) = (11100001111000011110000)$ n = 10

Exercise 2

Based on the provided description of the square- and-multiply algorithm, write a program to calculate exponentiations $x^e \mod m$

Exercise 3

Based on the provided description of RSA cryptosystem, write a program in Matlab or using C++ to implement RSA encryption and decryption process. System parameters p, q, e or d are given. Define keypair, ciphertext C if plaintext M is given, and reversely.

Test the program with following parameters:

- 1. p = 5, q = 11, e = 3, M = 9
- 2. p = 3, q = 11, d = 7, M = 5

Note

Documents are provided via email.