Foundations of Cryptography
Exam (duration 3h), 27.10.2017

In the exam, one is allowed to have pencil, eraser, ruler, permissible calculator, and a sheet of mathematical formulas (given by the invigilators of the exam).

Answer to all the questions in the exam.

1. (a) Give the definition of a *congruence* of a and b modulo n.

   (b) Calculate the remainder when $7^{3333} + 251617^8$ is divided by 11.

   (c) Solve the linear congruence

$$91x \equiv 13 \pmod{205}.$$

2. Consider an RSA cryptosystem with the public key $n = 221$ and $e = 35$ (the encryption exponent).

   (a) Encrypt the message $M = 17$.

   (b) Determine the decryption exponent d. Then decrypt the secret message $m = 205$.

3. Using Chinese remainder theorem, solve the system of congruences

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 1 \pmod{7} \end{cases}.$$

4. (a) Give the definitions of *quadratic* and *non-quadratic residues modulo n*.

   (b) Assume known that 857 and 503 are primes. Determine whether 503 is a quadratic residue modulo 857 or not.

   (c) Solve the second degree congruence equation $2x^2 + 3x - 11 \equiv 0 \pmod{31}$.