Foundations of Cryptography

Exam (duration ca. 3h), 5th of December 2016

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. Let a and b be integers and n be a positive integer.
   (a) Give the definition of a *congruence* of a and b modulo n.
   (b) Show that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
   (c) Determine the remainder when $5^{2017} + 120520^5$ is divided by 11.

2. Let n be a positive integer.
   (a) Give the definition of the *reduced residue system* $\mathbb{Z}_n^*$ *modulo* n.
   (b) List the elements of $\mathbb{Z}_{30}^*$.
   (c) Prove that all elements in the reduced residue system $\mathbb{Z}_n^*$ modulo n have an inverse regarding the multiplication congruence classes. (Formal proof is required.)
   (d) Find the inverse of $\overline{11}$ in $\mathbb{Z}_{30}^*$.

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

$$\begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 5 \pmod{13} \\ x \equiv 1 \pmod{14} \end{cases}.$$

4. Consider the polynomial ring $\mathbb{Z}_2[x]$.
   (a) Show that $r(x) = x^3 + x + 1$ is an irreducible polynomial in $\mathbb{Z}_2[x]$.
   (b) List the elements of the finite field $GF(2^3)$ induced by the irreducible polynomial $r(x) = x^3 + x + 1$.
   (c) Let $p(x) = x^2 + x + 1$ and $q(x) = x^2 + 1$. Calculate $p(x) + q(x) \pmod{r(x)}$ and $p(x)q(x) \pmod{r(x)}$.