06-20008 *Cryptography*
Autumn Semester 2019
David Galindo

The University of Birmingham
School of Computer Science
Week 7

Exercise Sheet 3

Solutions will be published on **22 November 2019, 5pm**.

This is a **formative** assignment (i.e. it does not count towards the final mark). You can ask questions in the exercise classes on November 15th, 22nd.

In this assignment, we are going to study the *plain RSA* cryptosystem.

1. **Modular arithmetic.** Compute by hand the following discrete exponentiations in $\mathbb{Z}_{11}^*$:

   (a) 4^{13} (b) 3^3 (c) 5^{12} (d) 10^{-10}

   Make sure to use as much as possible Fermat and Euler's theorems.

   2

2. **Toy RSA example.** Perform by hand RSA secret key generation, encryption, and decryption for the following parameters:

   (a) $p = 7, q = 11, e = 67, M = 75$

   (b) $p = 5, q = 13, e = 35, M = 54$

   Make use as much as possible of Fermat, Euler theorems and of the properties of the GCD function (and related algorithms).

   2

   The Collaborative Calculation in the Cloud (CoCalc) project contains the **open-source mathematical software** SAGEMATH, which provides software libraries for operating with cryptography and large integers. You can register and use it for free at `https://cocalc.com`. As a taster of its functionalities, you are invited to experiment with the worksheet

   https://cocalc.com/projects/c8485f58-7b8f-4a8e-a1f4-4e71cd290077/files/Part%201.sagews

3. **Common modulus.** Assume that Alice and Bob want to share the same modulus N but use different public exponent. Alice uses $e_A = 3$ and Bob uses $e_B = 5$. Now Charlie wants to encrypt a message m for Alice and Bob. He sends:

   $$c_A = m^3 \mod N$$

   to Alice and

   $$c_B = m^5 \mod N$$

   to Bob.

   (a) Explain how Eve can recover m from N, e_A, e_B, c_A and c_B by only using publicly available information.

   (b) Apply the procedure above to recover m from the values of N, e_A, e_B, c_A and c_B given in the Sagemath worksheet at

   https://cloud.sagemath.com/projects/c8485f58-7b8f-4a8e-a1f4-4e71cd290077/files/Part%202.sagews

   4